Capítulo 4: Capa Red - III

ELO322: Redes de Computadores

Agustín J. González

Este material está basado en:

- Material de apoyo al texto *Computer Networking: A Top Down Approach Featuring the Internet*. Jim Kurose, Keith Ross.

Capítulo 4: Capa de Red

- 4. 1 Introducción
- 4.2 Circuitos virtuales y redes de datagramas
- 4.3 ¿Qué hay dentro de un router?
- 4.4 IP: Internet Protocol
  - Formato de Datagrama
  - Fragmentación
  - Direccionamiento IPv4
  - NAT: Netwoork Address Translation
  - ICMP
  - IPv6
- 4.5 Algoritmo de ruteo
  - Estado de enlace
  - Vector de Distancias
  - Ruteo Jerárquico
- 4.6 Ruteo en la Internet
  - RIP
  - OSPF
  - BGP

Direcciones IP: ¿Cómo obtener una?

Q: ¿Cómo obtiene un *host* su dirección IP?

- Configurada por el administrador en un archivo
  - Windows: ver versión específica
  - Linux: ver versión específica
- Vía protocolo de configuración dinámica DHCP: Dynamic Host Configuration Protocol: el host obtiene la dirección dinámicamente desde un servidor
  - “plug-and-play”

DHCP: Dynamic Host Configuration Protocol

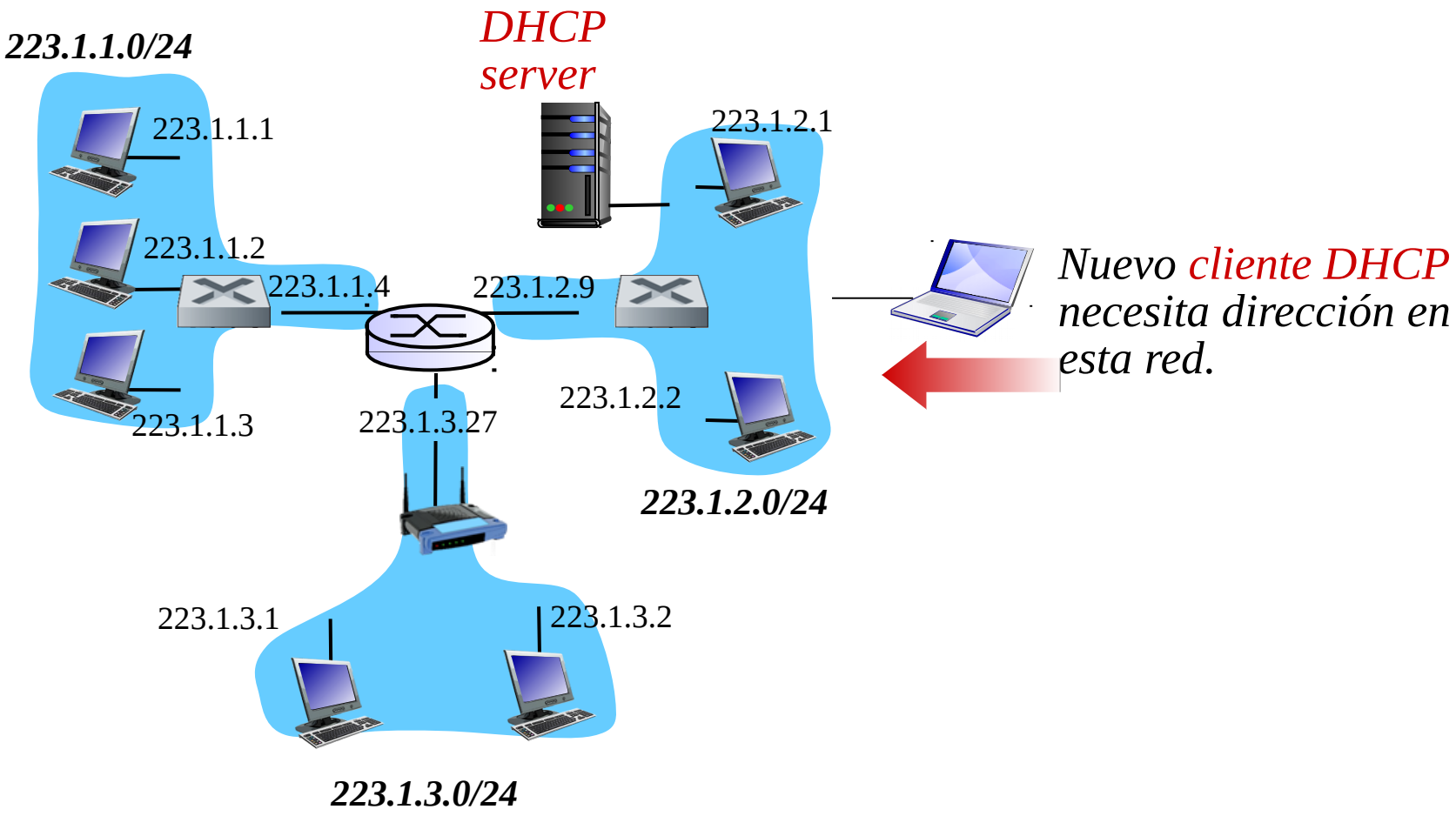
Objetivo: permitir a un host obtener *dinámicamente* su dirección IP desde un servidor en la red cuando el host se integra a la red.

- El host puede renovar y extender el uso de su dirección
- Permite el reuso de direcciones (la dirección sólo se mantiene mientras se esté conectado).
- Conveniente para usuarios móviles que se conectan por corto tiempo.

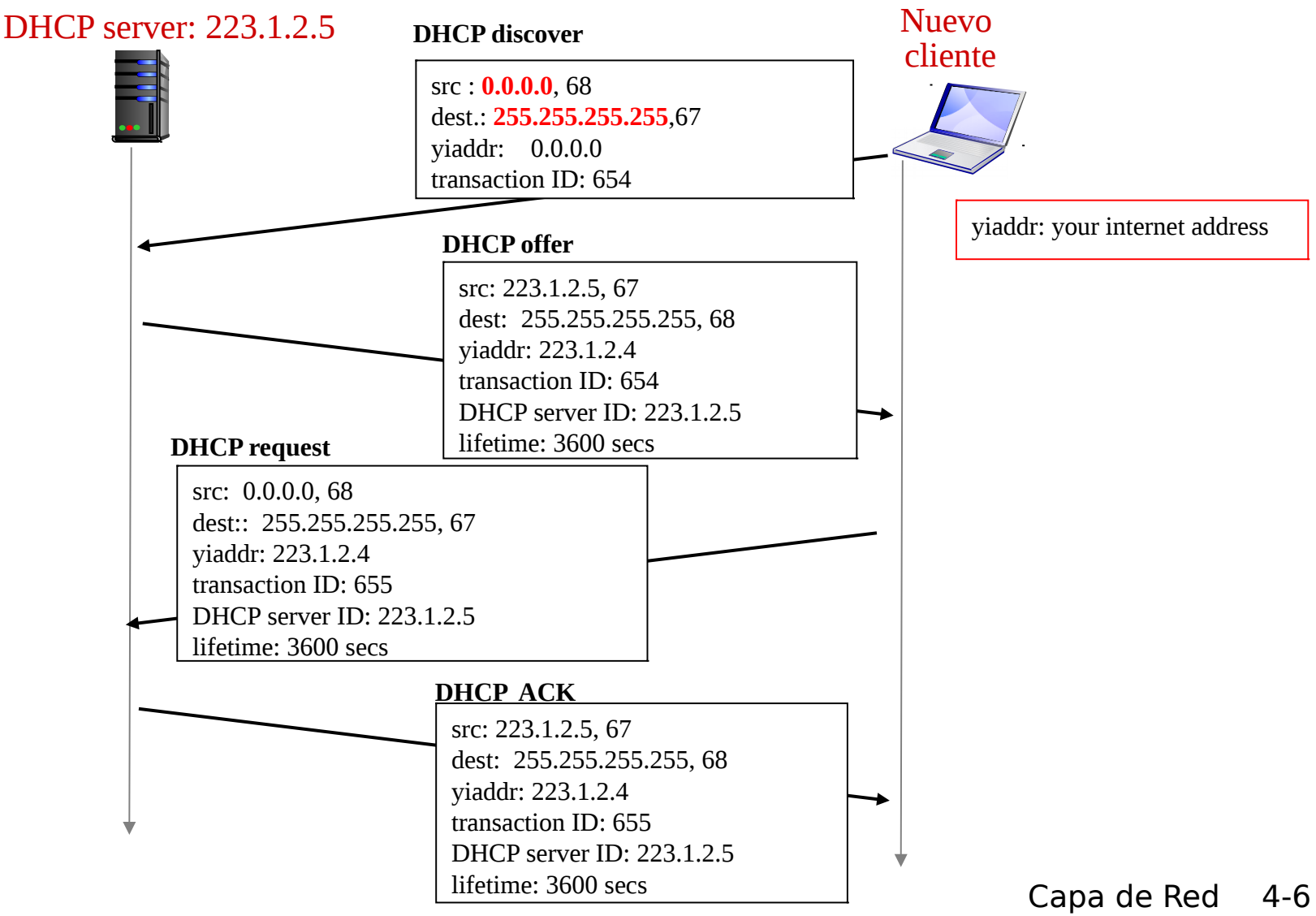
DHCP cómo funciona en general:

- host difunde (broadcasts) mensaje "DHCP discover"
- Servidor DHCP responde con mensaje "DHCP offer"
- Host pide una dirección IP mensaje: "DHCP request"
- Servidor DHCP envía mensaje con dirección: "DHCP ack"

Escenario cliente-servidor DHCP



Escenario cliente-servidor DHCP

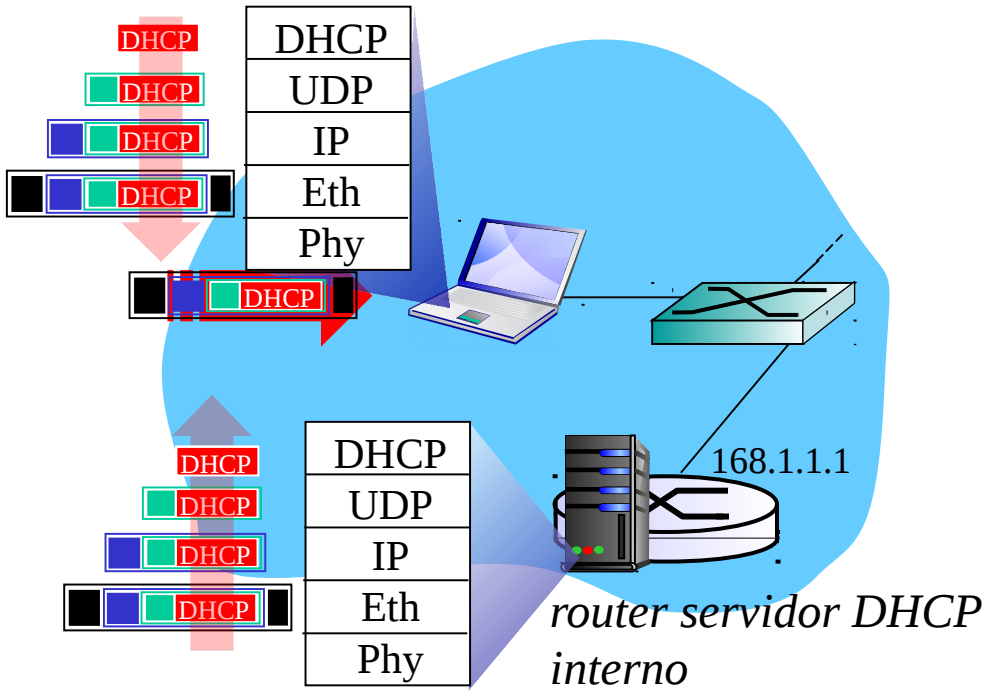


DHCP: más que direcciones IP

DHCP puede retornar además de la dirección IP:

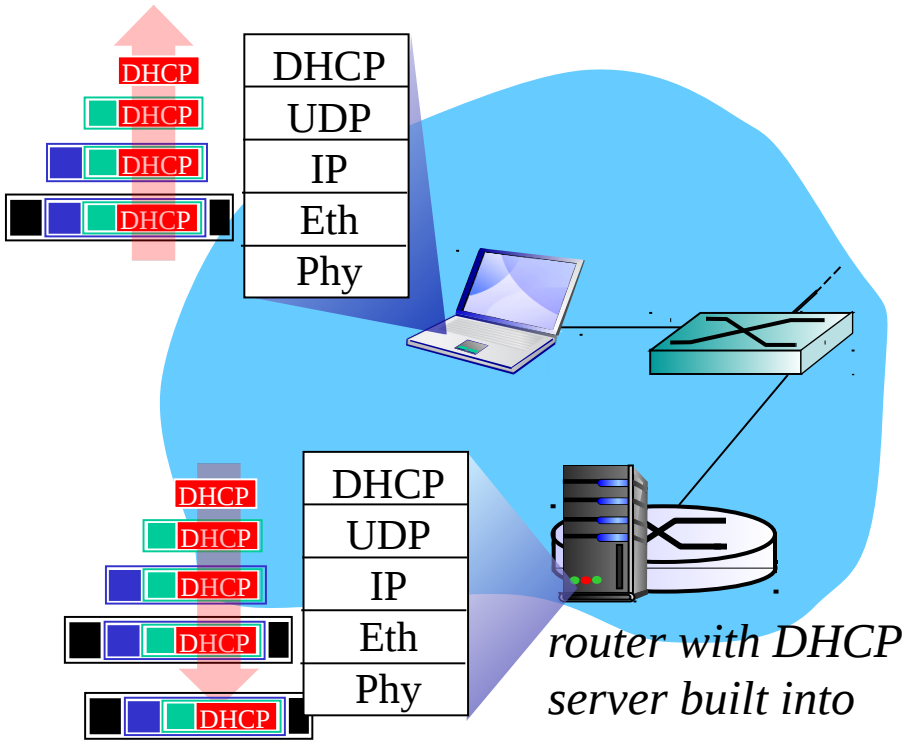
- Dirección del router de salida para ese cliente
- Nombre y dirección IP del servidor DNS
- Máscara de la subred (indicando la porción de la dirección de red de la porción de la dirección del host)

DHCP: ejemplo



- Notebook necesita dirección IP, dirección de router, dir de servidor DNS: usa DHCP
- Notebook envía requerimiento DHCP encapsulado en UDP, encapsulado en IP, encapsulado en Ethernet
- Trama Ethernet (dest: FFFFFFFFFFFF) en LAN es recibida en el router que corre el servidor DHCP
- Ethernet, IP, UDP demultiplexan trama DHCP

DHCP: ejemplo



- Servidor DHCP prepara mensaje DHCP ACK con la dirección IP del cliente, dirección IP del primer router para el cliente, nombre & dir IP del servidor DNS
- Servidor DHCP encapsula el mensaje DHCP ACK, trama es enviada al cliente, allí se demultiplexa y pasa al DHCP en cliente
- Cliente ahora conoce su dir IP, nombre y dir IP del servidor DNS local, dir IP del primer router para salir de la LAN.

DHCP: Wireshark output (home LAN)

request

Message type: **Boot Request (1)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) **DHCP Message Type = DHCP Request**
Option: (61) Client identifier
    Length: 7; Value: 010016D323688A;
    Hardware type: Ethernet
    Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
    Length: 11; Value: 010F03062C2E2F1F21F92B
    1 = Subnet Mask; 15 = Domain Name
    3 = Router; 6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    ……

reply

Message type: **Boot Reply (2)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
    Length: 12; Value: 445747E2445749F244574092;
    IP Address: 68.87.71.226;
    IP Address: 68.87.73.242;
    IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."

Esta lámina es referencial, no se requiere su estudio detallado

Direcciones IP: ¿Cómo obtener varias?

Q: ¿Cómo la red obtiene la dirección de subred? parte común más significativa de la dirección IP.

A: Obteniendo una porción del espacio de direcciones del proveedor ISP.

Ejemplo:

ISP's block	11001000 00010111 00010000	00000000	200.23.16.0/20
Organization 0	11001000 00010111 0001000**0**	00000000	200.23.16.0/23
Organization 1	11001000 00010111 0001001**0**	00000000	200.23.18.0/23
Organization 2	11001000 00010111 0001010**0**	00000000	200.23.20.0/23
...	.....	....	....
Organization 7	11001000 00010111 0001111**0**	00000000	200.23.30.0/23

También podrían haberse definido redes de distinto tamaño.

Direccionamiento IP: la última palabra...

Q: ¿Cómo un ISP obtiene un bloque de direcciones?

A: ICANN: Internet Corporation for Assigned Names and Numbers

- Asigna direcciones
- Administra DNS
- Asigna nombre de dominio, resuelve disputas

Para América Latina la oficina es LACNIC: http://lacnic.net/

Hay otras cuatro para otras regiones del mundo.

Agotamiento de Direcciones IP

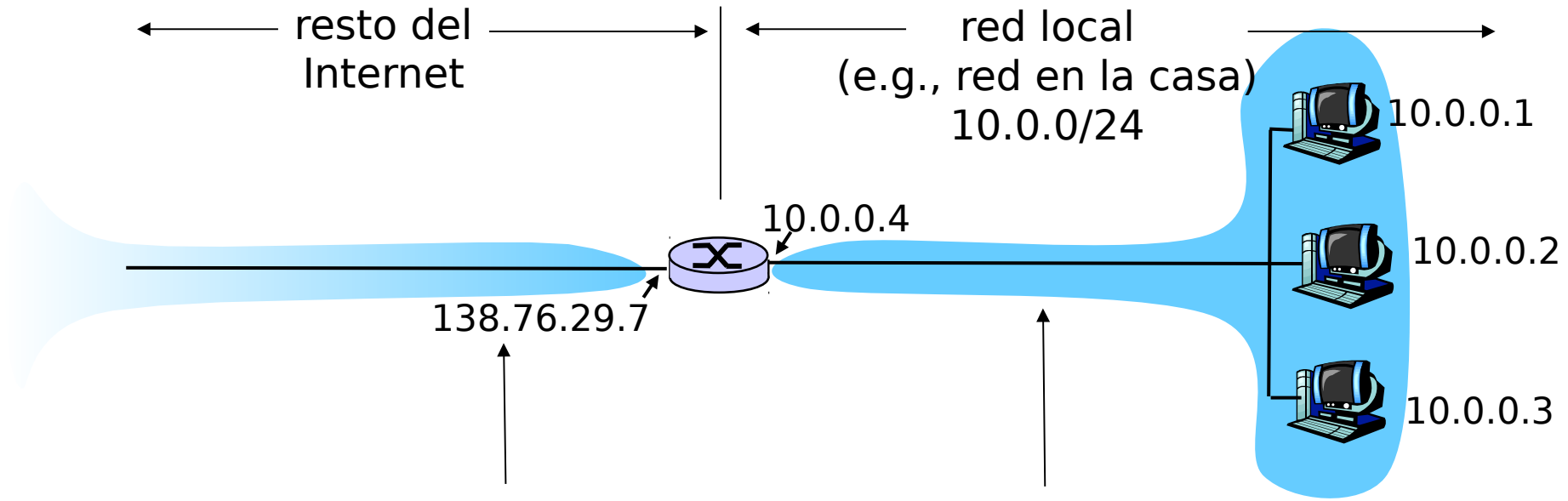
- Conforme más subredes se crearon y conectaron a Internet, las direcciones IP se comenzaron a agotar. Hoy 4 de las 5 regiones de mundo no tienen nuevas direcciones para asignar.
- Se desarrollaron dos estrategias para extender el uso de Ipv4:
  - Flexibilizar el tamaño de las subredes:surge Classless InterDomain Routing (CIDR) *.
  - Permitir acceso a Internet de redes privadas a través del uso de NAT (Network Address Translation)

(*) Antes el número de bits de la dirección de sub-red era 8 bits, Clase A; 16 bits, Clase B, ó 24 bits, Clase C.

NAT: Network Address Translation

- Motivación: ¿Cómo podemos dar salida a Internet a una red con direcciones privadas? Usamos un representante.
- La idea es usar sólo una dirección IP para acceder al mundo exterior:
  - No necesitamos asignación de un rango del ISP: sólo una dirección externa es usada por todos los equipos internos
  - Podemos cambiar la dirección de equipos en red local sin notificar al mundo exterior
  - Podemos cambiar ISP sin cambiar direcciones de equipos en red local
  - Equipos dentro de la red no son explícitamente direccionables o visibles desde afuera (una ventaja de seguridad).

NAT: Network Address Translation



Todos los datagramas *saliendo* de la red local tienen la misma dirección NAT IP: 138.76.29.7, pero diferentes números de puerto

Datagramas con fuente o destino en esta red tienen direcciones 10.0.0/24
(También se puede usar: 192.168.0/24 ó 172.16.0/24)

NAT: Network Address Translation

Implementación ruteador NAT:

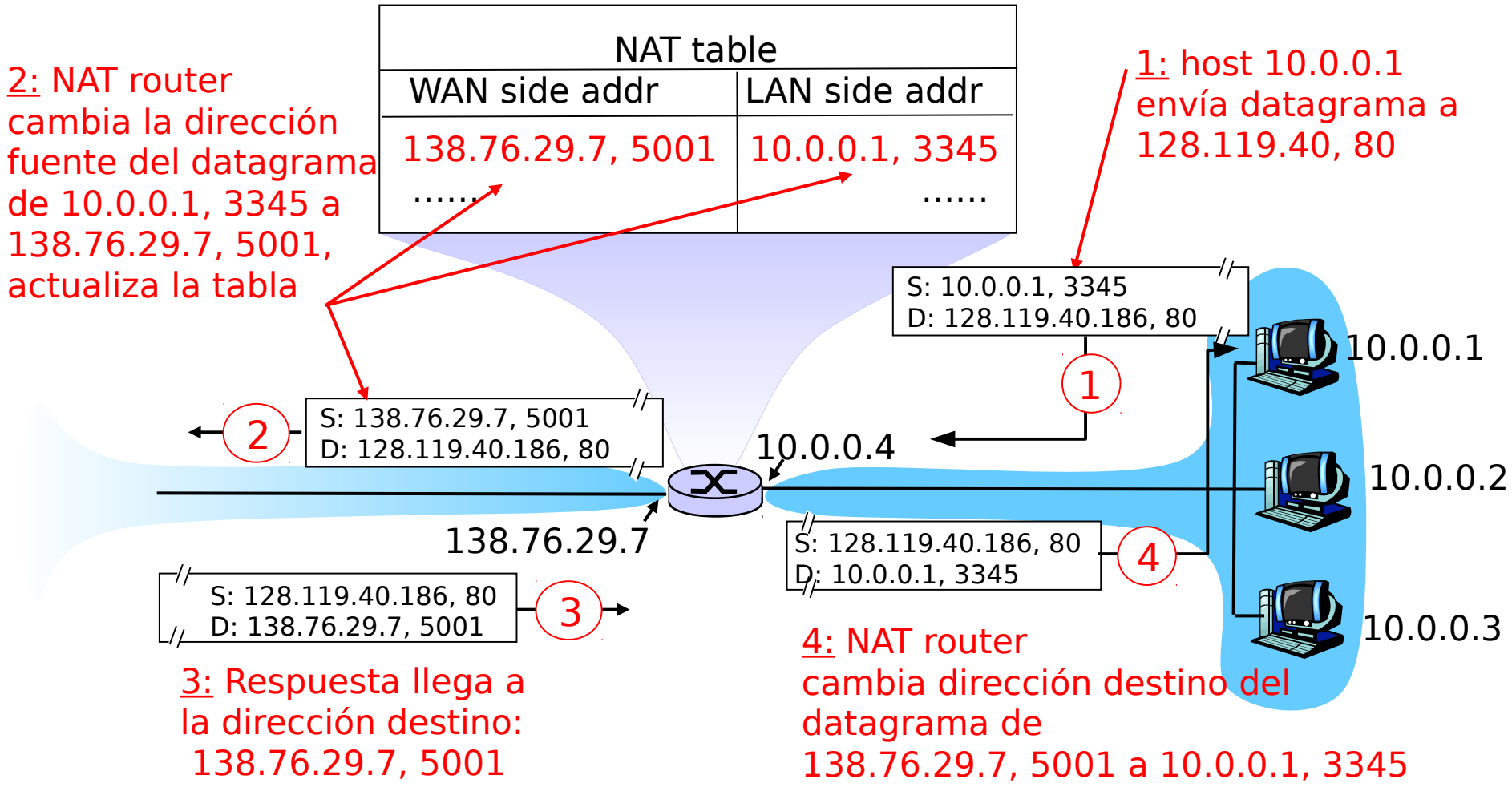
- Para Datagramas salientes: remplazar (IP fuente, # puerto) de cada datagrama saliente por (IP NAT, nuevo # puerto)

  . . . Clientes y servidores remotos responderán usando (IP NAT, nuevo # puerto) como dirección destino.

- Recordar (en tabla de traducción NAT) cada par de traducción (IP fuente, # puerto) a (IP NAT, nuevo # puerto)

- Para Datagramas entrantes: remplazar (IP NAT, nuevo # puerto) en campo destino de cada datagrama entrante por correspondiente (IP fuente, # puerto) almacenado en tabla NAT

NAT: Network Address Translation



NAT: Network Address Translation

- Campo número de puerto es de 16 bits:
  - Máx. ~65,000 conexiones simultáneas pueden salir con sólo una dirección IP válida en Internet!
- NAT es controversial:
  - Routers deberían procesar sólo hasta capa 3
  - Viola argumento extremo-a-extremo
    - Los NAT deben ser tomados en cuenta por los diseñadores de aplicaciones, eg, aplicaciones P2P
  - En lugar de usar NAT, la carencia de direcciones debería ser resuelta por IPv6
- Si Ud. tiene una máquina detrás de un NAT, ésta puede ser visible usando UPnP (Universal Plug and Play). Importante: hay formas de entrar.

La red wifi de la USM usa direcciones IP privadas ¿Qué hace posible que usted pueda acceder a Internet? ¿Puede usted instalar un servidor (web por ejemplo) conectado a esta red inalámbrica? ¿Sería accesible desde la misma red wifi? ¿Sería accesible desde Internet?

?

- La presencia de un NAT. Sí. Sí. No. Nota: Lo último puede ser Sí indicando el uso de “port forwarding en el NAT (tema no cubierto en el ramo, pero puede ser de su conocimiento)

Un alumno se conecta vía ssh desde la red con NAT en su casa a un servidor en la Universidad. Si deja su conexión inactiva por un largo rato, al volver detecta que está caída. Explique cómo el servidor NAT puede causar tal pérdida de conexión. ?

- El servidor NAT mantiene una tabla con los puertos que han sido asignados a flujos provenientes de la red privada. Si no hay actividad luego de un rato, este puerto es liberado para ser asignado a otros flujos de datos. En este caso la conexión ssh ya no funciona porque el puerto asignado en el NAT ya no pertenece a esa conexión.

- En un “cyber café” todos los usuarios navegan en Internet y salen a través de un único NAT. Analizando el tráfico que sale del “cyber café” hacia Internet ¿cómo podría usted estimar cuántos clientes están usando su red? Se sabe que la capa IP de cada computador usa números de identificación secuenciales en cada datagrama saliente.

- Basta con observar cuántas secuencias de números de identificación están saliendo. El número de secuencias indicará el número de capas IP enviando paquetes y será el número de clientes del cyber café.

Capítulo 4: Capa de Red

- 4. 1 Introducción
- 4.2 Circuitos virtuales y redes de datagramas
- 4.3 ¿Qué hay dentro de un router?
- 4.4 IP: Internet Protocol
  - Formato de Datagrama
  - Direccionamiento IPv4
  - ICMP
  - IPv6
- 4.5 Algoritmo de ruteo
  - Estado de enlace
  - Vector de Distancias
  - Ruteo Jerárquico
- 4.6 Ruteo en la Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Ruteo Broadcast y multicast

ICMP: Internet Control Message Protocol

- Usado por hosts & routers para comunicar información a nivel de la red
  - Reporte de errores: host inalcanzable, o red, o puerto, o protocolo
  - Echo request/reply (usado por ping)
  - Usado por traceroute (TTL expired, dest port unreachable)
- Opera en capa transporte:
  - ICMP son llevados por datagramas IP
- Mensajes ICMP: tipo y código de error, más primeros 8 bytes del datagrama que causó el error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - seldom used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Traceroute e ICMP

- La fuente envía una serie de segmentos UDP al destino
  - Primero usa TTL=1
  - Luego usa TTL=2, etc.
  - Número de puerto (probablemente) no usado en destino
- Cuando el n-ésimo datagrama llega a n-ésimo router:
  - Router descarta el datagrama, y
  - Envía a la fuente un mensaje ICMP "TTL expirado" (tipo 11, código 0)
  - Mensaje incluye nombre del router y dirección IP
- Cuando mensaje ICMP llega, la fuente calcula el RTT
- Traceroute hace esto 3 veces

Criterio de parada

- Segmento UDP eventualmente llega al host destino
- Host destino retorna paquete ICMP "puerto inalcanzable" (tipo 3, código 3)
- Cuando la fuente recibe este ICMP, para.

Capítulo 4: Capa de Red

- 4. 1 Introducción
- 4.2 Circuitos virtuales y redes de datagramas
- 4.3 ¿Qué hay dentro de un router?
- 4.4 IP: Internet Protocol
  - Formato de Datagrama
  - Fragmentación
  - Direccionamiento IPv4
  - NAT (Network Address Translation)
  - ICMP
  - IPv6
- 4.5 Algoritmo de ruteo
  - Estado de enlace
  - Vector de Distancias
  - Ruteo Jerárquico
- 4.6 Ruteo en la Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Ruteo Broadcast y multicast

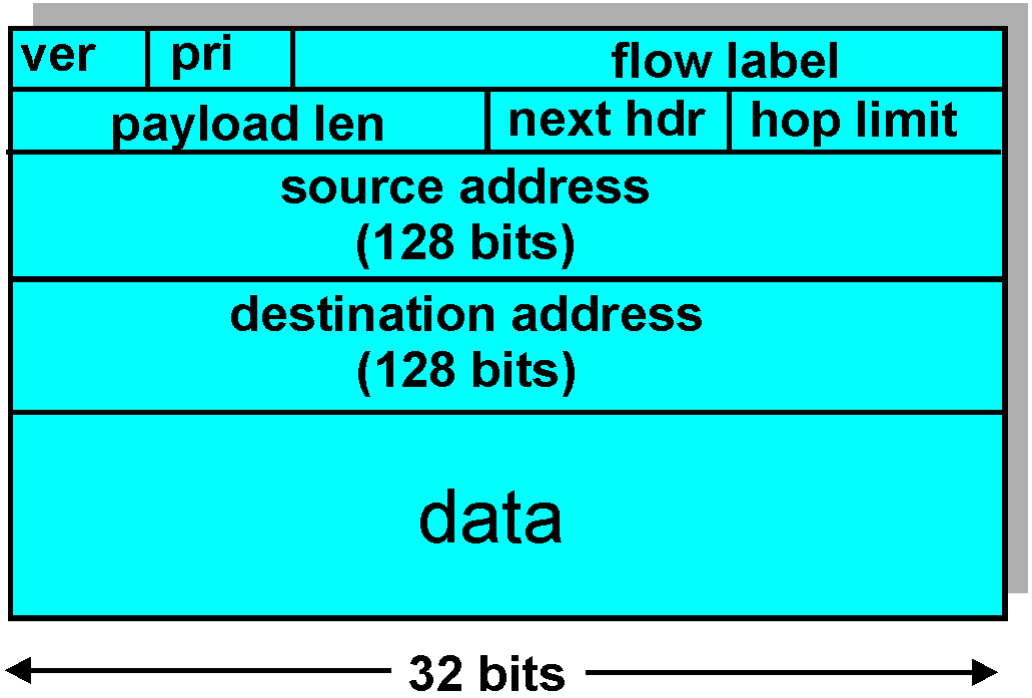
IPv6

- Motivación Inicial: espacio de direcciones de 32-bit pronto serán completamente asignadas.
- Motivación adicional:
  - Formato de encabezado debería ayudar a acelerar el procesamiento y re-envío (por aumento de tasas en red)
  - Cambiar encabezado para facilitar QoS (Quality of Service)

  Formato de datagrama IPv6:
  - Encabezado de largo fijo de 40 bytes (se duplicó)
  - Fragmentación no es permitida

Encabezado IPv6

- *Prioridad (8bits):* identifica prioridad entre datagramas en flujo
- *Flow Label:* identifica datagramas del mismo "flujo." (concepto de "flujo" no está bien definido).
- *Next header:* identifica protocolo de capa superior de los datos



Otros cambios de IPv4 a v6

- *Checksum*: eliminada enteramente para reducir tiempo de procesamiento en cada router al ser redundante, ya está en capa transporte y enlace (Ethernet)
- *Options:* permitidas, pero fuera del encabezado, indicado por campo “Next Header”
- *ICMPv6:* nueva versión de ICMP
  - Tipos de mensajes adicionales, e.g. “Paquete muy grande” (usado en el descubrimiento de MTU: unidad máxima de transmisión)
  - Funciones para administrar grupos multicast

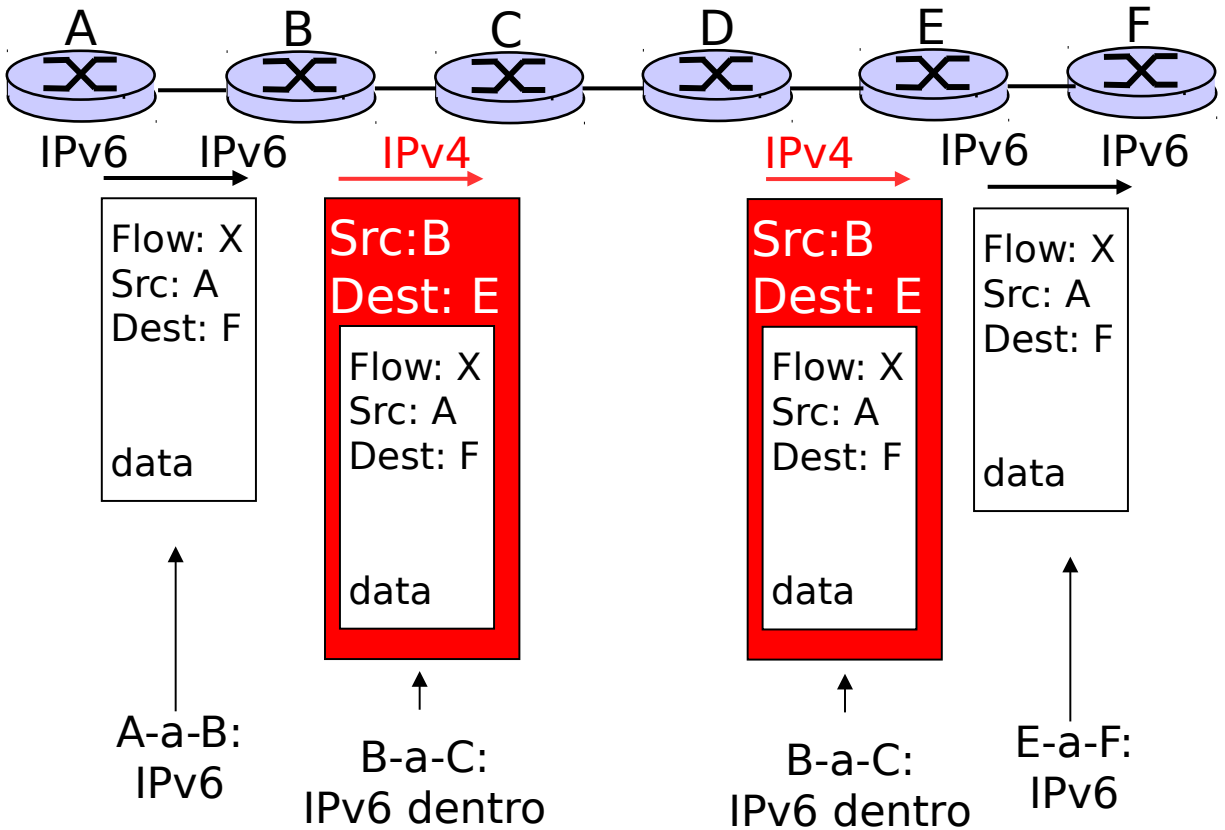
Transición de IPv4 a IPv6

- No todos los routers pueden ser actualizados (upgraded) simultáneamente
  - No es posible definir un día para cambio “día de bajada de bandera”
  - ¿Cómo operará la red con routers IPv4 e IPv6 mezclados?
- *“Tunneling”:* IPv6 es llevado como carga en datagramas IPv4 entre routers IPv4

Tunneling

Vista lógica:

Vista física:



- ¿Por qué el protocolo IPv6 decidió eliminar el campo de suma de chequeo que sí tiene IPv4?

- Porque así cada paquete puede ser procesado más rápidamente al no requerir recalcular una suma de chequeo cada vez que el “hop limit” cambiaba.

Capítulo 4: Capa de Red

- 4. 1 Introducción
- 4.2 Circuitos virtuales y redes de datagramas
- 4.3 ¿Qué hay dentro de un router?
- 4.4 IP: Internet Protocol
  - Formato de Datagrama
  - Fragmentación
  - Direccionamiento IPv4
  - NAT (Network Address Translation)
  - ICMP
  - IPv6
- 4.5 Algoritmos de ruteo
  - Estado de enlace
  - Vector de Distancias
  - Ruteo Jerárquico
- 4.6 Ruteo en la Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Ruteo Broadcast y multicast