



INTERNETWORKING

Karima Velásquez

karima.velasquez@ciens.ucv.ve



Agenda

- ◉ Internetwork
- ◉ IP
- ◉ ARP
- ◉ DHCP
- ◉ Subnetting y Supernetting
- ◉ IPv6
- ◉ Enrutamiento

Conectando redes: Problemas

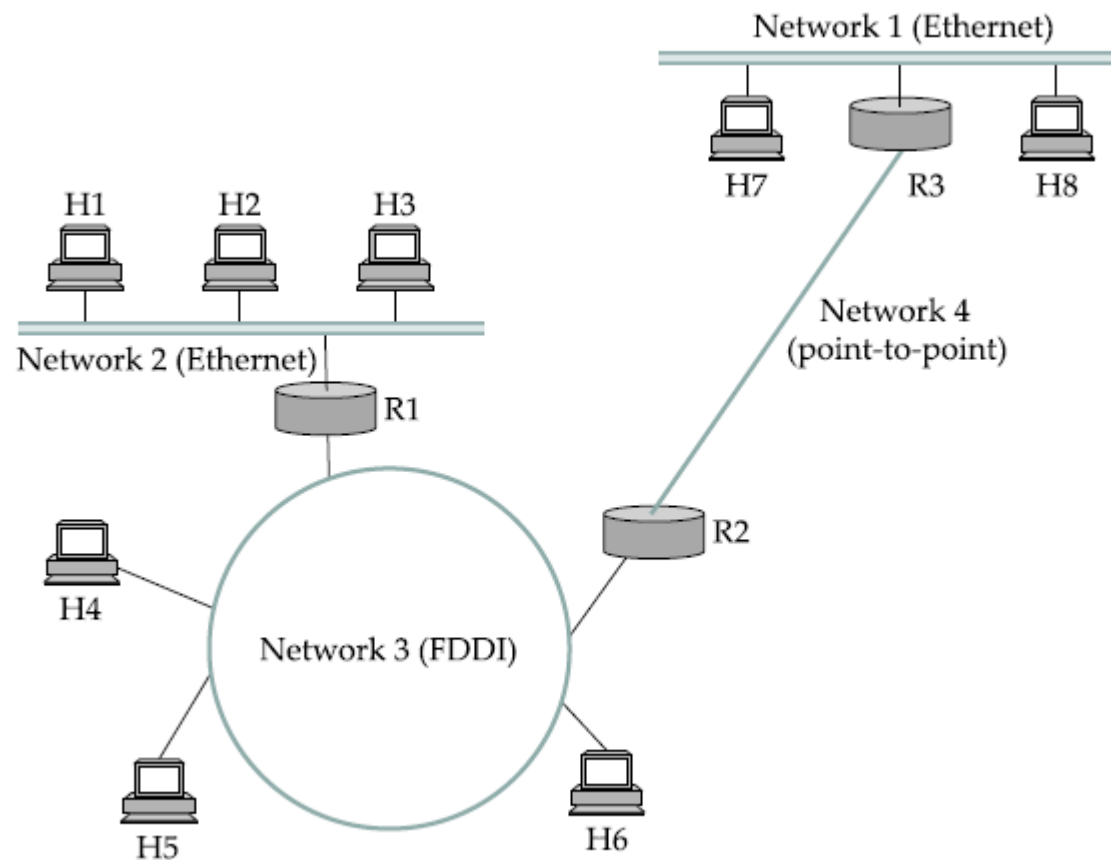
- Heterogeneidad
- Escalabilidad



INTERNETWORK

- Se usa el término *internetwork* o *internet* para referirse a una colección de redes interconectadas para proporcionar un servicio de entrega de paquetes de host-a-host.
- Una *internetwork* también se ver como una colección de redes interconectadas.

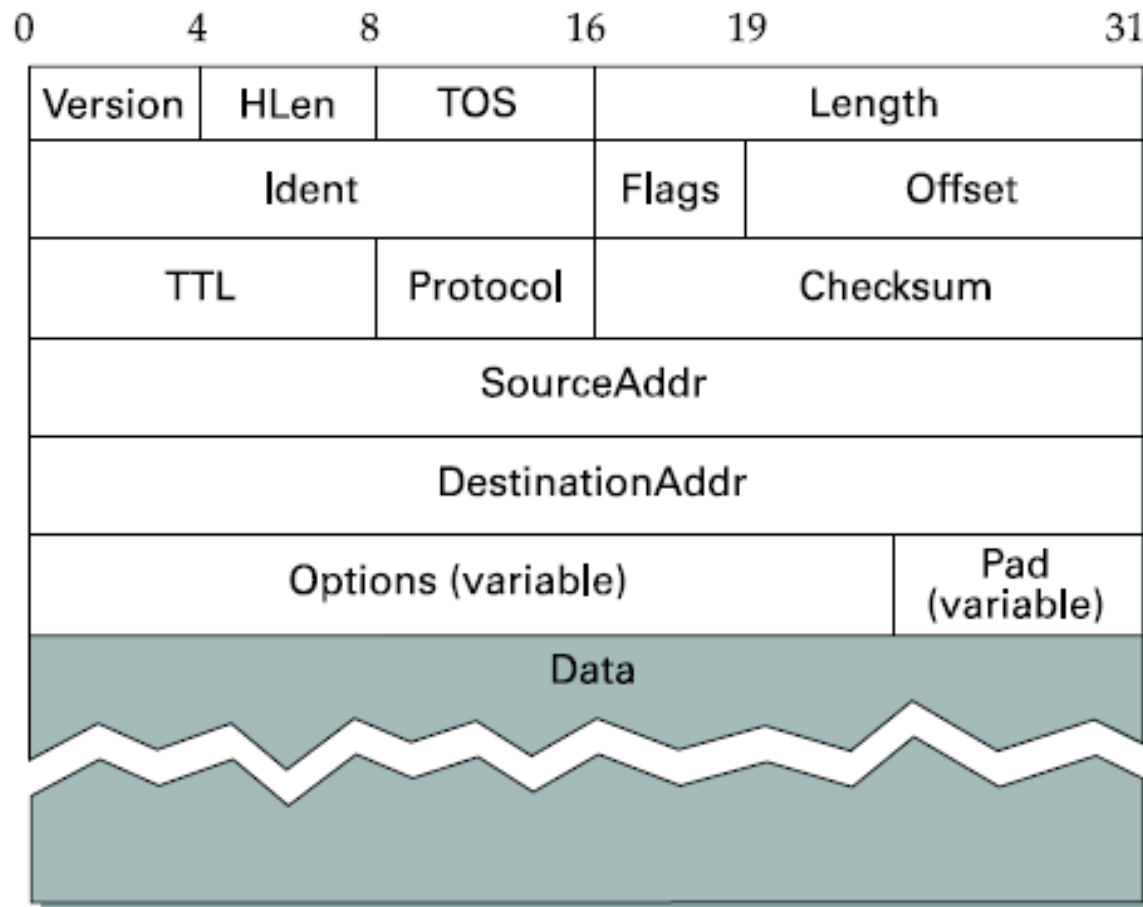
INTERNETWORK: EJEMPLO



INTERNETWORKING: IP

- Modelo de Servicio:
 - Direccionamiento
 - Entrega de paquetes: datagrama
 - Entrega basada en mejor esfuerzo:
 - Si el paquete se pierde, se daña, es entregado erróneamente, falla en llegar a su destino, la “red “no hace nada”
 - Se dice que IP es capaz de correr sobre “cualquier cosa”.

IP: FORMATO DEL PAQUETE



IP: FORMATO DEL PAQUETE

Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 519

Identification: 0x0f45 (3909)

Flags: 0x02 (Don't Fragment)

0.. = Reserved bit: Not Set

.1. = Don't fragment: Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 128

Protocol: TCP (0x06)

Header checksum: 0x9010 [correct]

[Good: True]

[Bad : False]

Source: 145.254.160.237 (145.254.160.237)

Destination: 65.208.228.223 (65.208.228.223)

IP: FORMATO DEL PAQUETE

- Versión (VER): versión del protocolo IP. Actualmente, la versión 4.
- Longitud de la cabecera (HLEN): la longitud total de la cabecera de datagrama en palabras de 4 bytes.
- Servicios: tipo de servicio o servicios diferenciados.
- Longitud total: longitud total (encabezado más datos) del datagrama en bytes.
 - Longitud total de la data = longitud total - longitud de la cabecera

IP: FORMATO DEL PAQUETE

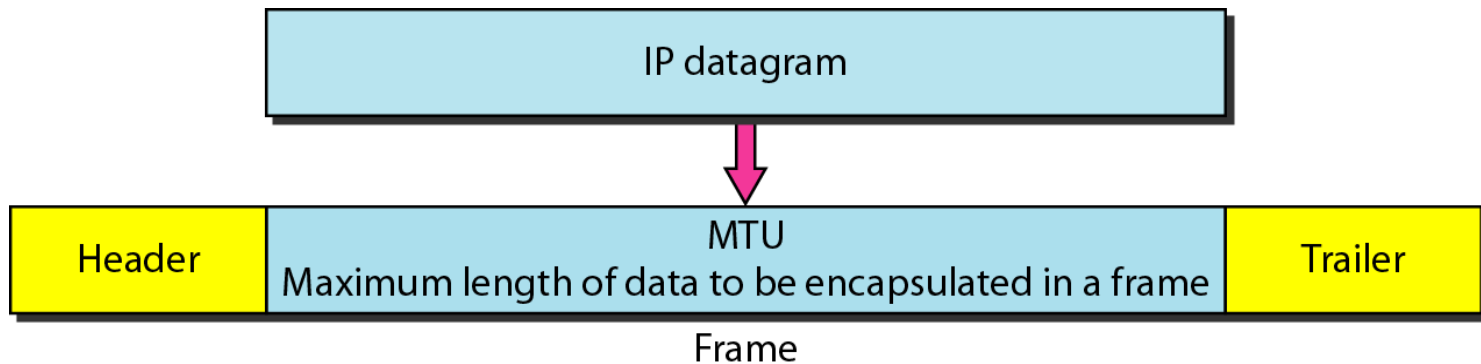
- Identificación: se utiliza en la fragmentación (explicado más adelante).
- Banderas: utilizado en la fragmentación (explicado más adelante).
- La fragmentación offset: utilizado en la fragmentación (explicado más adelante).
- Tiempo de vida: en la actualidad se utiliza para controlar el número máximo de saltos visitados por el datagrama.
- Protocolo: define el protocolo de nivel superior que utiliza los servicios de la capa de IPV4.

IP: FORMATO DEL PAQUETE

- ◉ Checksum: usado en la detección de errores.
- ◉ Dirección de origen: es la dirección IPv4 de la fuente.
- ◉ Dirección de destino: es la dirección IPv4 de la fuente.

IP: FRAGMENTACION Y REESAMBLADO

MAXIMUM TRANSFER UNIT (MTU)



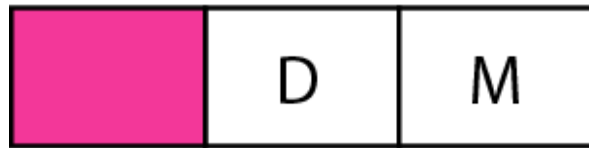
IP: FRAGMENTACION Y REESAMBLADO

<i>Protocol</i>	<i>MTU</i>
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

IP: FRAGMENTACION Y REESAMBLADO

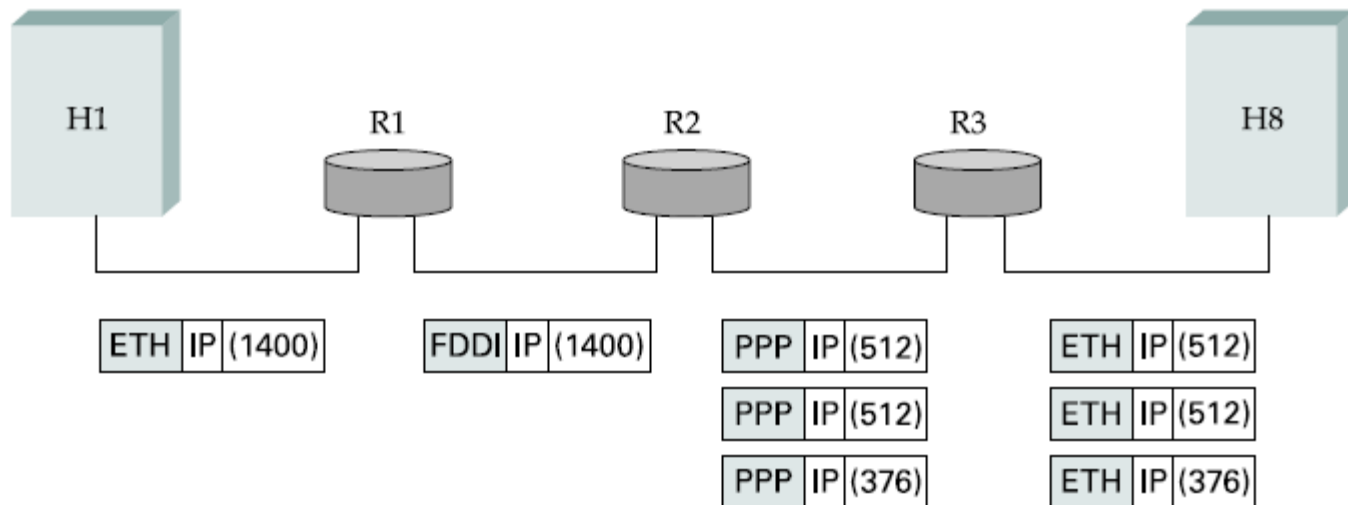
- Identificación: identifica un datagrama procedente del host de origen.
 - Una combinación de la identificación y la dirección de origen únicamente debe definir un datagrama.
- Banderas: vea la siguiente diapositiva.
- Fragmentación offset: es el desplazamiento de los datos en el datagrama original y se mide en unidades de 8 bytes.

IP: FRAGMENTACION Y REESAMBLADO



D: Do not fragment
M: More fragments

IP: FRAGMENTACION Y REESAMBLADO



IP: FRAGMENTACION Y REESAMBLADO

(a)

Start of header				
Ident = x			0	Offset = 0
Rest of header				
1400 data bytes				

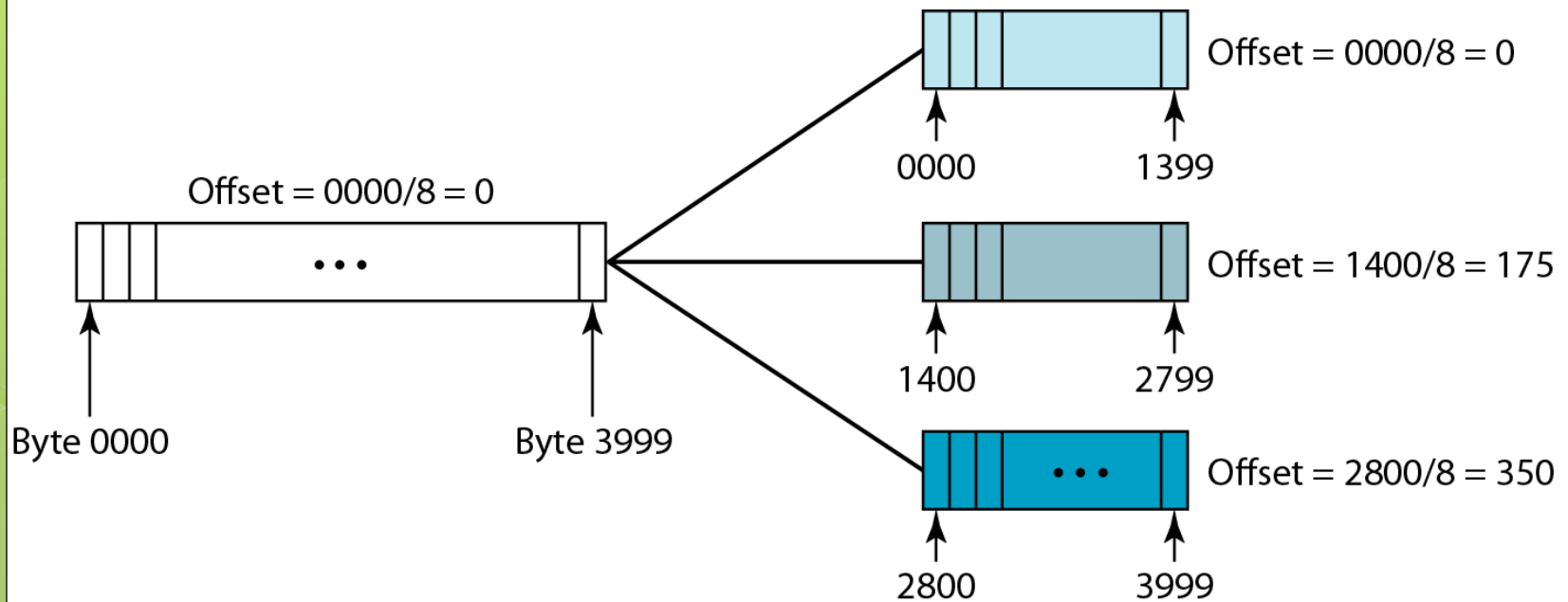
(b)

Start of header				
Ident = x			1	Offset = 0
Rest of header				
512 data bytes				

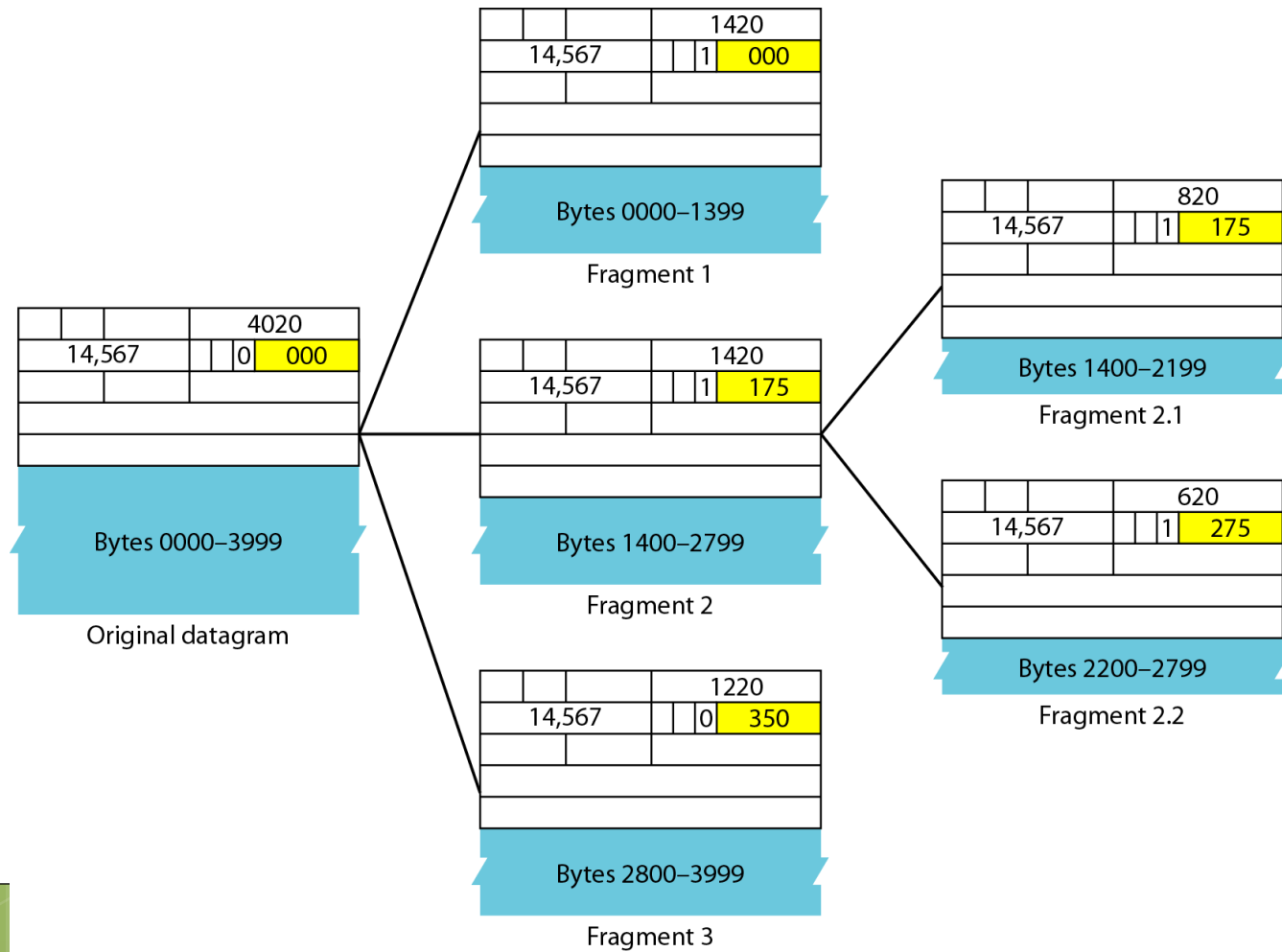
Start of header				
Ident = x			1	Offset = 64
Rest of header				
512 data bytes				

Start of header				
Ident = x			0	Offset = 128
Rest of header				
376 data bytes				

IP: FRAGMENTACION Y REESAMBLADO



IP: FRAGMENTACION Y REESAMBLADO



IP: FRAGMENTACION Y REESAMBLADO

- [CapturaFragmentacion.pcap](#)

CAPTURA DE PAQUETES DE
LONGITUD 5000 BYTES
FRAGMENTADOS

IP: FRAGMENTACION Y REESAMBLADO: EJERCICIO

- Suponga que el host A está conectado a un router R1, R1 está conectado a otro router R2, y R2 está conectado al host B. Suponga que un mensaje TCP que contiene 920 bytes (incluyendo el encabezado TCP) se pasa al código IP del Host A para ser enviado a B. Muestre los valores de los campos de Longitud total, ID, DF, MF y desplazamiento de los paquetes IP enviados sobre los 3 enlaces. Asuma que el enlace A-R1 puede soportar un MTU de 1024 bytes, el enlace R1-R2 puede soportar un MTU de 512 bytes, y el enlace R2-B puede soportar un MTU de 500 bytes. Asuma que las opciones IP no son usadas.

IP: DIRECCIONES

- En el esquema de direccionamiento basado en clases (*classful*), el espacio de direcciones se divide en : A, B, C, D, y E.

IP: DIRECCIONES

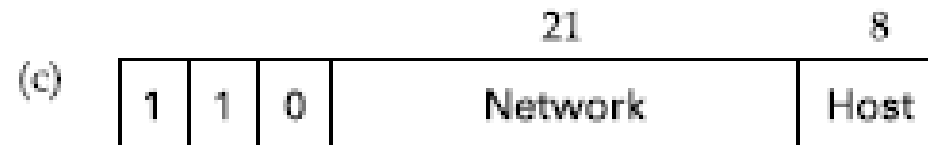
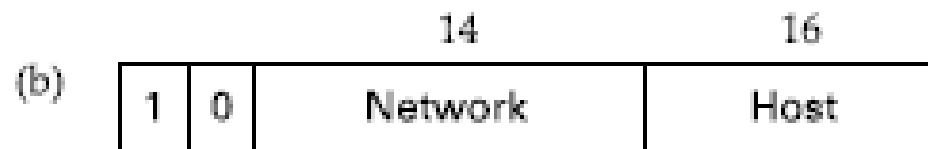
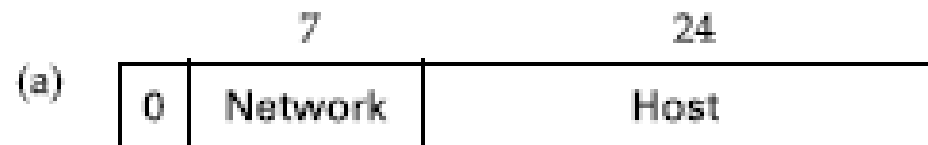
	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

IP: DIRECCIONES



IP: FORWARDING

- *Forwarding* es el proceso de tomar un paquete desde una entrada y enviarlo por la salida apropiada.
- *Enrutamiento*: es el proceso de construir tablas que permiten determinar por donde debe ser enviado un paquete.

IP: FORWARDING

- Cada datagrama contiene la dirección IP del host de destino.
- La parte de red de una dir IP identifica unívocamente una simple red física que es parte de la Internet.
- Todos los hosts y enrutadores que comparten la misma parte de red de su dirección están conectados y se pueden comunicar enviando tramas sobre la red.
- Cada red física que es parte de la internet tiene al menos un enrutador que por defecto esta también conectado a al menos un enlace físico; este enrutador puede intercambiar paquetes por a cada enlace físico.

IP: FORWARDING

if (NetworkNum of destination = NetworkNum of one of my interfaces) then

 deliver packet to destination over that interface

else

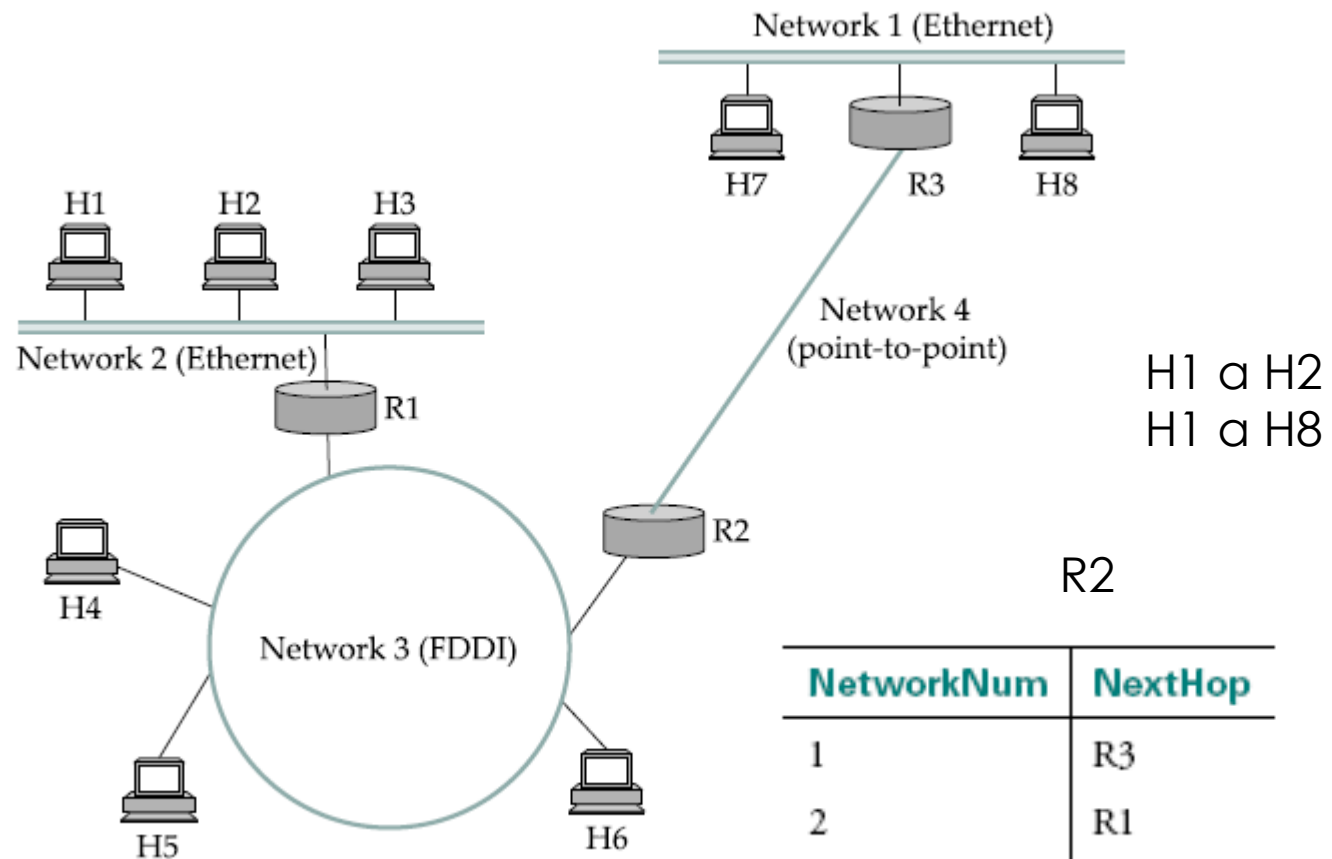
 if (NetworkNum of destination is in my forwarding table) then

 deliver packet to NextHop route

 else

 deliver packet to default router

IP FORWARDING



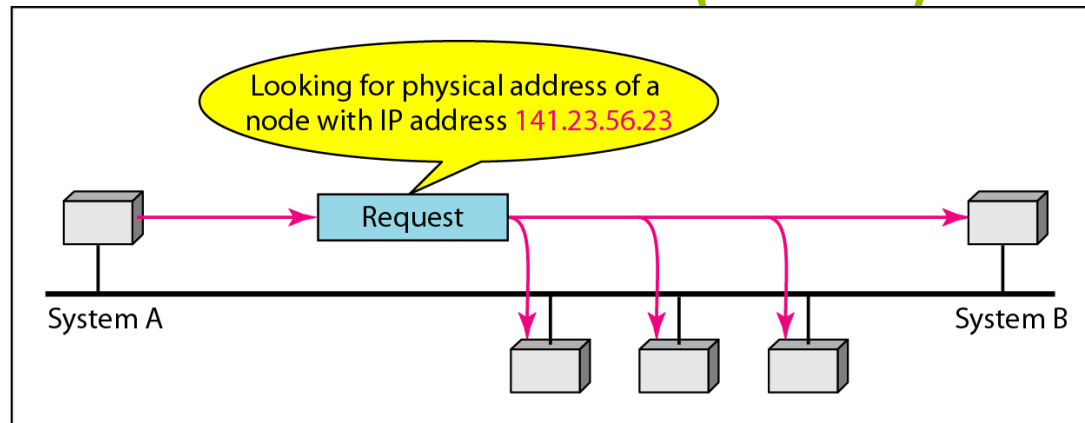
R2

NetworkNum	NextHop
1	R3
2	R1
3	Interface 1
4	Interface 0

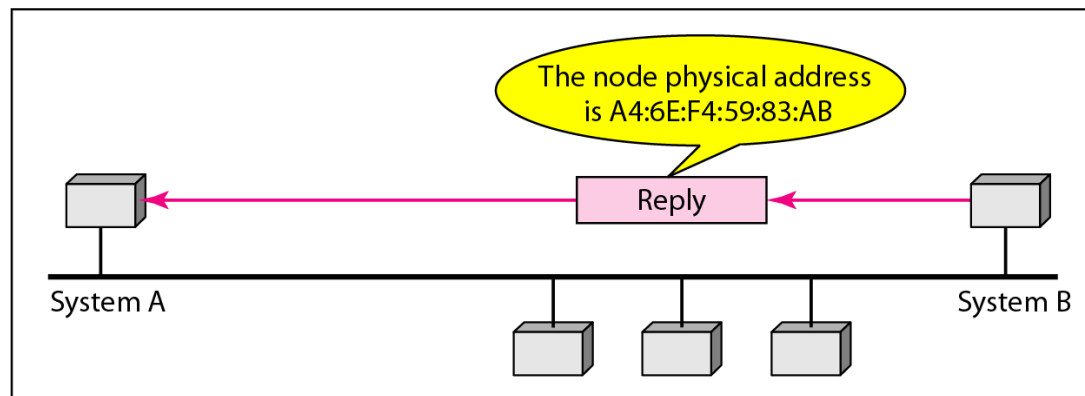
Mapeo de Direcciones

- El envío de paquetes a un host o a un enrutador requiere de direcciones:
 - Lógicas
 - Físicas
- Se requiere mapear direcciones lógicas a físicas y viceversas.
- Esto se puede hacer de forma estática o dinámica.

Operación de Address Resolution Protocol (ARP)



a. ARP request is broadcast

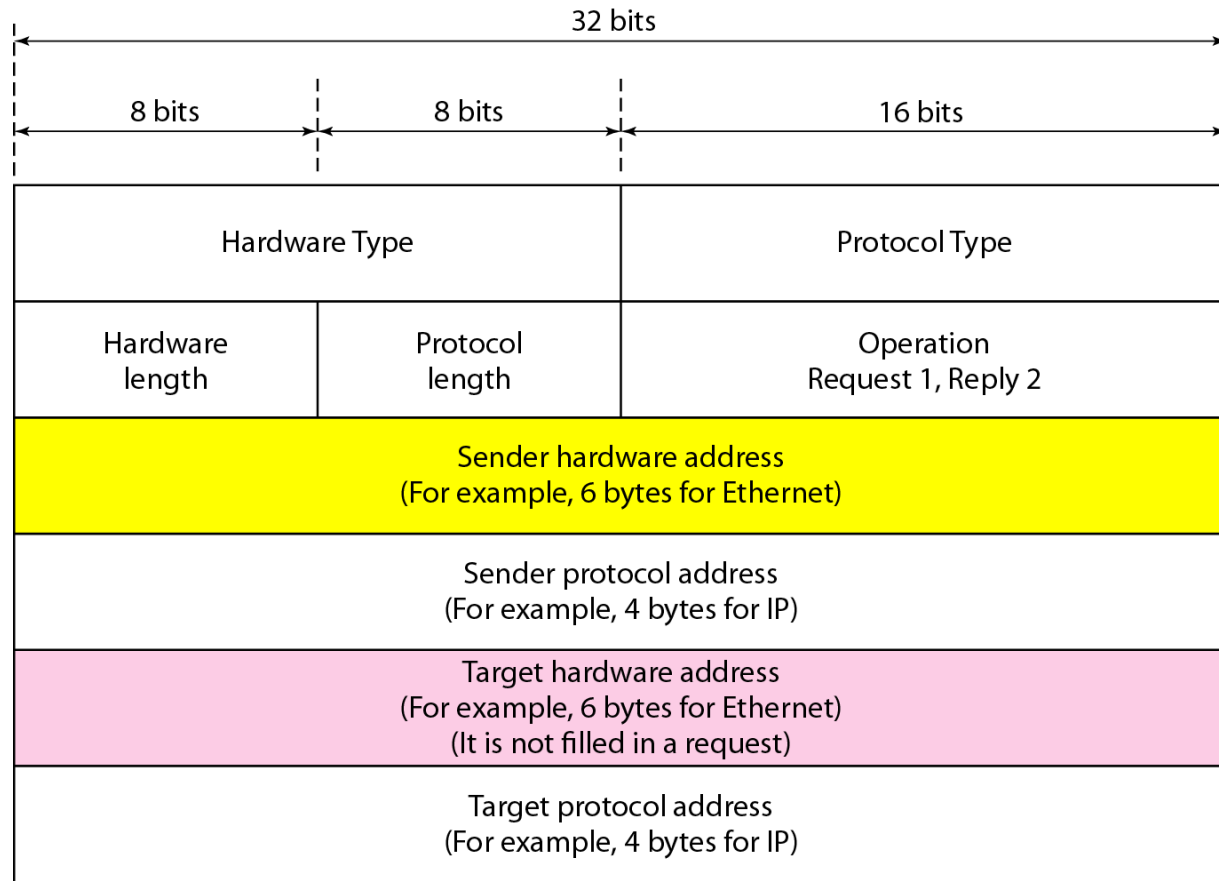


b. ARP reply is unicast

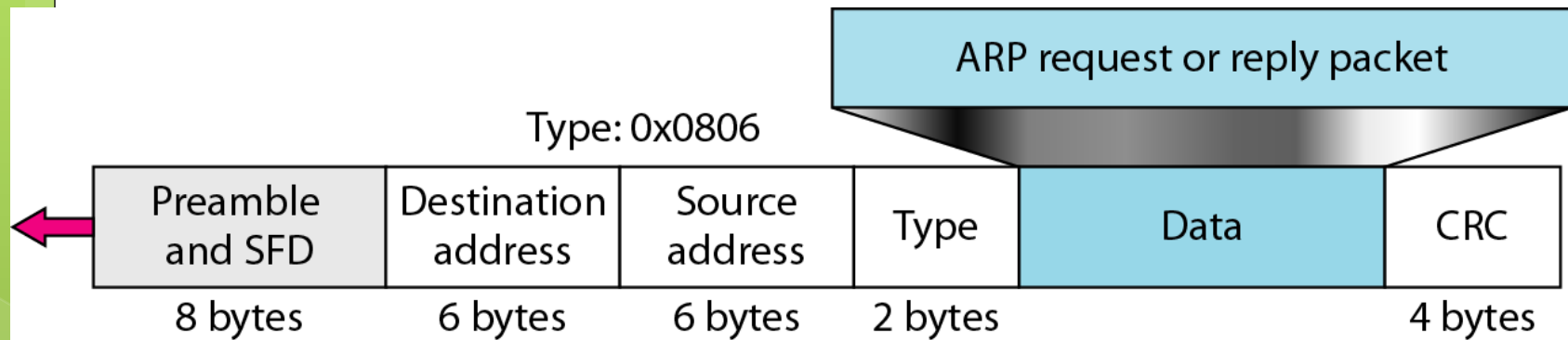
Address Resolution Protocol (ARP)

- El *ARP reply* is guardado en cache por un tiempo.

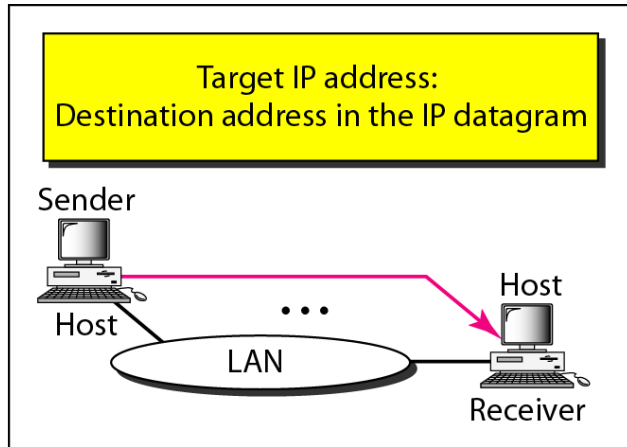
Paquete ARP



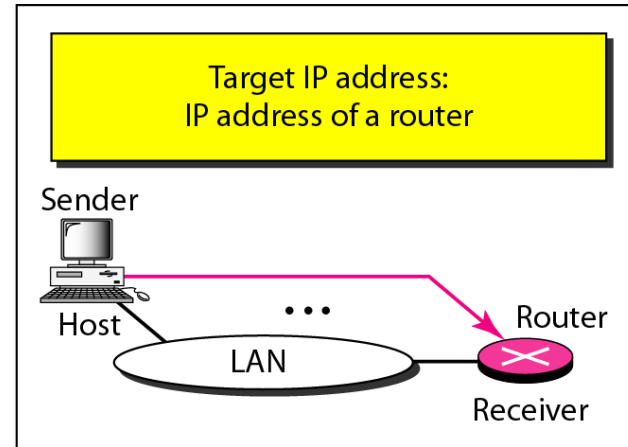
Encapsulamiento de Paquetes ARP



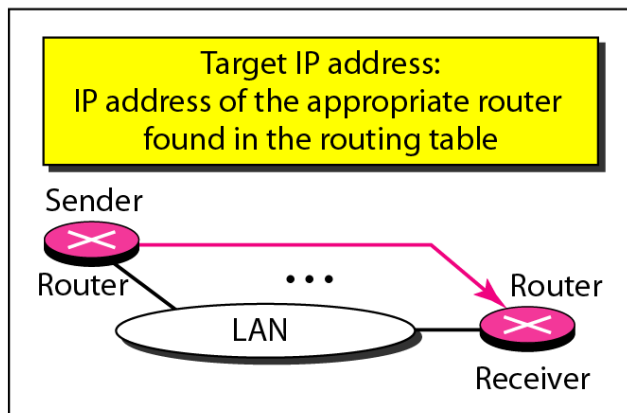
Cuatro casos usando ARP



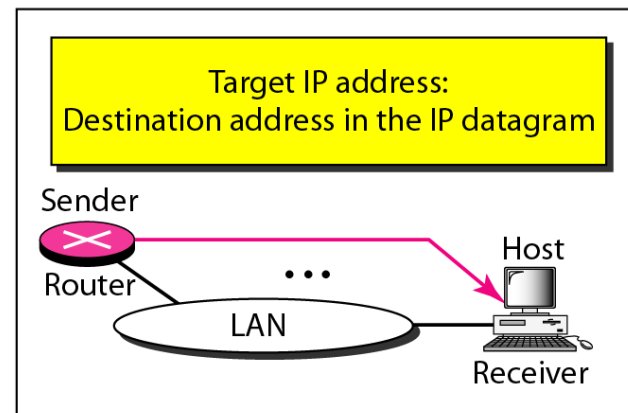
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.



Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



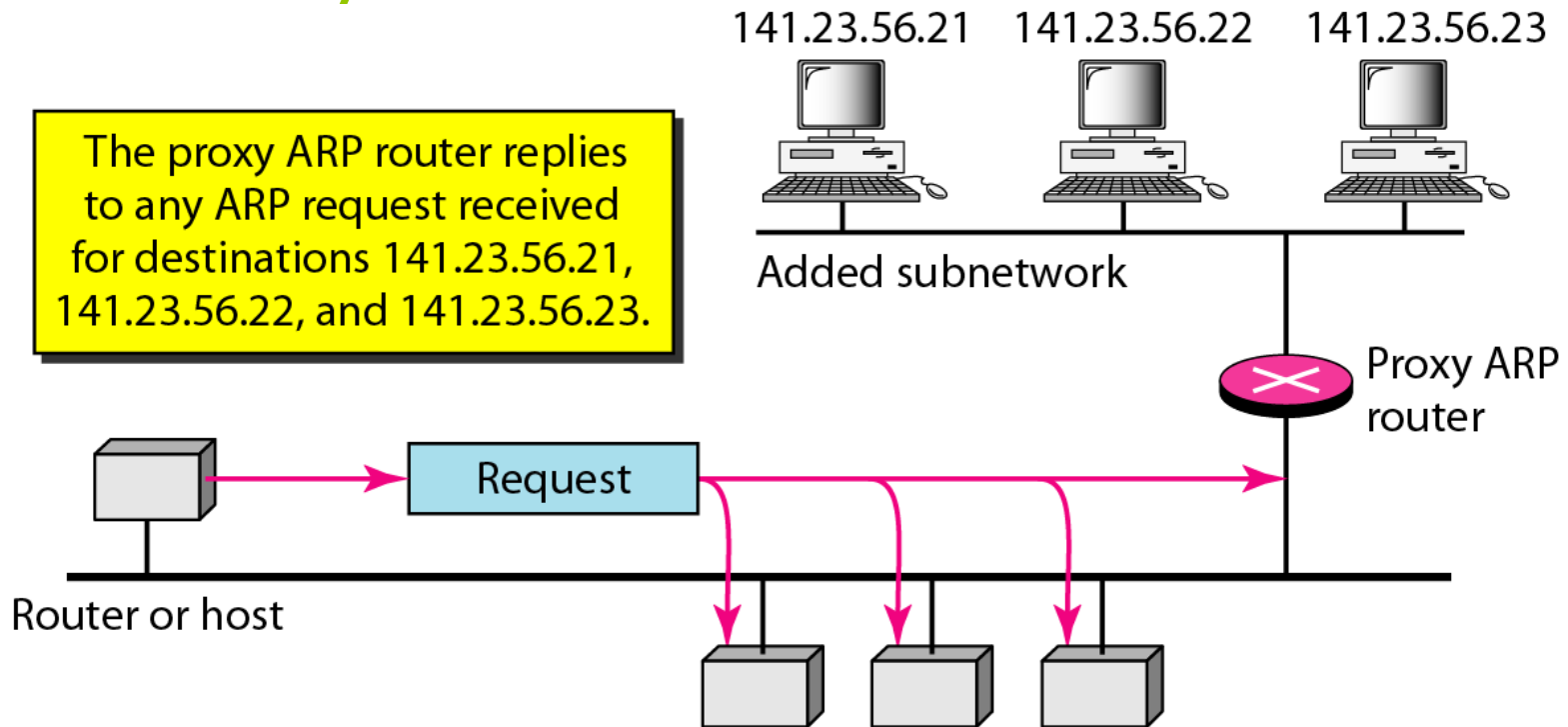
Case 4. A router receives a packet to be sent to a host on the same network.

ARP

- Un *ARP request* es broadcast.
- Un *ARP reply* es unicast

Proxy ARP

The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.



ARP

```
C:\Windows\system32\cmd.exe

224.0.0.252      01-00-5e-00-00-fc      static
224.0.0.253      01-00-5e-00-00-fd      static
239.255.255.250  01-00-5e-7f-ff-fa      static
255.255.255.255  ff-ff-ff-ff-ff-ff      static

C:\Users\Maria Elena>arp d

C:\Users\Maria Elena>arp -d
The ARP entry deletion failed: The requested operation requires elevation.

C:\Users\Maria Elena>arp -a

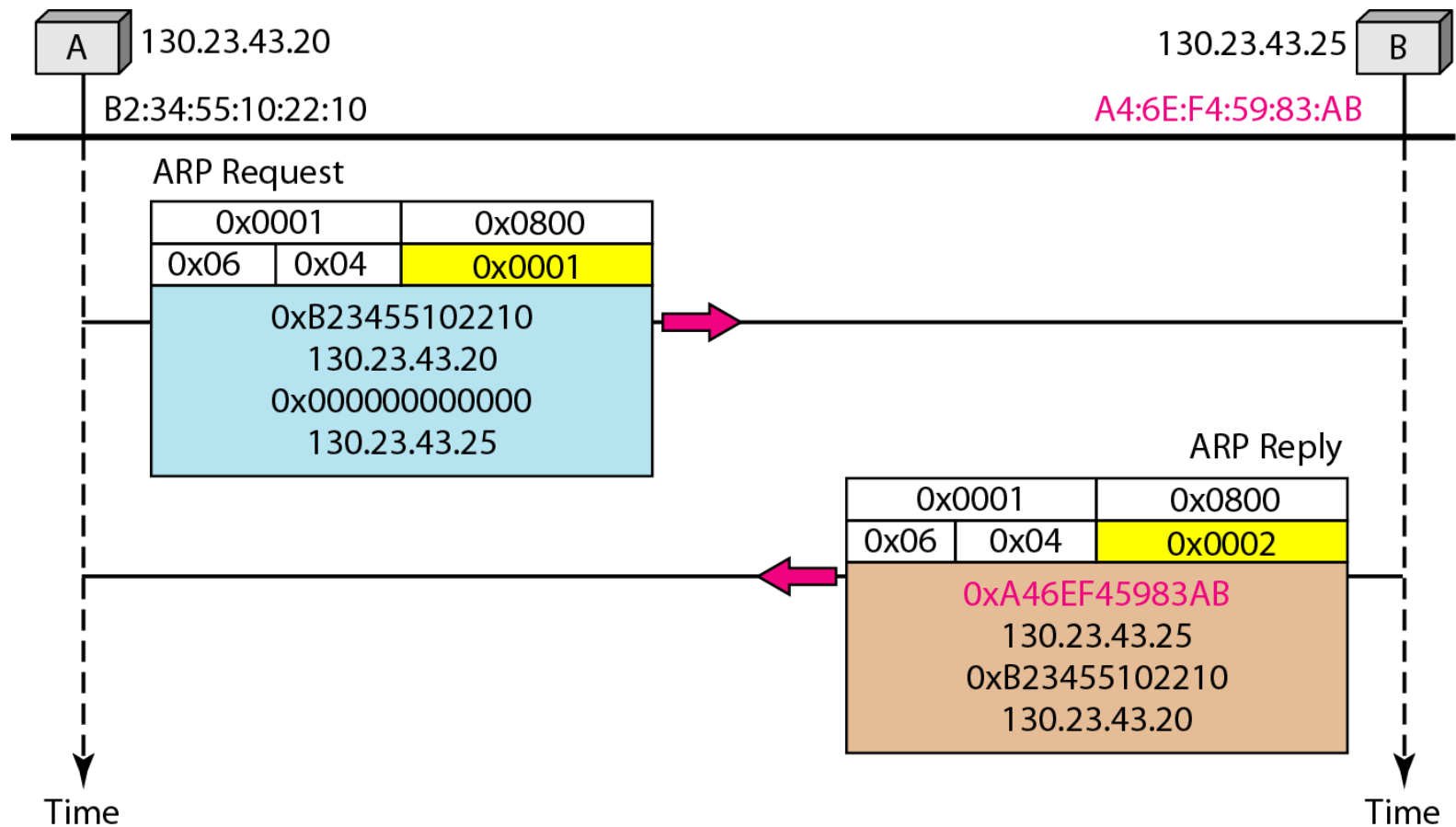
Interface: 192.168.0.103 --- 0xc
Internet Address      Physical Address      Type
192.168.0.1           00-15-e9-79-f1-3c     dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Maria Elena>
```

Ejemplo de ARP

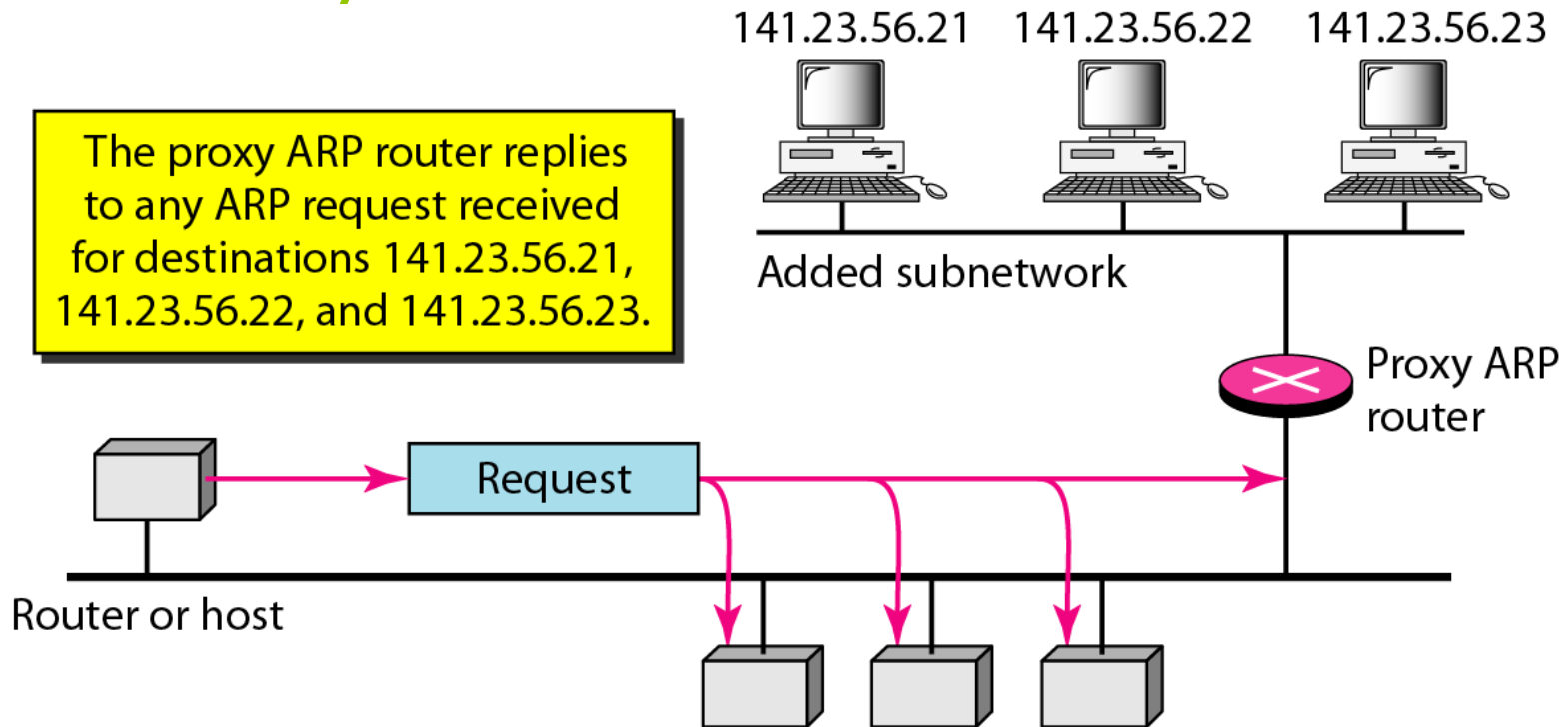
- Un host con dir IP 130.23.43.20 y la dir física B2:34:55:10:22:10 tiene un paquete para ser enviado a otro host con dir IP 130.23.43.25 y dir física. A4:6E:F4:59:83:AB. Los dos hosts están en la misma red Ethernet. Muestre los paquetes ARP request y reply.

Ejemplo de ARP



Proxy ARP

The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.



Proxy ARP y ARP Gratuito

- *Gratuitous ARP* es un paquete ARP enviado por un nodo para espontáneamente causar que un nodo actualice una entrada en su cache ARP.
- Los campos *ARP Sender Protocol Address* y *ARP Target Protocol Address* se colocan en la dir IP del cache que debe ser actualizada.
- El campo *ARP Sender Hardware Address* es determinado a la dir de la capa de enlace de datos a la cual esta entrada en el cahe debería ser actualizada.

ARP Gratuito: Ejemplo

The [High-Availability Linux Project](#) utilizes a command-line tool called `send_arp` to perform the gratuitous ARP needed in their failover process.

A typical clustering scenario might play out like the following:

Two nodes in a cluster are configured to share a common IP address 192.168.1.1. Node A has a hardware address of 01:01:01:01:01:01 and node B has a hardware address of 02:02:02:02:02:02.

Assume that node A currently has IP address 192.168.1.1 already configured on its NIC. At this point, neighboring devices know to contact 192.168.1.1 using the MAC 01:01:01:01:01:01.

Using the heartbeat protocol, node B determines that node A has died. Node B configures a secondary IP on an interface with `ifconfig eth0:1 192.168.1.1`.

Node B issues a gratuitous ARP with `send_arp eth0 192.168.1.1 02:02:02:02:02:02 192.168.1.255`. All devices receiving this ARP update their table to point to 02:02:02:02:02:02 for the IP address 192.168.1.1.

ARP Gratuito: Ejemplo

Example Traffic

```
Ethernet II, Src: 02:02:02:02:02:02, Dst: ff:ff:ff:ff:ff:ff
  Destination: ff:ff:ff:ff:ff:ff (Broadcast)
  Source: 02:02:02:02:02:02 (02:02:02:02:02:02)
  Type: ARP (0x0806)
  Trailer: 000000000000000000000000000000000000000000000000
Address Resolution Protocol (request/gratuitous ARP)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 02:02:02:02:02:02 (02:02:02:02:02:02)
  Sender IP address: 192.168.1.1 (192.168.1.1)
  Target MAC address: ff:ff:ff:ff:ff:ff (Broadcast)
  Target IP address: 192.168.1.1 (192.168.1.1)
0000  ff ff ff ff ff ff 02 02 02 02 02 02 08 06 00 01  .....
0010  08 00 06 04 00 01 02 02 02 02 02 02 c0 a8 01 01  .....
0020  ff ff ff ff ff ff c0 a8 01 01 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Dynamic Host Configuration Protocol (DHCP)

- El *Dynamic Host Configuration Protocol (DHCP)* proporciona parámetros de configuración a host.
- Consiste de:
 - Protocolo para enviar información de parámetros de configuración específicas del host.
 - Mecanismo para la reservación de direcciones a los host.

DHCP: FORMATO PAQUETE

Operation code	Hardware type	Hardware length	Hop count
Transaction ID			
Number of seconds		Unused	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server name (64 bytes)			
Boot filename (128 bytes)			
Options			

DHCP: FORMATO PAQUETE

- Opción: tipo de mensaje , 1 = BOOTREQUEST, 2 = BOOTREPLY .
- Tipo de hardware: por ejemplo, '1' = 10mb ethernet.
- Long Hardware: por ejemplo 6 para 10 Mb ethernet.
- Hops: los clientes lo colocan en cero.
- ID de la transacción: usado para asociar mensajes y respuestas.
- Número de segundos: segundos desde que le cliente comienza el proceso de adquisición o renovación de la dirección.
- Banderas: unicast/broadcast.

DHCP: FORMATO PAQUETE

- ◉ Dir IP del Cliente
- ◉ Tu Dir IP
- ◉ Dir IP del servidor
- ◉ Gateway Dir IP: Dir IP de un agente de relevo
- ◉ Dir de hardware del cliente
- ◉ Nombre del servidor (opcional)
- ◉ Nombre del archivo de boot
- ◉ Parámetros opcionales

DHCP: MENSAJES

- ◉ DHCPDISCOVER – el cliente difunde estos mensajes para localizar clientes disponibles.
- ◉ DHCPOFFER – del servidor al cliente en respuesta al DHCPDISCOVER con oferta de parámetros de configuración.
- ◉ DHCPREQUEST – del cliente a los servidores:
 - ◉ Requiriendo parámetros ofrecidos de un servidor e implícitamente declinando los otros.
 - ◉ Confirmando dir reservada después de por ejemplo un reboot del sistema.
 - ◉ Extendiendo la reserva de un dirección en particular.

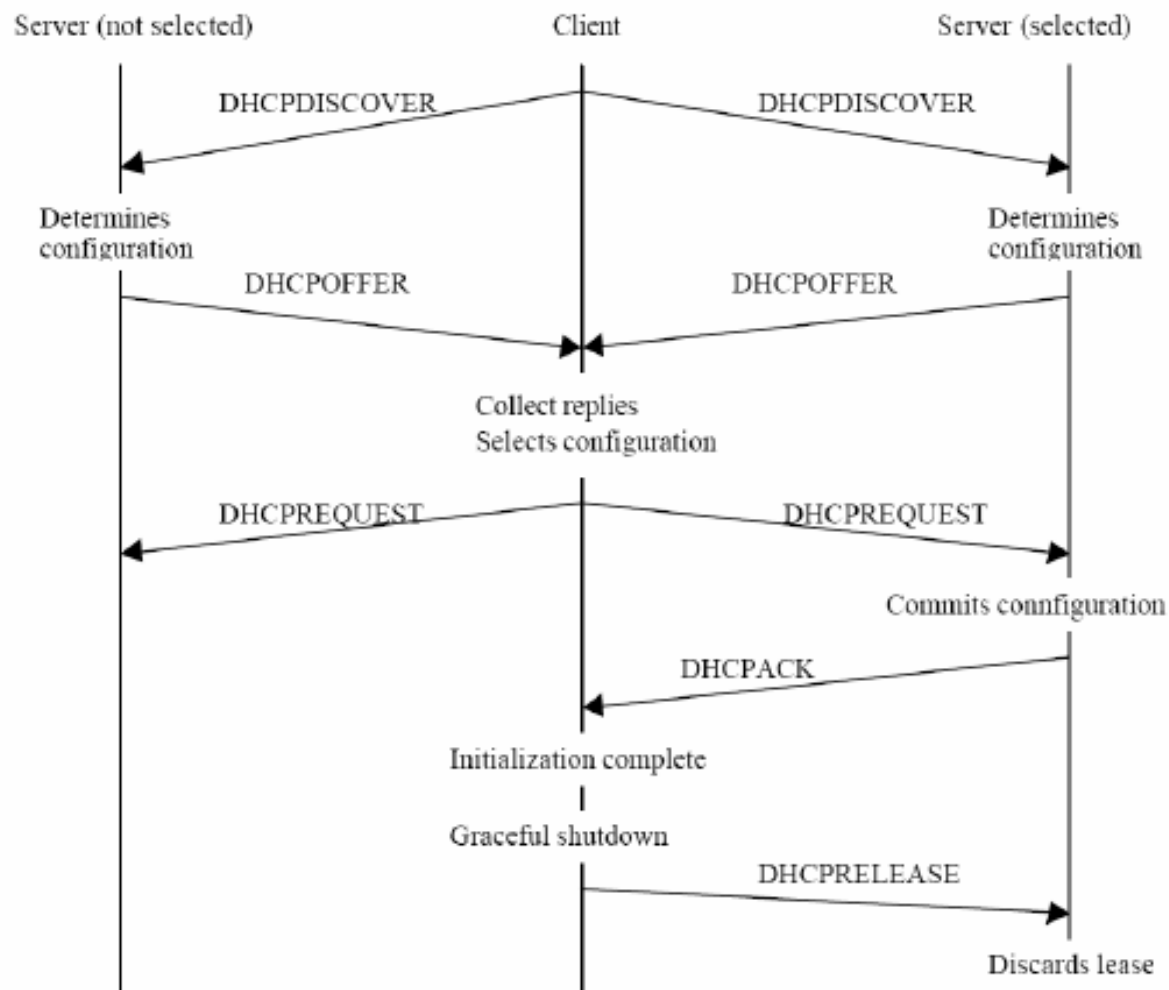
DHCP: MENSAJES

- DHCPACK – servidor al cliente con los parámetros de configuración incluyendo la dir de red negociada.
- DHCPNAK – servidor al cliente indicando que la dir de red es incorrecta (por ejemplo el cliente se ha movido a una nueva subred) o la renta del cliente ha expirado.
- DHCPDECLINE – cliente a servidor indicando que la dir de red esta en uso.

DHCP: MENSAJES

- DHCPRELEASE – cliente al servidor abandonando la dir de red y cancelando cualquier arrendamiento restante.
- DHCPINFORM – cliente a servidor preguntando por parámetros de configuración locales; el cliente tiene una dir de red configurada externamente ya.

DHCP: MENSAJES



DHCP: EJEMPLO

- [CapturaDHCP.pcap](#)

DIRECCIONES PARA INTERNETWORKS

FORMATO DE LAS DIRECCIONES IPv4

- Originalmente la arquitectura de direcciones IP está basada en cinco clases.
- Este sistema proporciona dos niveles de jerarquía:
 - Dirección de la red.
 - Dirección del host.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

FORMATO DE LAS DIRECCIONES IPv4

adecuada para todas la mayoría de las organizaciones por lo tanto se estaban acabando rápidamente

muchos host aquí

Class			
A			
B			
C			
D			
E	1	208,455,456	Reserved

Adicionalmente,
Nunca nadie chequeó como las direcciones eran usadas!!!

pocos host aquí



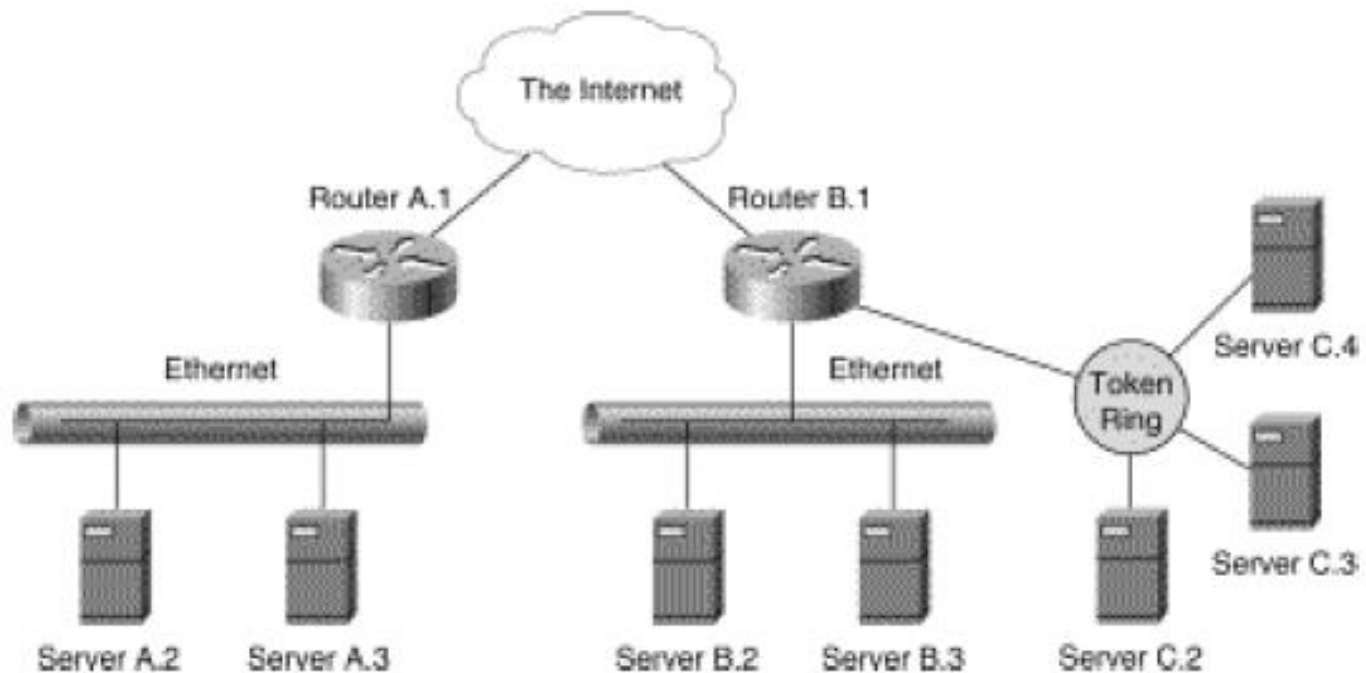
Direccionamiento basado en clases:
Gran parte de las direcciones eran
desperdiciadas

FORMATO DE LAS DIRECCIONES IPv4

- Extensiones al direccionamiento IP para solventar problemas anteriores:
 - Máscaras de subred
 - VLSM
 - CIDR

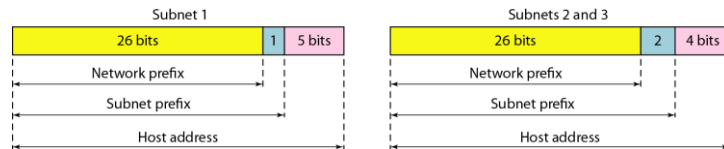
SUBNETTING

Emergen múltiples redes por sitio, esto viola la jerarquía dual de IP



SUBNETTING

Se incluye un nuevo nivel de jerarquía para hacer un modelo con *tres jerarquías de direcciones*



SUBNETTING

- Usa esquema de clases.
- Permite dividir estas redes clase A,B,C en pequeñas subredes, consistentes de:
 - Parte de red
 - Parte de subred
 - Host
- Subnetting es especificado en [RFC 950](#).

SUBNETTING

- Definición de subred según [RFC 950](#):
- *Una subred de redes Internet son sub-secciones lógicamente visibles de una simple red Internet.*
- Las subredes son identificadas usando una pseudo dirección IP llamada *máscara de subred*.
- Le indica a routers y host cuantos bits son usados para identificar la parte de red y subred (prefijo de red extendido).
- En una máscara los bits que representan la red están en “1” y los que representan el host en “0”.

SUBNETTING

- ◉ Ejemplo de máscara de subred:
- ◉ 11111111.11111111.11111111.11000000
(255.255.255.192)
- ◉ Hay 64 host posibles por red.
- ◉ Usualmente, la primera dirección identifica la subred misma.
- ◉ El último es la dirección *broadcast* para la subred.
- ◉ Entonces tenemos 62 dir usables.

SUBNETTING

Table 2-6: Subnetting a Class C Address Space

Number of Bits in Network Prefix	Subnet Mask	Number of Usable Subnet Addresses	Number of Usable Host Addresses, Per Subnet
2	255.255.192.0	2	62
3	255.255.224.0	6	30
4	255.255.240.0	14	14
5	255.255.248.0	30	6
6	255.255.252.0	62	2

SUBNETTING

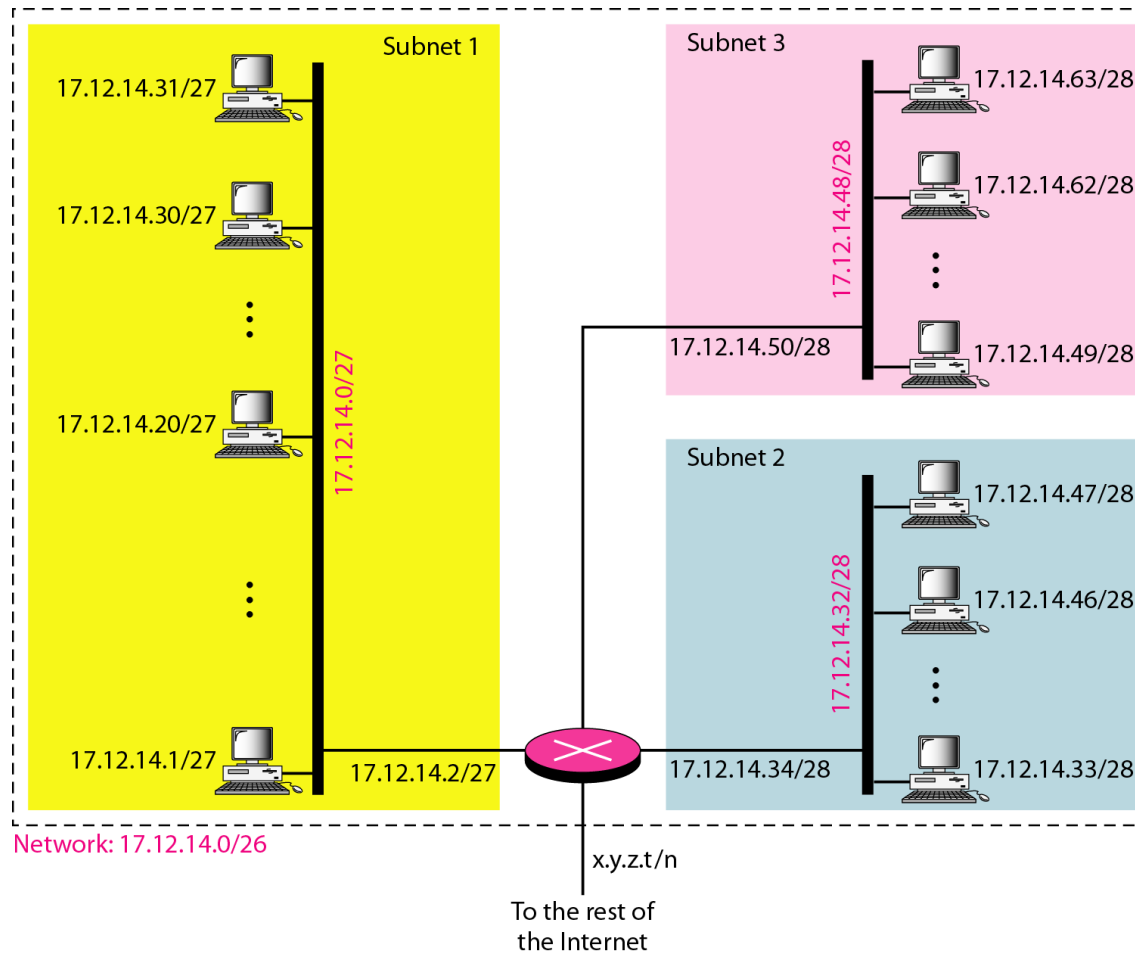
- Se desea crear 6 subredes a partir de la Dirección clase C 192.168.125.0, calcule:
 - Número de subred
 - Máscara
 - Dirección de inicio

VARIABLE LENGTH SUBNET MASK: VLSM

- *Subnetting* limita a una sola máscara para toda la red.
- Por lo tanto, una organización no podrá tener subredes de distinto tamaño.
- La solución fue publicada por el IETF en el [RFC 1009](#), que especifica como una red dividida en subredes podría usar mas de una máscara de subred.

VLSM: EJEMPLO

Calcule la máscara para cada subred



CLASSLESS INTERDOMAIN ROUTING: CIDR

- Se propone a raíz de los siguientes problemas:
- Se estaban acabando la dir IPv4 no asignadas, en particular las B.
- Rápido crecimiento de las tablas de enrutamiento.
- Se eliminan el mecanismo ineficiente de clases, creándose CIDR.
- Descrito en RFCs 1517-1520.

CIDR

- Características:
 - Eliminación del esquema basado en clases.
 - Mejoramiento de agregación de rutas:
 - Una simple entrada en una tabla puede representar el espacio de direcciones de muchas redes:
 - Supernetting.

SUPERNETTING

- *No es mas que usar bloques contiguos de direcciones clase C para simular un red simple.*
- *Varias redes son usadas para crear un super red (supernet).*

SUPERNETTING

- Por ejemplo, una organización que necesita 1000 direcciones se le pueden otorgar 4 bloques continuos de direcciones clase C.
- Con esta direcciones se le crea una super red.
- Note que la máscara cambia de /24 a /22.

SUPERNETTING (TOMADO DE RFC 1338)

Consider the block of 2048 class-C network numbers beginning with 192.24.0.0 (0xC0180000 and ending with 192.31.255.0 (0xC01FFF00) allocated to a single network provider, "RA". A "supernetted" route to this block of network numbers would be described as 192.24.0.0 with mask of 255.248.0.0 (0xFFF80000).

Assume this service provider connects six clients in the following order (significant because it demonstrates how temporary "holes" may form in the service provider's address space):

- "C1" requiring fewer than 2048 addresses (8 class-C networks)
- "C2" requiring fewer than 4096 addresses (16 class-C networks)
- "C3" requiring fewer than 1024 addresses (4 class-C networks)
- "C4" requiring fewer than 1024 addresses (4 class-C networks)
- "C5" requiring fewer than 512 addresses (2 class-C networks)
- "C6" requiring fewer than 512 addresses (2 class-C networks)

SUPERNETTING (TOMADO DE RFC 1338)

In all cases, the number of IP addresses "required" by each client is assumed to allow for significant growth. The service provider allocates its address space as follows:

C1: allocate 192.24.0 through 192.24.7. This block of networks is described by the "supernet" route 192.24.0.0 and mask 255.255.248.0

C2: allocate 192.24.16 through 192.24.31. This block is described by the route 192.24.16.0, mask 255.255.240.0

C3: allocate 192.24.8 through 192.24.11. This block is described by the route 192.24.8.0, mask 255.255.252.0

C4: allocate 192.24.12 through 192.24.15. This block is described by the route 192.24.12.0, mask 255.255.252.0

C5: allocate 192.24.32 and 192.24.33. This block is described by the route 192.24.32.0, mask 255.255.254.0

C6: allocate 192.24.34 and 192.24.35. This block is described by the route 192.24.34.0, mask 255.255.254.0

COMO TRABAJA CIDR

- El prefijo puede ser de cualquier longitud.
- Cada dirección de red se anuncia con una máscara.
- Esta máscara identifica la longitud del prefijo de red.
- Ejemplo, 192.125.61.8/20 identifica una dir de red CIDR con un prefijo de longitud 20.

	Network number	Host number
Binary address	11000000.1111101.0011	1101.00000000

CIDR: EJEMPLO (TOMADO DE RFC 4632)

Consider the block of 524288 (2^{19}) addresses, beginning with 10.24.0.0 and ending with 10.31.255.255, allocated to a single network provider, "PA". This is equivalent in size to a block of 2048 legacy "Class C" network numbers (or /24s). A classless route to this block would be described as 10.24.0.0 with a mask of 255.248.0.0 and the prefix 10.24.0.0/13.

Assume that this service provider connects six sites in the following order (significant because it demonstrates how temporary "holes" may form in the service provider's address space):

- o "C1", requiring fewer than 2048 addresses (/21 or 8 x /24)
 - o "C2", requiring fewer than 4096 addresses (/20 or 16 x /24)
 - o "C3", requiring fewer than 1024 addresses (/22 or 4 x /24)
 - o "C4", requiring fewer than 1024 addresses (/22 or 4 x /24)
 - o "C5", requiring fewer than 512 addresses (/23 or 2 x /24)
 - o "C6", requiring fewer than 512 addresses (/23 or 2 x /24)

CIDR: EJEMPLO (TOMADO DE RFC 4632)

In all cases, the number of IPv4 addresses "required" by each site is assumed to allow for significant growth. The service provider delegates its address space as follows:

- o C1. assign 10.24.0 through 10.24.7. This block of networks is described by the route 10.24.0.0/21 (mask 255.255.248.0).
- o C2. Assign 10.24.16 through 10.24.31. This block is described by the route 10.24.16.0/20 (mask 255.255.240.0).
- o C3. Assign 10.24.8 through 10.24.11. This block is described by the route 10.24.8.0/22 (mask 255.255.252.0).
- o C4. Assign 10.24.12 through 10.24.15. This block is described by the route 10.24.12.0/22 (mask 255.255.252.0).
- o C5. Assign 10.24.32 and 10.24.33. This block is described by the route 10.24.32.0/23 (mask 255.255.254.0).
- o C6. Assign 10.24.34 and 10.24.35. This block is described by the route 10.24.34.0/23 (mask 255.255.254.0).

CIDR: EJEMPLO (TOMADO DE RFC 4632)

To make this example more realistic, assume that C4 and C5 are multi-homed through some other service provider, "PB". Further assume the existence of a site, "C7", that was originally connected to "RB" but that has moved to "PA". For this reason, it has a block of network numbers that are assigned out PB's block of (the next) 2048 x /24.

- o C7. Assign 10.32.0 through 10.32.15. This block is described by the route 10.32.0.0/20 (mask 255.255.240.0).

For the multi-homed sites, assume that C4 is advertised as primary via "RA" and secondary via "RB"; and that C5 is primary via "RB" and secondary via "RA". In addition, assume that "RA" and "RB" are both connected to the same transit service provider, "BB".

```

10.24.0.0 -- 10.24.7.0___10.32.0.0 - 10.32.15.0
C1: 10.24.0.0/21 \ / C7: 10.32.0.0/20
\ /
+-----+ +-----+
10.24.16.0 - 10.24.31.0_ | | 10.24.12.0 - 10.24.15.0_ | |
C2: 10.24.16.0/20 \ | | / C4: 10.24.12.0/20 \ | |
\ | | / \ | |
| | / \ | |
10.24.8.0 - 10.24.11.0___/ | PA \ \ | PB |
C3: 10.24.8.0/22 | | \___10.24.32.0 - 10.24.33.0___| |
| | C5: 10.24.32.0/23 | |
| | | |
10.24.34.0 - 10.24.35.0___/ | | | |
C6: 10.24.34.0/23 | | | |
+-----+ +-----+
| | | |
routing advertisements: | | | |
| | | |
10.24.12.0/22 (C4) | | 10.24.12.0/22 (C4) | |
10.32.0.0/20 (C7) | | 10.24.32.0/23 (C5) | |
10.24.0.0/13 (PA) | | 10.32.0.0/13 (PB) | |
| | | |
VV VV
+-----+
BACKBONE NETWORK BB

```



IPv6

IPv6

- El IETF ha adoptado una nueva versión de IP, llamada IPv6, diseñada para reemplazarlo IPv4.



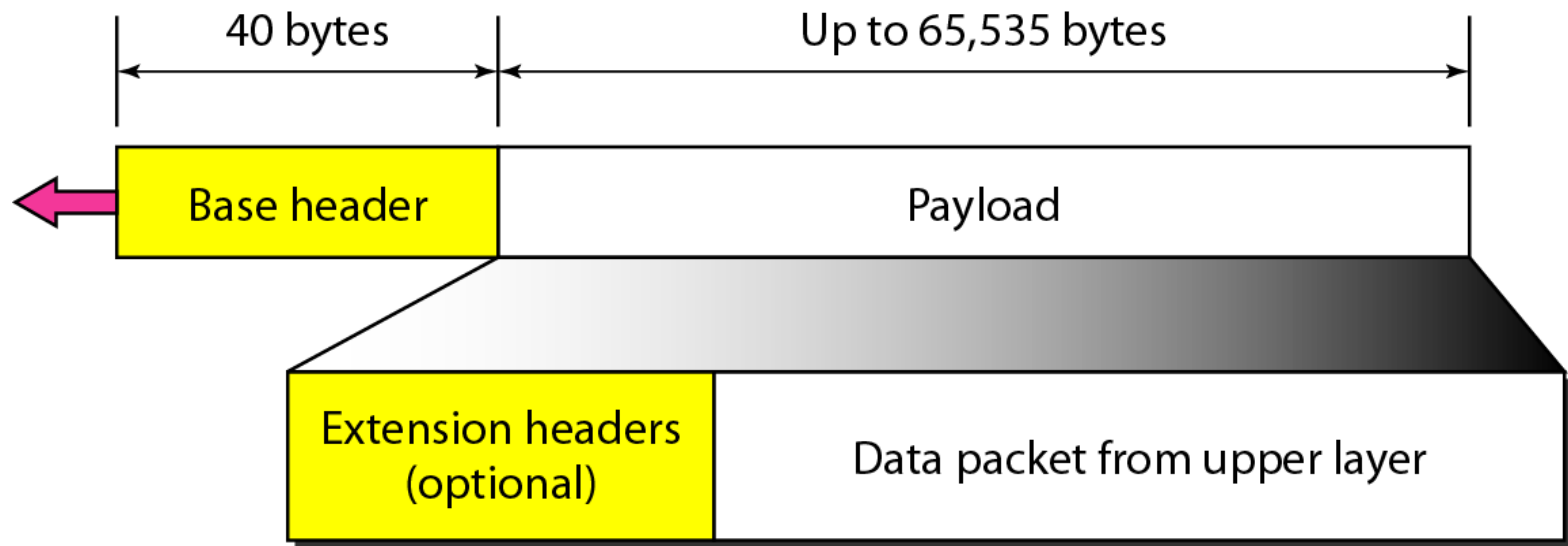
IPv6!

IPv6

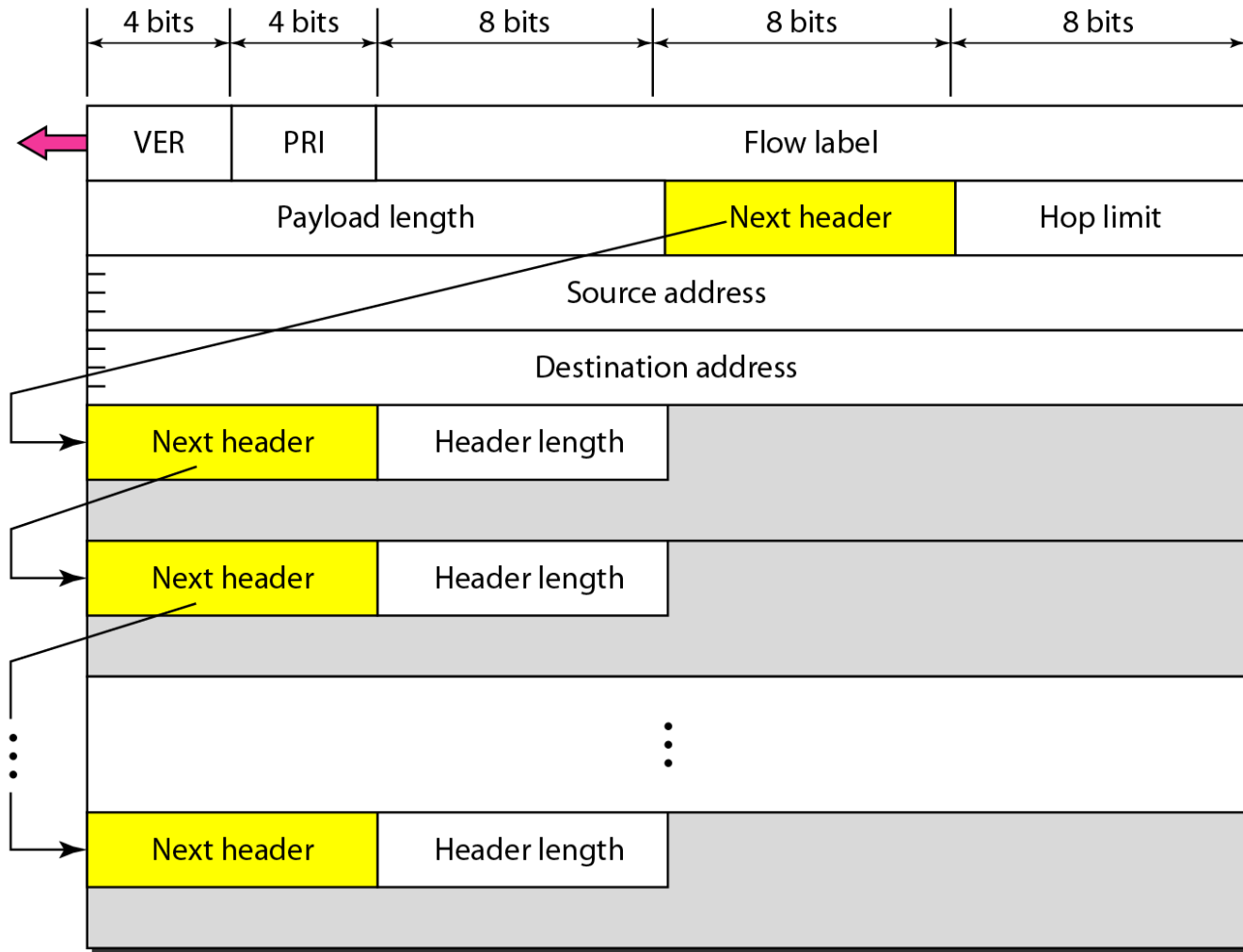
- ◉ Espacio de direcciones mas largo.
- ◉ Mejor formato del encabezado.
- ◉ Nuevas opciones.
- ◉ Permite extensiones.
- ◉ Soporte para reservación de recursos.
- ◉ Soporte a mayor seguridad.



IPv6



IPv6



IPv6

- **Versión:** versión del protocolo.
- **Prioridad:** valor de prioridad.
- **Etiqueta de flujo:** usado para etiquetar paquetes que requieren manejo especial por los enrutadores.

IPv6

- ◉ **Longitud de la carga útil:** indica la longitud total de todos los encabezados de extensión mas el PDU de la capa mas alta.
- ◉ **Próximo encabezado:** identifica el tipo de encabezado que sigue el encabezado IPv6.
- ◉ **Límite de salto:** indica el número restante de saltos para este paquete.
- ◉ **Dir fuente**
- ◉ **Dir destino**

IPv6

Table 20.6 *Next header codes for IPv6*

<i>Code</i>	<i>Next Header</i>
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

IPv6

Table 20.7 *Priorities for congestion-controlled traffic*

<i>Priority</i>	<i>Meaning</i>
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

IPv6

Table 20.8 *Priorities for noncongestion-controlled traffic*

<i>Priority</i>	<i>Meaning</i>
8	Data with greatest redundancy
...	...
15	Data with least redundancy

IPv6: Comparación con IPv4



- El campo de longitud del encabezado es eliminado porque la longitud del encabezado es fija.
- El campo TOS es eliminado. Los campos de prioridad y etiqueta de flujo asumen sus funciones.
- El campo de longitud total es eliminado en IPv6 y reemplazado por el campo de longitud total.
- La identificación, el flag y los campos de desplazamiento son eliminados. Ahora están ubicados en el encabezado de fragmentación.

IPv6: Comparación con IPv4



- El campo TTL es llamado límite de saltos.
- El checksum es eliminado porque es provisto por las capas superiores.
- Los campos de opción en IPv4 son implementados como encabezados de extensión en IPv6.

IPv6: Comparación con IPv4



- Las opciones de fin-de opciones y no operación en IPv4 son reemplazadas por las opciones Pad1 y PadN.
- La opción de registro de ruta no está implementada en IPv6.
- La opción de *timestamp* no está implementada.
- La opción de ruta es llamada encabezado de extensión de ruta fuente.
- Los campos de fragmentación en la sección de encabezado base de IPv4 se ha movido al encabezado de extensión en IPv6.
- El encabezado de extensión de autenticación es nuevo.
- El encabezado de seguridad de cifrado es nuevo.

IPV6: DIRECCIONAMIENTO

- Tipos de direcciones:
 - **Unicast:** un identificador para una interfaz
 - **Multicast:** un identificador para un conjunto de interfaces. Un paquete es enviado a todas las interfaces identificadas por esa dir.
 - **Anycast:** un identificador para un conjunto de interfaces. El paquete es enviado a una de las interfaces.

IPV6: DIRECCIONAMIENTO- AGREGACION

- Las direcciones IPv6 son agregables:
 - Direcciones que comparten el mismo prefijo pueden ser enviadas por la misma ruta.

IPV6: FORMATO DE LAS DIRECCIONES

- Representadas preferiblemente como una secuencia de valores de 16 bit.
- XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XX
XX
- Ejemplos:
- FEDC:BA98:7654:3210:FEDC:BA98:7654:321
0
- 1080:0:0:0:8:800:200C:417

IPV6: FORMATO DE LAS DIRECCIONES

- Debido a lo largo del formato de direcciones algunas simplificaciones se han tomado.
- El uso de "::" indica múltiples grupos de 16 bits en cero.
- "::" puede aparecer solo una vez.

Address type	Standard representation	Compressed
Unicast address	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast address	FF01:0:0:0:0:0:0:101	FF01::101
Loopback address	0:0:0:0:0:0:0:1	::1
Unspecified addresses	0:0:0:0:0:0:0:0	::

IPV6: FORMATO DE LAS DIRECCIONES

- Cuando se trabaja en un ambiente mixto IPv6 e IPv4:
 - x:x:x:x:x:x:d.d.d.d
 - x es definido como en láminas anteriores.
 - d son valores decimales de 8 bits.
- Ejemplo:
 - 0:0:0:0:0:0:13.1.68.3
 - 0:0:0:0:0:FFFF:129.144.52.38
- O comprimido:
 - ::13.1.68.3
 - ::FFFF:129.144.52.38

IPV6: REPRESENTACION DE UN PREFIJO DE DIRECCION

- ipv6-address/prefix-length
- ipv6-address: es un dirección IPv6.
- prefix-length: es un número decimal especificando cuanto bits contiguos a la izquierda de la dirección comprenden el prefijo.
- Ejemplo de representaciones legales del prefijo de 60 bits 20010DB80000CD3 (hexadecimal):
- 2001:0DB8:0000:CD30:0000:0000:0000:0000/60
- 2001:0DB8::CD30:0:0:0:0/60
- 2001:0DB8:0:CD30::/60

IPV6: REPRESENTACION DE UN PREFIJO DE DIRECCION

- Representaciones NO legales
 - 2001:0DB8:0:CD3/60
 - Se puede remover ceros iniciales pero no finales
 - 2001:0DB8::CD30/60
 - esto se interpretaría como
 - 2001:0DB8:0000:0000:0000:0000:0000:CD30
 - 2001:0DB8::CD3/60
 - esto se interpretaría como
 - 2001:0DB8:0000:0000:0000:0000:0000:0CD3

IPV6: REPRESENTACION DE UN PREFIJO DE DIRECCION

- ◉ Representaciones prefijo mas dir nodo:
- ◉ Dir nodo
- ◉ 2001:0DB8:0:CD30:123:4567:89AB:CDEF
- ◉ Y su número de subred
- ◉ 2001:0DB8:0:CD30::/60
- ◉ Puede ser abreviado como
- ◉ 2001:0DB8:0:CD30:123:4567:89AB:CDEF/60

IPV6: TIPOS DE DIRECCIONES

UNICAST

- **Unicast Global:** pueden ser enrutadas en la Internet IPv6 global.
- **Unicast del enlace local (unicast link local):** direccionamiento de un enlace simple. Estas direcciones no son enviadas mas allá del enlace.
- **Unicast del sitio local (unicast site local):** direccionamiento en un sitio tal como un campus u organización.
- **Direcciones con IPv4 o NSAP embebidas**

IPV6: IDENTIFICACION DE LOS TIPOS DE DIRECCIONES

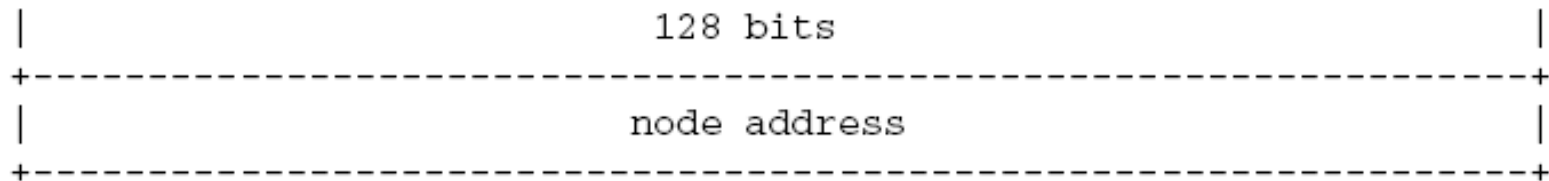
Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Site-local unicast	1111111011	FEC0::/10
Global unicast	(everything else)	

IPV6: TIPOS ESPECIALES DE DIRECCIONES UNICAST

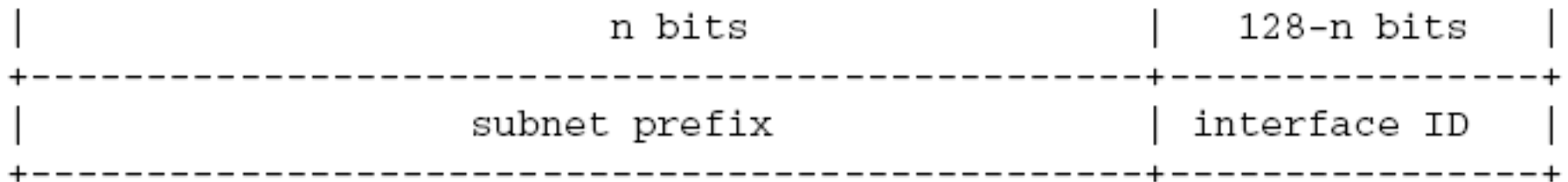
- Dirección No Especificada:
 - 0:0:0:0:0:0:0:0
- Loopback
 - 0:0:0:0:0:0:0:1

IPV6: FORMATO DE LA DIRECCION

Visión General

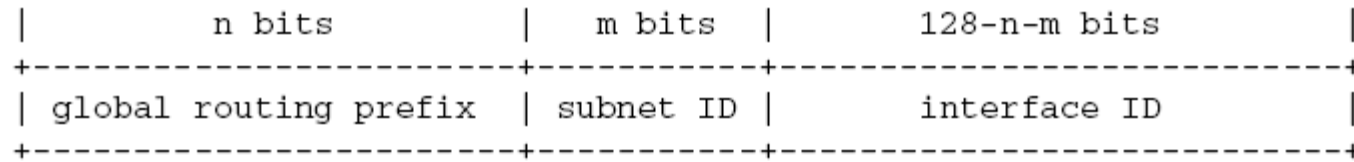


Forma mas sofisticada



Donde el *prefijo de subred* es identificable como el enlace local al cual el nodo está conectado

IPV6: FORMATO DE LA DIRECCION



- El prefijo de enrutamiento global es un valor asignado a un sitio (cluster de subredes/enlaces).
- El ID de subred es un identificador de un enlace dentro del sitio.

IPV6: DIRECCIONES ANYCAST

- Las direcciones anycast se asignan desde el espacio de direcciones unicast.
- Utilizan cualquiera de los formatos de dirección definida unicast.
- Por lo tanto, las direcciones anycast son sintácticamente indistinguibles de las direcciones unicast.
- Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndola en una dirección anycast, los nodos a los que la dirección es asignada debe ser configurada explícitamente para saber que se trata de una dirección de difusión ilimitada.

IPV6: DIRECCIONES MULTICAST



- T=0 dir permanentemente asignada.

IPV6: DIRECCIONES MULTICAST

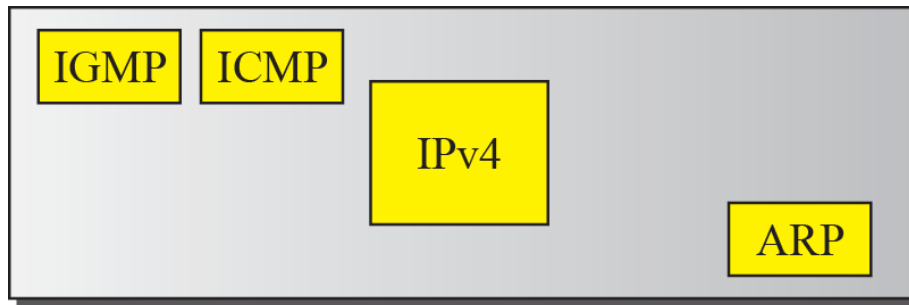
El campo scop puede tener algunos de los siguientes valores

0	reserved
1	Interface-Local scope
2	Link-Local scope
3	reserved
4	Admin-Local scope
5	Site-Local scope
6	(unassigned)
7	(unassigned)
8	Organization-Local scope
9	(unassigned)
A	(unassigned)
B	(unassigned)
C	(unassigned)
D	(unassigned)
E	Global scope
F	reserved

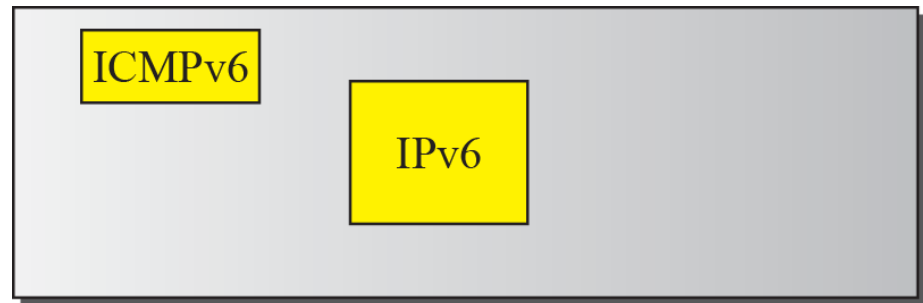
ICMPv6

- Otro protocolo que ha sido modificado en la versión 6 del protocolo TCP / IP es ICMP.
- Esta nueva versión, de control de Internet Mensaje Protocolo versión 6 (ICMPv6), sigue la misma estrategia y los objetivos de la versión 4.
- ICMPv6, sin embargo, es más complicado que ICMPv4:
 - algunos protocolos que eran independientes en la versión 4 ahora son parte de ICMPv6
 - algunos mensajes nuevos se han añadido para hacerlo más útil.

ICMPv6



Network layer in version 4

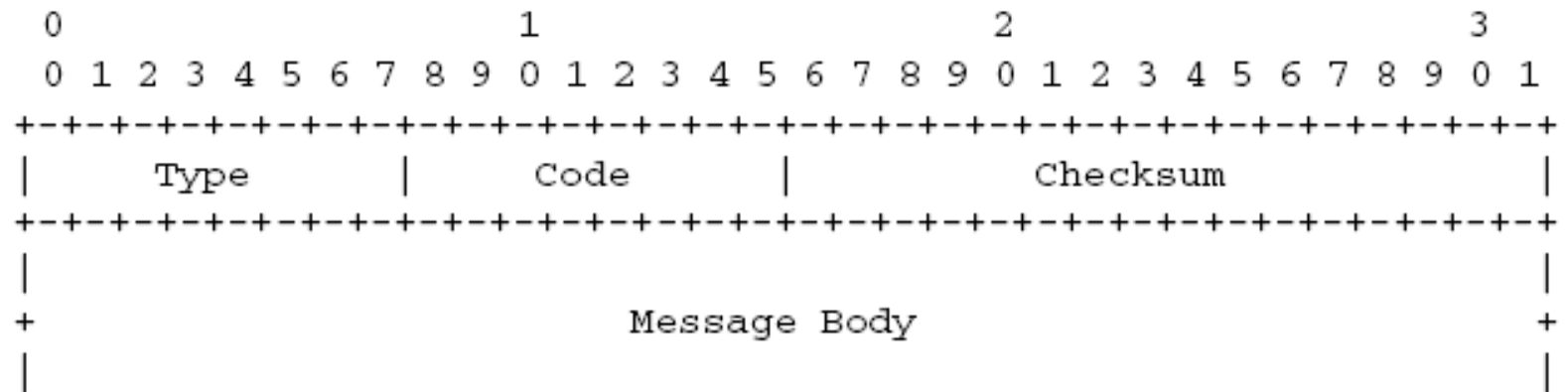


Network layer in version 6

ICMPv6: FUNCIONES

- Incorpora mensajes para reportar condiciones de error.
- Incorpora funciones de diagnóstico como ping y traceroute.
- Incorpora funciones como *Path MTU Discovery* and *Neighbor Discovery*

ICMPV6: FORMATO MENSAJES



ICMPV6: FORMATO MENSAJES

Type	Name	Reference
1	Destination Unreachable	[RFC2463]
2	Packet Too Big	[RFC2463]
3	Time Exceeded	[RFC2463]
4	Parameter Problem	[RFC2463]
128	Echo Request	[RFC2463]
129	Echo Reply	[RFC2463]
130	Multicast Listener Query	[RFC2710]
131	Multicast Listener Report	[RFC2710]
132	Multicast Listener Done	[RFC2710]
133	Router Solicitation	[RFC2461]
134	Router Advertisement	[RFC2461]
135	Neighbor Solicitation	[RFC2461]
136	Neighbor Advertisement	[RFC2461]
137	Redirect Message	[RFC2461]
138	Router Renumbering	[RFC2894]
139	ICMP Node Information Query	[RFC2894]
140	ICMP Node Information Response	[RFC2894]
141	Inverse Neighbor Discovery Solicitation Message	[RFC3122]
142	Inverse Neighbor Discovery Advertisement Message	[RFC3122]

ICMPV6: TIPOS DE MENSAJES

- ◉ Destino inalcanzable:
 - ◉ No ruta al destino
 - ◉ Comunicación con el destino administrativamente prohibida
 - ◉ Dir inalcanzable
 - ◉ Puerto inalcanzable

ICMPV6: TIPOS DE MENSAJES

- Tiempo excedido
 - Paquetes que han estado en la red por mucho tiempo.
 - Paquetes que han excedido su tiempo máximo de resemblance del fragmento.

ICMPV6: TIPOS DE MENSAJES

- Mensaje de eco
 - Echo Request
 - Echo reply

ICMPV6: DESCUBRIMIENTO DEL CAMINO

- Fragmentación solo soportada en el origen y en el destino.
- No fragmentación salto por salto.
- La idea es que se conozca el *path MTU* antes de enviar el paquete.
- El *path MTU* es el paquete mas largo que puede transportar una red a lo largo de la ruta entre el origen y el destino sin fragmentación

ICMPV6 PATH DISCOVERY

- Un nodo envía el más largo paquete permisible en su propio enlace al destino.
- Si un nodo intermedio no puede manejar paquetes de ese tamaño, el enrutador retorna un mensaje ICMPv6 de error.
- La fuente enviará otro paquete de menor tamaño.
- Así sucesivamente.
- El *path MTU* es el más reciente MTU.

ICMPv6: DESCUBRIMIENTO DE VECINOS

- *Neighbor Discovery (ND)* es un protocolo de alcance en el enlace local que puede correr en enrutadores y hosts.
- Combina las funciones de *Address Resolution Protocol (ARP)*, *ICMP Router Discovery* y *ICMP Redirect*.
- Un vecino es un nodo conectado sobre un enlace del nivel de enlace de datos .

ICMPv6: DESCUBRIMIENTO DE VECINOS-FUNCIONES

- ◉ **Address Protocol Resolution:** un nodo puede determinar la dir física de un nodo dado su dir IPv6.
- ◉ **Redirect:** un nodo puede notificar a la fuente de la existencia de un mejor salto para su destino. Este proporciona su dir física para este mejor salto.

ICMPV6: DESCUBRIMIENTO DE VECINOS

- **Reachability:** un nodo puede verificar si un vecino es directamente alcanzable. También puede notificar su cambio de dirección física.
- **Duplicate address detection:** un nodo puede detectar si la dirección ya está siendo utilizado por otro nodo.
- **Router Discovery:** un host puede localizar a un enrutador vecino.
- **Neighbor Discovery:** un host puede descubrir los destinos que se encuentran en su vínculo (en el vínculo) y los que son accesibles a través de un router.
- **Parameters Discovery:** un host puede descubrir diversos parámetros de enlace, como el tamaño de MTU.

ICMPV6: MENSAJES DE DESCUBRIMIENTO DE VECINOS

- **Router solicitation:** un host requiere a un router que anuncie su presencia
- **Router advertisement:** se usa para que un router anuncie su presencia.

ICMPV6: MENSAJES DE DESCUBRIMIENTO DE VECINOS

- **Neighbor Solicitation:** un nodo envía este mensaje para determinar una dirección física de un vecino o para verificar si un nodo es alcanzable por su enlace y detectar direcciones duplicadas.
- **Neighbor Advertisement:** puede ser generado en respuesta a la anterior o para notificar un cambio de dirección física.
- **Redirect:** un router envía este mensaje para notificar a un host de la existencia de un mejor primer salto en el camino hacia el destino.

IPV6: AUTOCONFIGURACION

- Autoconfiguración *stateful*: se usan servidores DHCP para que un nodo se auto configure.
- Autoconfiguración *stateless*: los nodos se auto configuran ellos mismos.
- Remuneración de enrutadores y redes: permite la reconfiguración de enrutadores *gateways*.

IPV6: AUTOCONFIGURACION STATEFUL

- **Direcciones**

- **All_DHCP_Relay_Agents_and_Servers (FF02::1:2):** una dir multicast de alcance local.
- **All_DHCP_Servers (FF05::1:3):** una dir multicast de alcance del sitio usada por agentes de relevo para comunicarse con servidores.

IPV6:DHCPV6

- SOLICIT
- ADVERTISE
- REQUEST
- CONFIRM
- RENEW
- REBIND
- REPLY

IPV6:DHCPV6

- **RELEASE**
- **DECLINE**
- **RECONFIGURE**
- **INFORMATION-REQUEST**
- **RELAY-FORW**
- **RELAY-REPL**

IPV6:DHCPV6

- 1. El cliente envía un mensaje de **SOLICIT** por multicast para encontrar un servidor DHCPv6 y pedir un contrato de arrendamiento.
- 2. Cualquier servidor que puede satisfacer la petición del cliente responde a ella con un mensaje de **ADVERTISE**.
- 3. El cliente elige uno de los servidores y envía un mensaje de **REQUEST** que le pide que confirme la dirección ofrecida y otros parámetros.
- 4. El servidor responde con un mensaje de **CONFIRM** al finalizar el proceso.

IPV6: AUTOCONFIGURACION STATELESS

- El proceso de auto-configuración incluye una serie de pasos:
- 1. Creación de una dirección local de vínculo para el nodo de auto-configuración.
- 2. Verificación de la unicidad de la dirección local de vínculo en el enlace.
- 3. Determinar qué información debe ser configuradas automáticamente y cómo esa información se debe obtener.

IPV6: AUTOCONFIGURACION STATELESS

- La autoconfiguración *stateless* no requiere configuración manual de los hosts.
- Muy poca de los enrutadores.
- No se necesita servidores.
- El host genera su dir usando una combinación de información disponible e información anunciada por los routers.
- Los routers anuncian los prefijos de red.
- Los hosts generan el ID de la interfaz.
- En ausencia de enrutadores un host solo puede generar dir de alcance local (link local address)



Enrutamiento

ENRUTAMIENTO

- Los protocolos de enrutamiento usan métricas para evaluar el mejor camino por el cual un paquete viajara a su destino.
- Una métrica es un medida estándar (e.g. ancho de banda) usada para determinar el camino optimo al destino.
- Los protocolos de enrutamiento inicializan, mantienen y actualizan tablas de enrutamiento.
- La información en las tablas depende el algoritmo de enrutamiento.

ENRUTAMIENTO

- Table de *Forwarding*:
 - Contiene mapeo de un número de red a una interfaz de salida e información sobre la MAC, tal como dir Ethernet.

Network Number	Interface	MAC Address
18	if0	8:0:2b:e4:b:1:2

ENRUTAMIENTO

- Tabla de enrutamiento:
 - Contiene mapeo de número de red a próximo salto.
 - Contiene información de cómo la información fue aprendida,
 - El *router* podría decidir si descartar algún información basado en el punto anterior.

Network Number	Next Hop
18	171.69.245.10

ENRUTAMIENTO

- Metas de diseño
 - Optimo -> capacidad de obtener mejor ruta.
 - Simplicidad y poco *overhead* -> mínimo software y *overhead* de utilización.
 - Robustez y estabilidad -> debe funcionar correctamente ante situaciones inusuales e imprevistas.
 - Convergencia rápida -> Acuerdo de todos los *routers* acerca de la ruta óptima.
 - Flexibilidad -> rápidamente adaptarse a una variedad de circunstancias de red.

ENRUTAMIENTO

- ◉ *Domino de enrutamiento:*
 - ◉ Una *internetwork* en la cual los *routers* están bajo el mismo control administrativo (un campus de la universidad, la red de un ISP).

ENRUTAMIENTO

- Tipos de algoritmos
 - Estático vs dinámico
 - Camino simple múltiples caminos
 - Plano vs jerárquico
 - Host inteligente vs router inteligente
 - Intra dominio vs inter dominio
 - Estado de enlace vs vector distancia

ENRUTAMIENTO

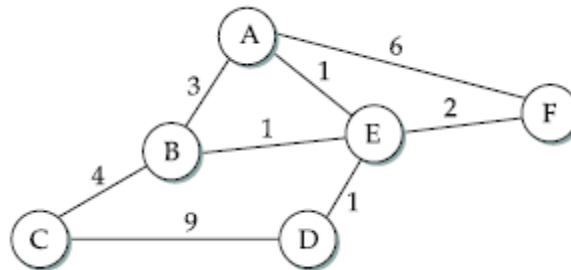
- Métricas de enrutamiento:
 - Longitud del camino
 - Confiabilidad -> por ejemplo, tasa errores en los bits
 - Retardo
 - Ancho de banda
 - Carga
 - Costo de la comunicación

ENRUTAMIENTO

- Protocolos de enrutamiento entre dominios:
 - Vector Distancia (RIP)
 - Estado del enlace (OSPF)

ENRUTAMIENTO

- Red como un grafo
 - Nodos = routers, switches, hosts o redes.
 - Arcos = enlaces de red.
 - Los arcos tienen costos (tasa de envío del enlace, RTT)

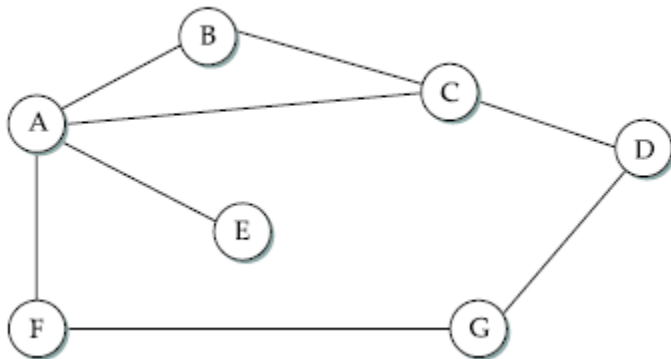


ENRUTAMIENTO: VECTOR DISTANCIA

- Cada nodo construye un arreglo unidimensional (vector) que contienen distancias (costos) a otros nodos.
- Distribuye su vector a los vecinos.
- Cada nodo conoce el costo del enlace a cada uno de sus vecino conectados directamente.
- Si el enlace está abajo el costo es infinito.

ENRUTAMIENTO: VECTOR DISTANCIA

- Red de ejemplo



Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

Table 4.5 Initial distances stored at each node (global view).

Destination	Cost	Next Hop
B	1	B
C	1	C
D	∞	—
E	1	E
F	1	F
G	∞	—

Table 4.6 Initial routing table at node A.

ENRUTAMIENTO: VECTOR DISTANCIA

- Próximo paso:
 - Cada nodo envía un mensaje a sus vecinos conectados directamente conteniendo su lista personal de distancias.

Destination	Cost	Next Hop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Table 4.7 Final routing table at node A.

ENRUTAMIENTO: VECTOR DISTANCIA

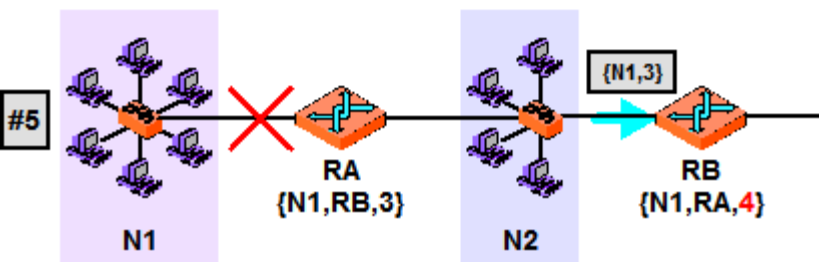
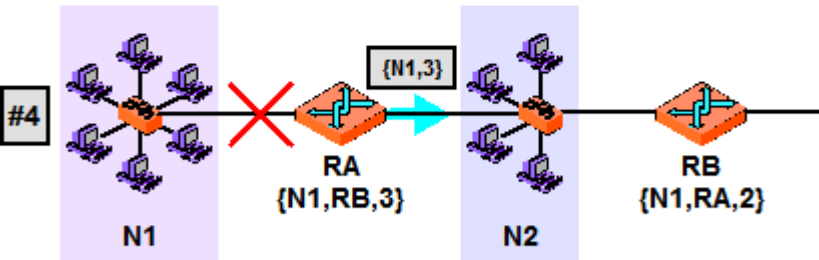
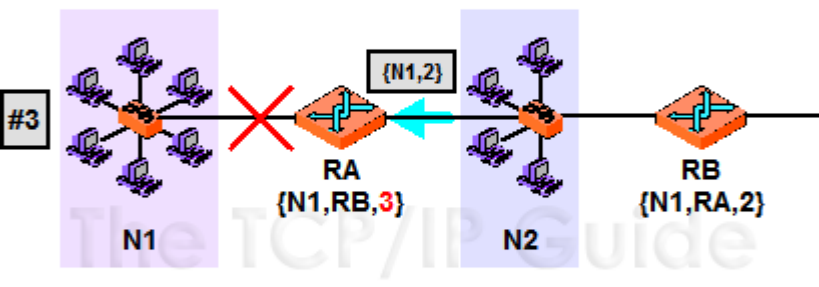
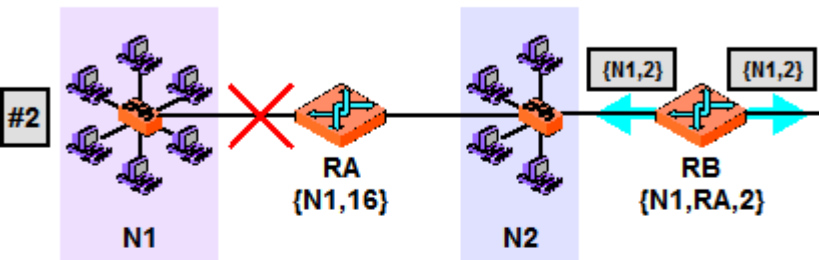
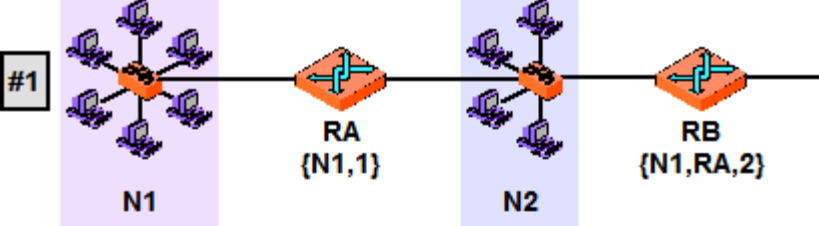
- Tabla cuando el enrutamiento ha convergido.

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table 4.8 Final distances stored at each node (global view).

ENRUTAMIENTO: VECTOR DISTANCIA

- ¿Cuándo cambian las tablas de enrutamiento?
 - Periódicamente -> cada cierto período de tiempo.
 - *Triggered* -> un nodo recibe información que hace que su tabla sea actualizada.



ENRUTAMIENTO: VECTOR DISTANCIA

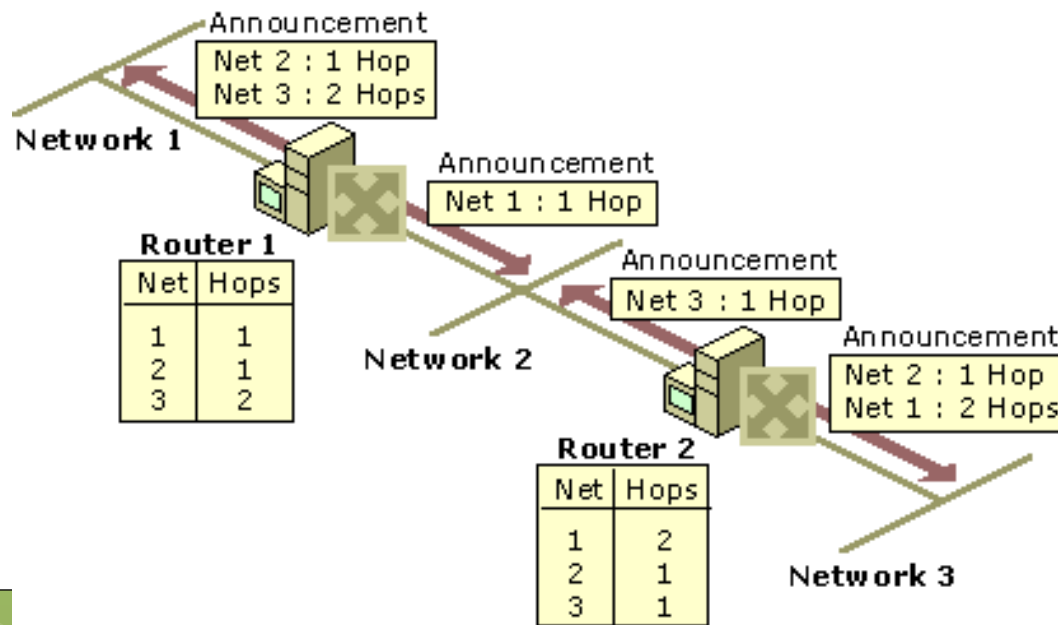
Problema del
Conteo Infinito

ENRUTAMIENTO: VECTOR DISTANCIA

- Solución 1:
 - Usar un pequeño número como una aproximación a infinito.
 - Por ejemplo, máximo número de saltos no puede ser mayor a 16.

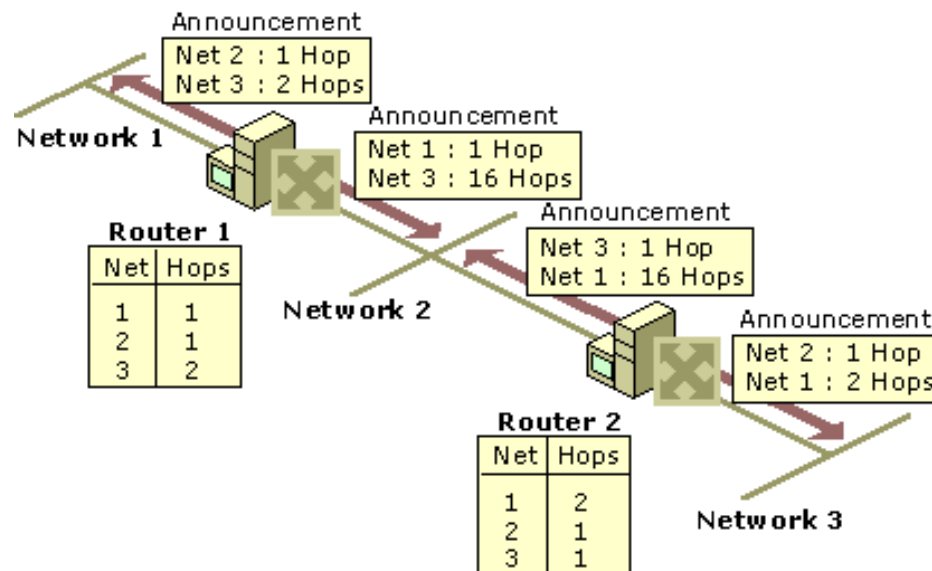
ENRUTAMIENTO: VECTOR DISTANCIA

- *Split horizon* no permite que los *routers* anuncien las redes en la dirección desde la cual esas redes fueron aprendidas.
- La única información enviada son para aquellas redes que están mas allá del *router* vecino en la dirección opuesta.
- Redes aprendidas del vecino no se incluyen.



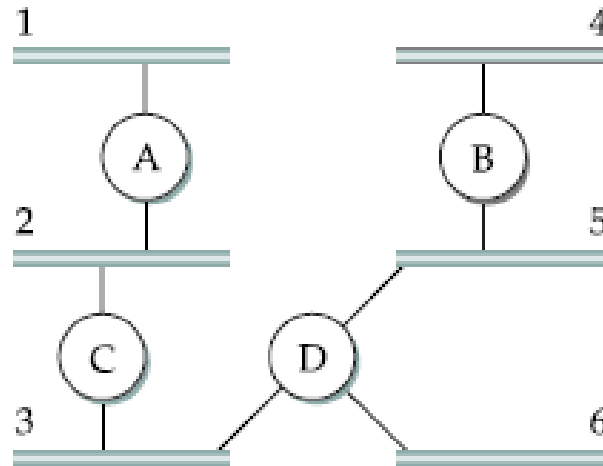
ENRUTAMIENTO: VECTOR DISTANCIA

- *Split horizon with poison reverse* difiere del anterior en que se anuncian todas las redes.
- Las redes aprendidas en una dirección dada se anuncian como infinitas (contador en 16) indicando que la red es inalcanzable.

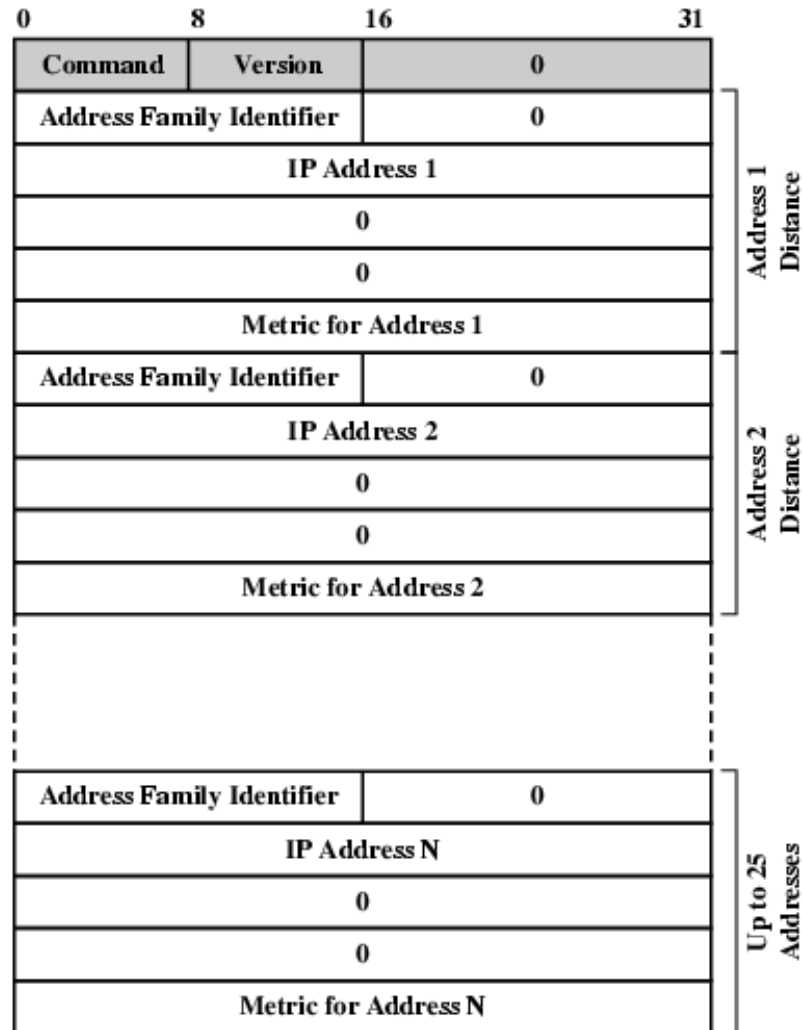


ENRUTAMIENTO: ROUTING INFORMATION PROTOCOL (RIP)

- Routers no se anuncian el costo de alcanzar otros routers sino otras redes.



ENRUTAMIENTO: ROUTING INFORMATION PROTOCOL (RIP)



ENRUTAMIENTO: ROUTING INFORMATION PROTOCOL (RIP)

- ◉ Command: 1=request 2=reply
- ◉ Versión: 1 o 2
- ◉ Familia de direccionamiento : 2 para IP
- ◉ Dirección IP: porción de la red no cero, porción del *host* cero
 - ◉ Identifica la red determinada
- ◉ Métrica
 - ◉ Distancia del camino de este *router* a la red
 - ◉ Típicamente 1, así que la métrica es el contador de saltos.

ENRUTAMIENTO: ROUTING INFORMATION PROTOCOL (RIP)

- Los enrutadores corren sus actualizaciones cada 30 s.
- Distancias válidas de 1 a 15 siendo 16 infinito.

ENRUTAMIENTO: ESTADO DEL ENLACE

- Cada nodo debe ser capaz de encontrar el estado de sus vecinos y el costo del enlace.
- Cada no do conoce como alcanzar sus vecinos conectados directamente.
- Cada nodo puede diseminar su conocimiento total de la red a cada nodo, para que tengan suficiente conocimiento de la red y construir la topología completa de la misma.
- Dos mecanismos existen:
 - Diseminación de la información de estado del enlace.
 - Cálculo de la rutas en base a la información acumulada recibida.

ENRUTAMIENTO: ESTADO DEL ENLACE

- Inundación Confiable
- Todos los nodos deben obtener información confiable de los demás nodos.
- La información es enviada a todos los vecinos directos de un nodo (*flooding*).
- Esto se hace hasta que todos los nodos reciben la información de todos los demás.

ENRUTAMIENTO: ESTADO DEL ENLACE

- ◉ link-state packet (LSP):
- ◉ Usado por cada nodo para diseminar su información.
- ◉ Compuesto de:
 - ◉ El ID del nodo que creo el LSP;
 - ◉ La lista de los vecinos conectados a ese nodo con su costo del enlace respectivo.
 - ◉ número de secuencia.
 - ◉ Tiempo de vida del paquete.

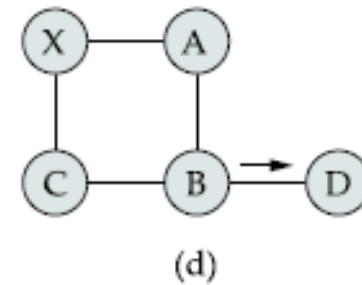
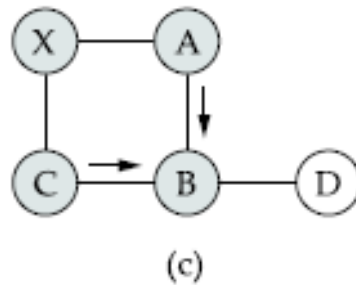
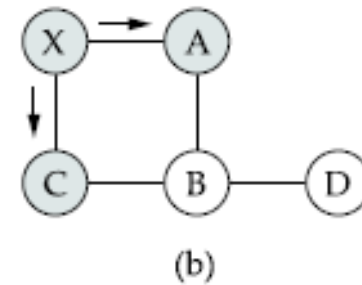
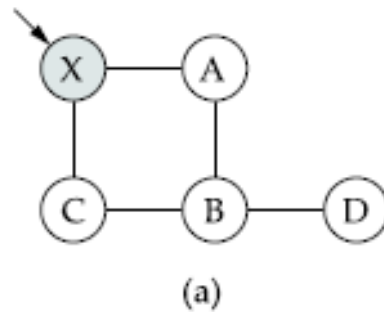
ENRUTAMIENTO: ESTADO DEL ENLACE

- La transmisión de LSPs entre nodos adyacentes se hace usando retransmisiones y ACKs (para la confiabilidad).

ENRUTAMIENTO: ESTADO DEL ENLACE

- El *flooding* trabaja de la siguiente forma:
 - Si X recibe una copia del LSP originado por Y:
 - Si hay una copia del LSP de Y:
 - Si el nuevo LSP tiene un número de sec mas largo, el nuevo LSP es almacenado (reemplaza al otro).
 - De lo contrario, descartar LSP.
 - Si el LSP recibido es el mas nuevo, X envía una copia a sus vecinos próximos excepto al vecino del cual fue recibido.
 - Este procedimiento garantiza que todos los nodos tendrán la copia mas reciente del LSP.

ENRUTAMIENTO: ESTADO DEL ENLACE



ENRUTAMIENTO: ESTADO DEL ENLACE

- Los LSPs son generados:
 - Periódicamente
 - Cuando cambia la topología (un enlace directo fallo o un vecino inmediato esta abajo).
- La pérdida de conectividad con un vecino es detectada a través de la transmisión de paquetes de HELLO.

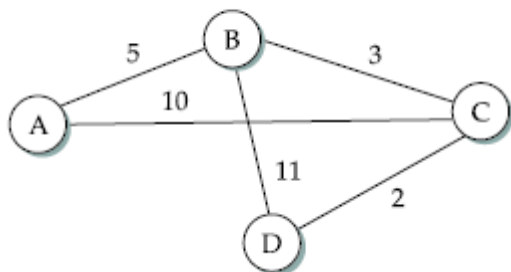
ENRUTAMIENTO: ESTADO DEL ENLACE

- Cada vez que un LSP se genera se genera un nuevo número de sec.
- El campo de sec es grande para evitar que los números se solapen.
- Cuando un nodo se cae, se inicia con un número de sec de 0.
- Si el nodo estuvo abajo por mucho tiempo, los LSPs viejos se borrarán (*timed out*).
- De lo contrario, el nodo recibirá un LSP con un número de sec mas alto.
- Esto asegura que los nuevos LSPs reemplazan a los viejos.
- Los LSPs tienen un tiempo de vida para asegurar que los viejos LSPs son removidos.

ENRUTAMIENTO: ESTADO DEL ENLACE

• Cálculo de la ruta

- 1 Initialize the **Confirmed** list with an entry for myself; this entry has a cost of 0.
- 2 For the node just added to the **Confirmed** list in the previous step, call it node **Next**, select its LSP.
- 3 For each neighbor (**Neighbor**) of **Next**, calculate the cost (**Cost**) to reach this **Neighbor** as the sum of the cost from myself to **Next** and from **Next** to **Neighbor**.
 - (a) If **Neighbor** is currently not on either the **Confirmed** or the **Tentative** list, then add (**Neighbor**, **Cost**, **NextHop**) to the **Tentative** list, where **NextHop** is the direction I go to reach **Next**.
 - (b) If **Neighbor** is currently on the **Tentative** list, and the **Cost** is less than the currently listed cost for **Neighbor**, then replace the current entry with (**Neighbor**, **Cost**, **NextHop**), where **NextHop** is the direction I go to reach **Next**.
- 4 If the **Tentative** list is empty, stop. Otherwise, pick the entry from the **Tentative** list with the lowest cost, move it to the **Confirmed** list, and return to step 2.



Step	Confirmed	Tentative	Comments
1	(D,0,-)		Since D is the only new member of the confirmed list, look at its LSP.
2	(D,0,-)	(B,11,B) (C,2,C)	D's LSP says we can reach B through B at cost 11, which is better than anything else on either list, so put it on Tentative list; same for C.
3	(D,0,-) (C,2,C)	(B,11,B)	Put lowest-cost member of Tentative (C) onto Confirmed list. Next, examine LSP of newly confirmed member (C).
4	(D,0,-) (C,2,C)	(B,5,C) (A,12,C)	Cost to reach B through C is 5, so replace (B,11,B). C's LSP tells us that we can reach A at cost 12.
5	(D,0,-) (C,2,C) (B,5,C)	(A,12,C)	Move lowest-cost member of Tentative (B) to Confirmed , then look at its LSP.
6	(D,0,-) (C,2,C) (B,5,C)	(A,10,C)	Since we can reach A at cost 5 through B, replace the Tentative entry.
7	(D,0,-) (C,2,C) (B,5,C) (A,10,C)		Move lowest-cost member of Tentative (A) to Confirmed , and we are all done.

Table 4.9 Steps for building routing table for node D (Figure 4.18).

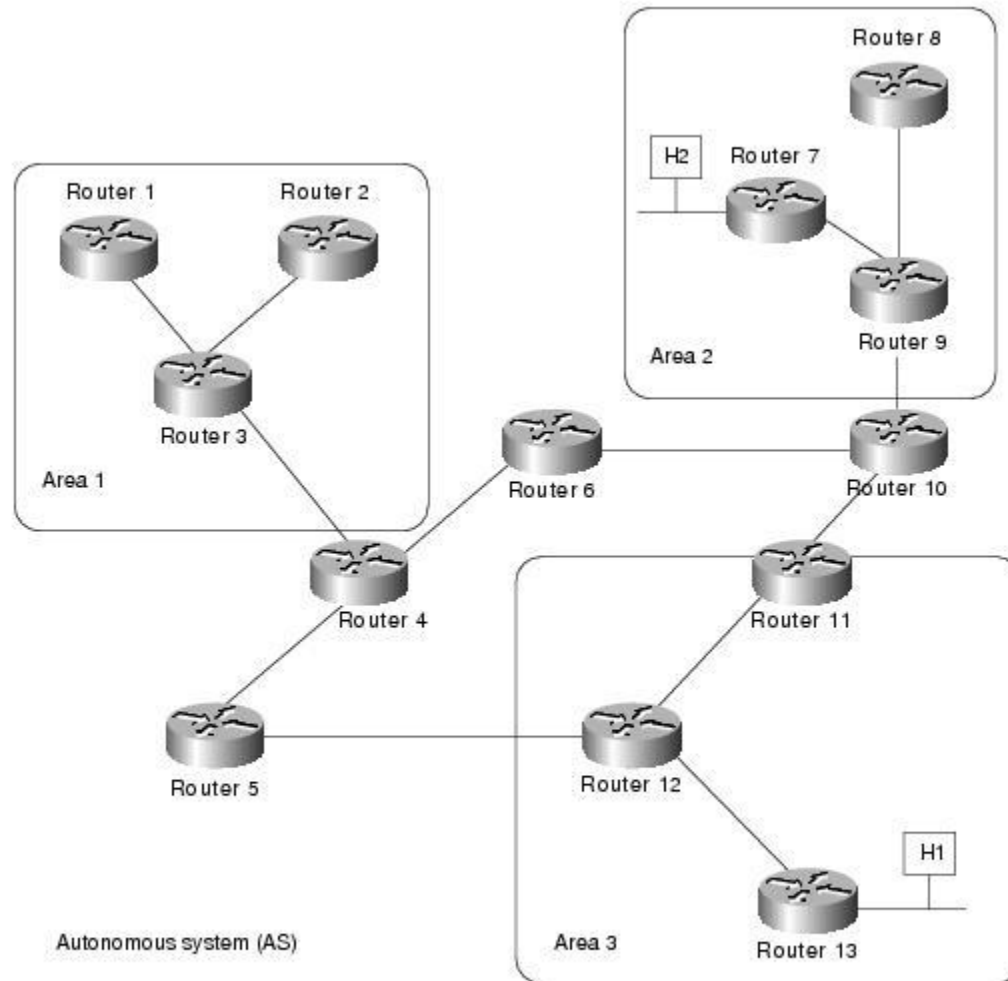
ENRUTAMIENTO: ESTADO DEL ENLACE

- Diferencias entre vector distancia y estado del enlace:
 - En vector distancia, cada nodo habla con sus vecinos directamente conectados, para anunciarles lo aprendido.
 - En enlace de estado, cada nodo habla con los otros para decirle solo lo que conoce (solo el estado de sus enlaces directamente conectados).

ENRUTAMIENTO: Open Shortest Path First Protocol (OSPF)

- Enrutamiento basado en estado del enlace
- Características
 - **Autenticación para los mensajes** -> por password, autenticación basada en cifrado.
 - **Jerarquía adicional** -> los dominios son particionados en áreas.
 - Un router no tiene que conocer como alcanzar cada red en un dominio, le basta con conocer como llegar al área correcta.
 - **Balanceo de carga:** distribuir cargas en múltiples caminos a un mismo destino.

ENRUTAMIENTO: Open Shortest Path First Protoc



Open Shortest Path First (OSPF): Paquete

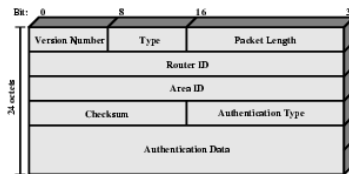


Figure 15.12 OSPF Packet Header

- Número de versión: 3 es la actual.
- Tipo: uno de 5
- Longitud del paquete: en octetos incluyendo cabecera.
- Identificación del *router*: fuente de este paquete, 32 bits.
- Identificación de área: Área a la cual el *router* de la fuente pertenece.
- Tipo de la autenticación: password simple, nula o cifrado,
- Datos de autenticación: utilizado por procedimiento de la autenticación

Open Shortest Path First (OSPF): Tipos de paquetes

- **Hello:** utilizado en descubrimiento del vecino
- **Descripción de la base de datos:** define el conjunto de información del estado de la conexión presente en cada base de datos del *router*
- **Link state request:** requiere de pedazos de la base de datos topológica de los *routers* vecinos. Son intercambiados después que un *router* descubre que parte de su base de datos topológica esta des actualizada.
- **Link state update:** responde a un paquete de LSR. Usado también para envíos regulares de *link-state advertisements (LSAs)*. Varios LSAs pueden estar en un LSU.
- **Link state acknowledgement:** ACKs de los LSUs.

BORDER GATEWAY PROTOCOL (BGP)

IANA

- Ya que Internet no tiene dueño, hay una necesidad de que ciertos aspectos sean coordinados.
- La Internet Assigned Numbers Authority (IANA):
 - Responsable por coordinar algunos elementos claves en lo que se refiere a enrutamiento en Internet.
 - Mantiene y reserva códigos únicos y sistemas de numeración usados en documentos estándares.

IANA

- Actividades de IANA:
 - Nombres de Dominio -> DNS root, dominios .arp y .arpa.
 - Número de recursos -> pool de direcciones IP y números de AS.
 - Asignación de protocolos -> sistema de numeración de los protocolos de Internet.

REGIONAL INTERNET REGISTRY (RIR)



Registry	Area Covered
AfriNIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Ver <http://www.iana.org/numbers/>

SISTEMA AUTONOMO: AUTONOMOUS SYSTEM (AS)

- La definición clásica de un sistema autónomo es un conjunto de routers bajo una administración única, utilizando un *interior gateway protocol* y métricas comunes para enrutar los paquetes dentro del AS, y utilizando un *exterior gateway protocol* para encaminar los paquetes a otros sistemas autónomos.

SISTEMA AUTONOMO: AUTONOMOUS SYSTEM (AS)

- Desde que esta definición clásica se desarrolló, se ha hecho común para un solo AS utilizar varios IGPs y a veces, varios conjuntos de parámetros dentro de un AS. El uso del término Sistema Autónomo aquí destaca el hecho de que, aun cuando se utilizan múltiples IGPs y métricas, la administración de un AS le hace creer a otros ASs que tiene un simple plan de enrutamiento único y coherente y presenta una imagen coherente de que redes son accesibles a través de él [RFC 1930].

SISTEMA AUTONOMO: AUTONOMOUS SYSTEM (AS)

- Lo anterior se puede resumir en lo siguiente:
- *Un AS es un grupo conectado de uno o más prefijos IP a cargo de uno o más operadores de red que tienen una única y claramente definida política de enrutamiento [RFC 1930].*

SISTEMA AUTONOMO: AUTONOMOUS SYSTEM (AS)

- El espacio de números usados para identificar un AS es de 2 octetos (16 bits).
- Esto limita el espacio a 65536 únicos números de AS [RFC 1930].
- Actualmente se esta trabajando en un espacio e números de 32 bits [RFC 4893].
- La asignación de números de AS según IANA se encuentra en:
- <http://www.iana.org/assignments/as-numbers/as-numbers.xml>

ASs: TIPOS

- *Stub AS*: un AS que tiene sólo una única conexión a otro AS, tal que un AS sólo se llevará a tráfico local.
- *Multihomed AS*: un AS que tiene conexiones a más de un AS, pero que se niega a llevar tráfico de tránsito.
- *Tránsito AS*: un AS que tiene conexiones a más de un AS y que es diseñada para llevar el tráfico de tránsito y el local.

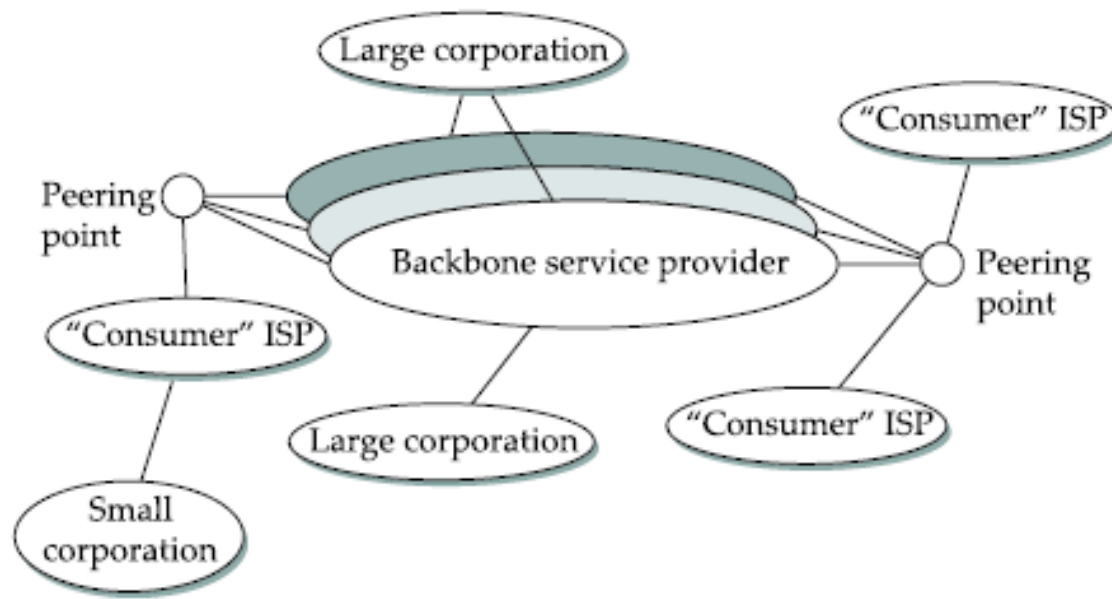
POLITICAS DE ENRUTAMIENTO: EJEMPLO

- Siempre que sea posible, prefiero enviar tráfico a través de AS X que a través de AS Y, pero voy a utilizar AS Y si es el único camino, y no quiero llevar tráfico procedente del AS X a AS Y o viceversa.

PROTOCOLOS DE ENRUTAMIENTO EXTERIORES

- ◉ Exterior Gateway Protocol (EGP):
 - ◉ Tiene limitaciones.
 - ◉ La principal considerar la topología de Internet como un árbol.
- ◉ Border Gateway Protocol (BGP):
 - ◉ Vino en sustitución del anterior.

INTERNET HOY



METAS DE LOS PROTOCOLOS DE ENRUTAMIENTO INTERDOMINIOS

- Encontrar un camino libre de loops.
- El camino debe estar de acuerdo a las políticas de enrutamiento de varios ASs.
 - Entonces se requiere calcular un camino que cumpla con las políticas y sea libre de loops.
- Debe ser capaz de enrutar paquetes a cualquier sitio en Internet significa tablas muy grandes.

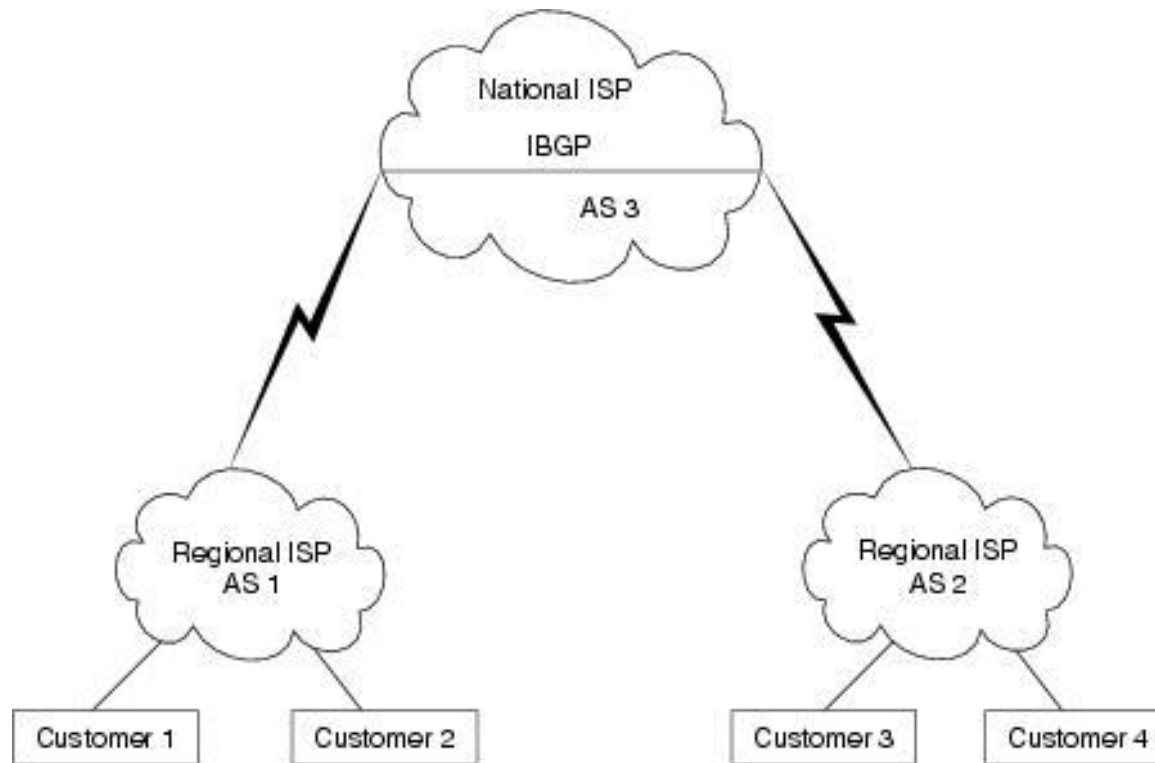
METAS DE LOS PROTOCOLOS DE ENRUTAMIENTO INTER DOMINIOS

- Calcular un camino óptimo que cruce muchos ASs que usan diferentes protocolos de enrutamiento internos es prácticamente imposible.
 - Entonces enrutamiento inter dominio solo anuncia alcanzabilidad.
- Confianza -> poder confiar que un router puede anunciar información correcta.

BGP

- Border Gateway Protocol (BGP) es un protocolo de enrutamiento entre sistemas autónomos.
- Cuando se usa para el enrutamiento entre sistema autónomos se llama EBGp.
- Cuando se usa dentro de un mismo AS se llama IBGP.
- Es el protocolo de enrutamiento actualmente usado en Internet.
- Especificado en RFC 1771.

IBGP VS EBG

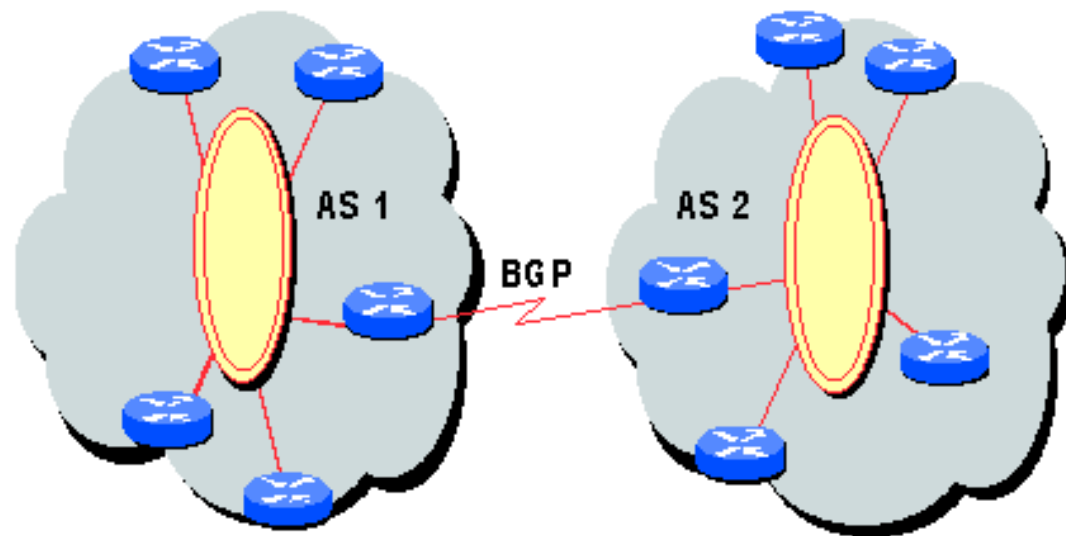


BGP

- Selecciona rutas de forma inteligente basado en prefijos y el camino de AS mas corto.
- Usa *classless interdomain routing (CIDR)* .
- Actualmente BGP versión 4.
- Usado para transportar información entre ASs.
- Protocolo de vector camino -> anuncia caminos completos como una lista de ASs para alcanzar una red particular.
- Usa TCP (179).
- Lleva información acerca de la topología de camino de AS.

BGP

► BGP Between AS's



BGP

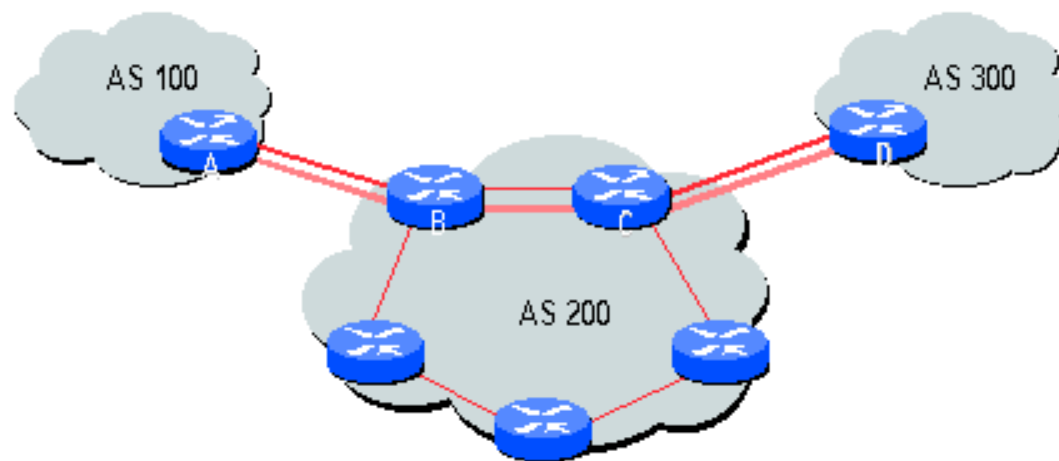
- Aprende sobre múltiples caminos vía BGP *speakers* internos y externos.
- Selecciona el mejor camino y los instala en la tabla de *forwarding*.
- Las políticas que se apliquen influenciarán la selección del mejor camino.

BGP: CUANDO USARLO

- Dual o multihomed -> *multihoming* implica que hay múltiples caminos para alcanzar un “home” destino.
- Proporcionar parcial o full enrutamiento a Internet a clientes *dowstream*.
- En cualquier momento que información sobre un camino AS es requerido.

BGP

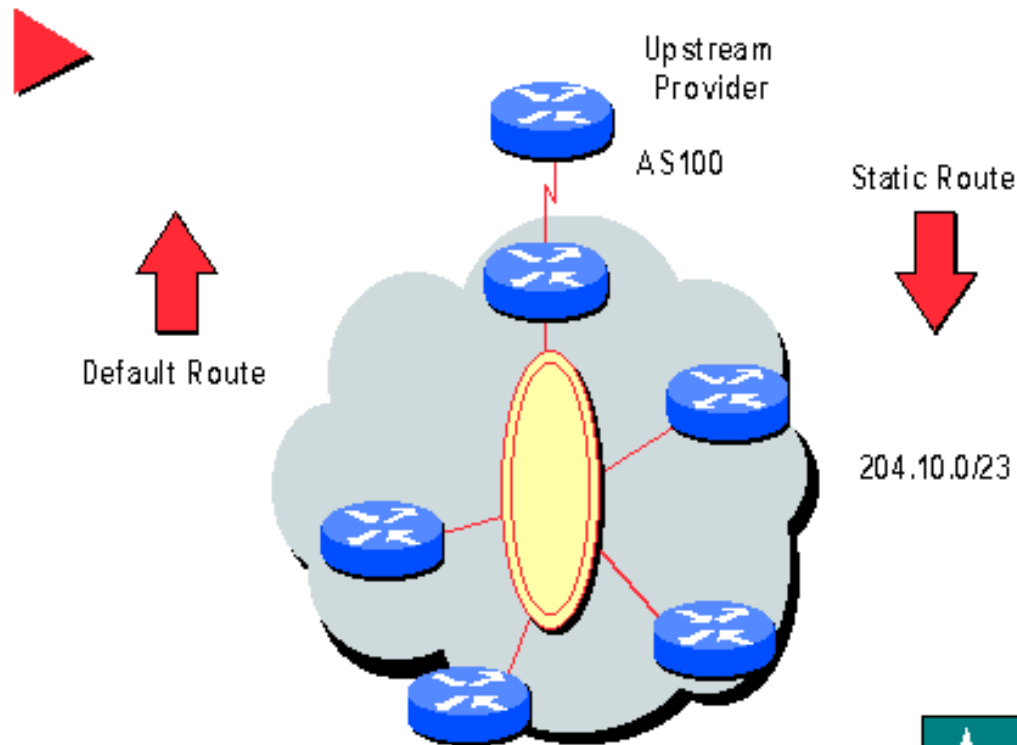
► Multi-Homed AS



BGP: CUANDO ES NO REQUERIDO

- Cuando *simple homed*.
- Si no hay enrutamiento *dowstream*.
- Usar la ruta por defecto.

BGP: CUANDO ES NO REQUERIDO



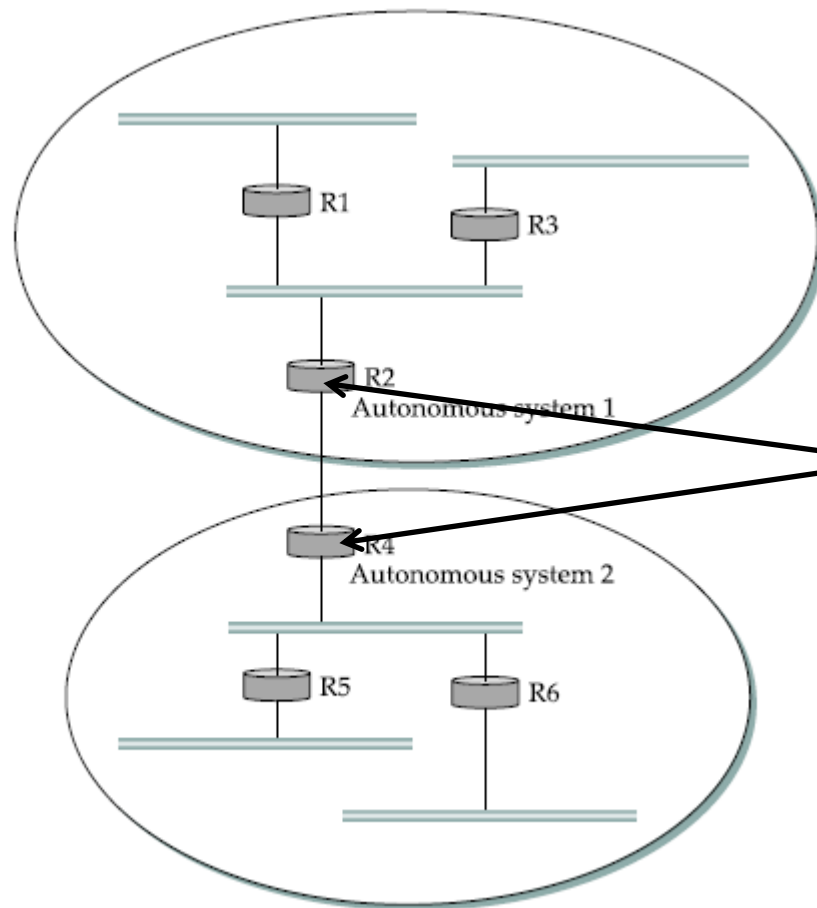
BGP SPEAKER

- ◉ Es el interlocutor para el AS entero.
- ◉ El speaker establece sesiones BGP con otros *speakers* en otros ASs.
- ◉ Las sesiones permiten intercambiar información entre Ass.
- ◉ Son establecidos administrativamente.

BORDER GATEWAYS

- Routers a través del cual los paquetes entran y salen de un AS.
- No necesariamente son los *speakers*.

BORDER GATEWAYS



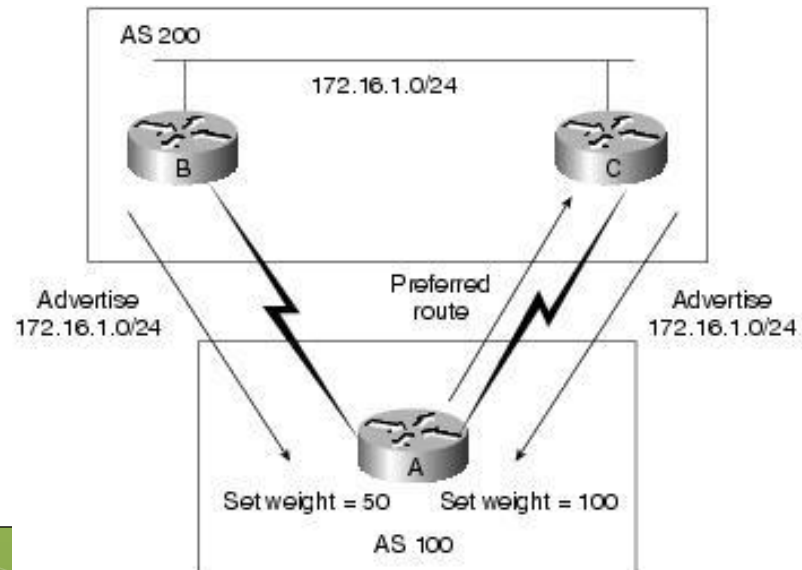
Border gateways

BGP: ATRIBUTOS

- Son las propiedades usada para determinar la mejor ruta a una destino cuando existen múltiples caminos.
 - Weight
 - Local preference
 - Multi-exit discriminator
 - Origin
 - AS_path
 - Next hop
 - Community

BGP: ATRIBUTOS

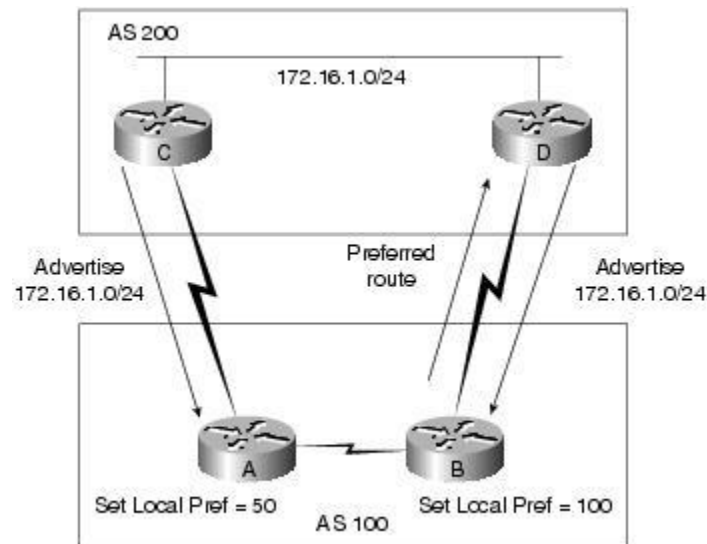
- ⦿ *Weight*
 - Es definido por CISCO.
 - Es local.



BGP: ATRIBUTOS

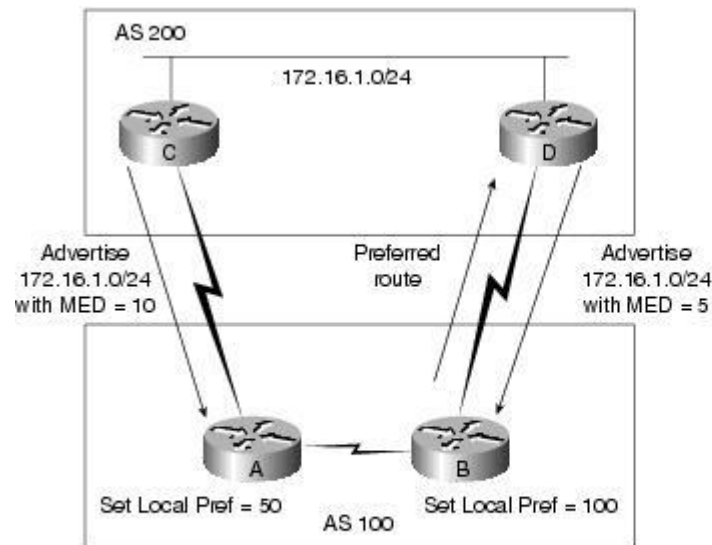
◎ *Local preference*

- Usado para elegir un punto de salida desde un AS.
- A diferencia del anterior puede ser intercambiado entre routers dentro de un AS.



BGP: ATRIBUTOS

- *Multi-exit discriminator (MED)*
 - Es una sugerencia del AS externo para el AS, que puede influenciar la elección de la ruta.

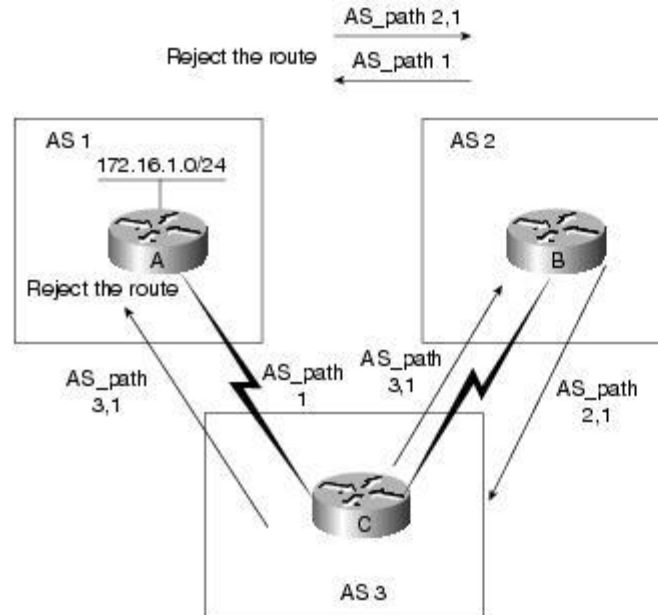


BGP: ATRIBUTOS

- ◉ *Origin Attribute*
- ◉ Indica como un router aprende una ruta en particular.
 - ◉ **IGP** – la ruta es interna al AS de origen.
 - ◉ **EGP** – la ruta es aprendida vía del Exterior Border Gateway Protocol (EBGP).
 - ◉ **Incomplete** – el origen de la ruta es desconocida o aprendida de alguna otra forma.

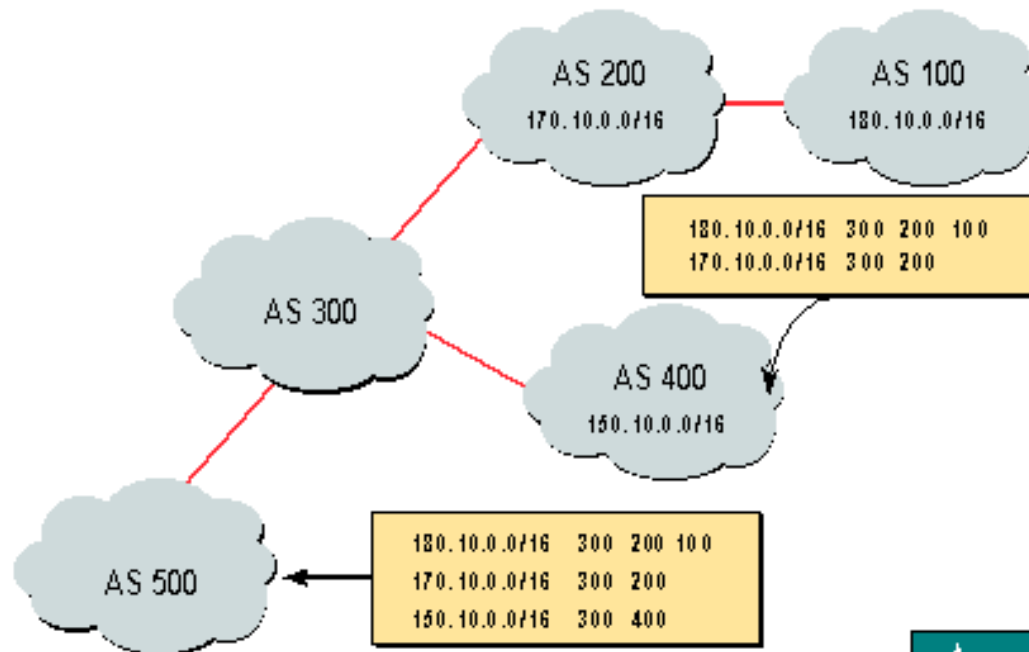
BGP: ATRIBUTOS

- Camino de ASs
 - Secuencia de ASs que se han cruzado.



BGP: ATRIBUTOS

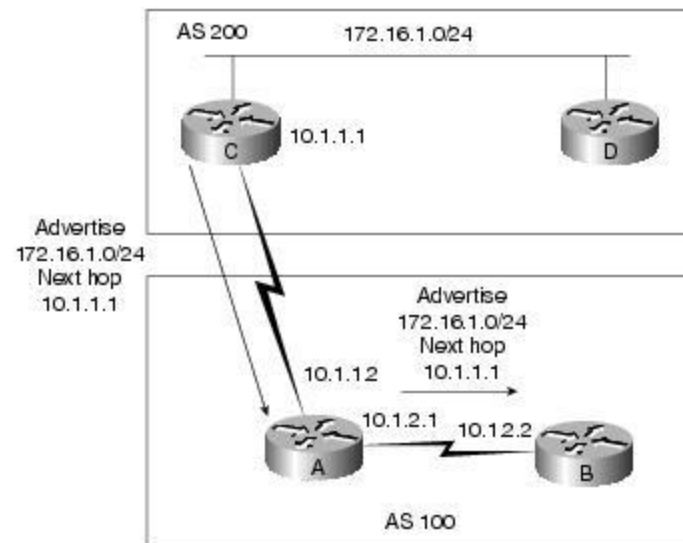
▶ AS-Path



BGP: ATRIBUTOS

- *Próximo-Salto*

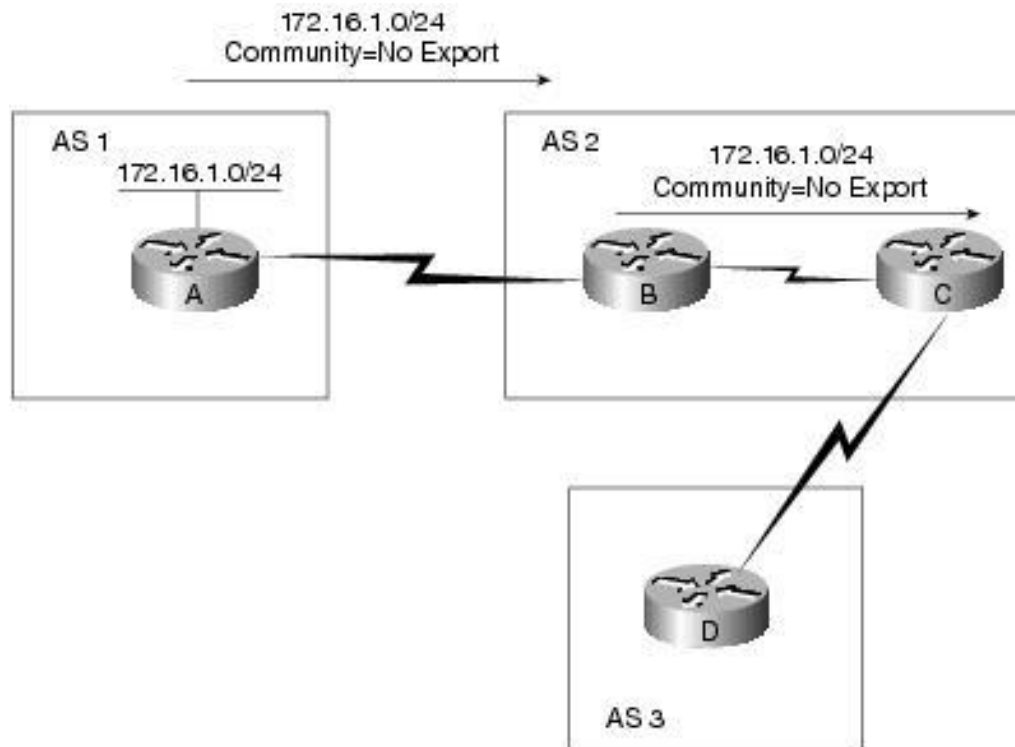
- Es la dir IP usada para alcanzar el router anunciado.
- Próximo salto para alcanzar una red.



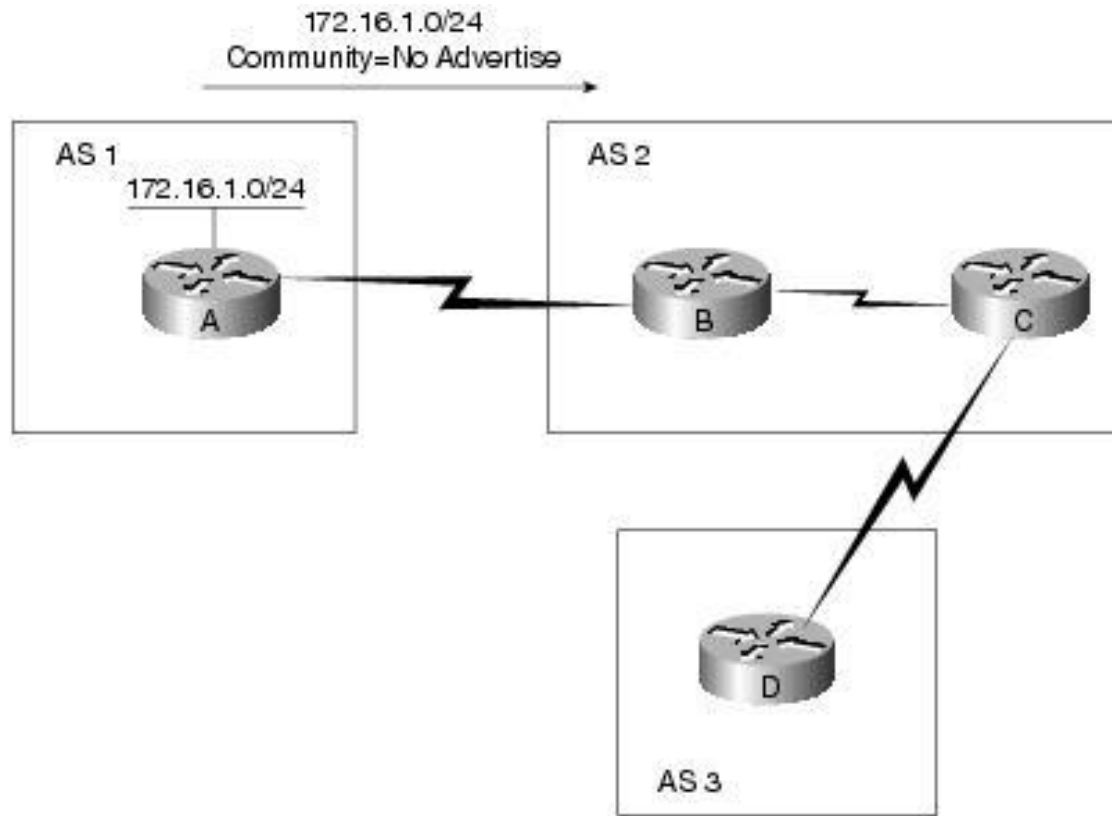
BGP: ATRIBUTOS

- *Comunidad*
 - Proporciona una forma de agrupar destinos.
 - Para las cuales las decisiones de enrutamiento pueden ser aplicadas.
 - Algunos atributos predefinidos son:
 - **no-export** – no anunciar esta ruta a ningún EBGp par.
 - **no-advertise** - no anunciar esta ruta a ningún par.
 - **internet** – anunciar esta ruta a la comunidad de Internet.

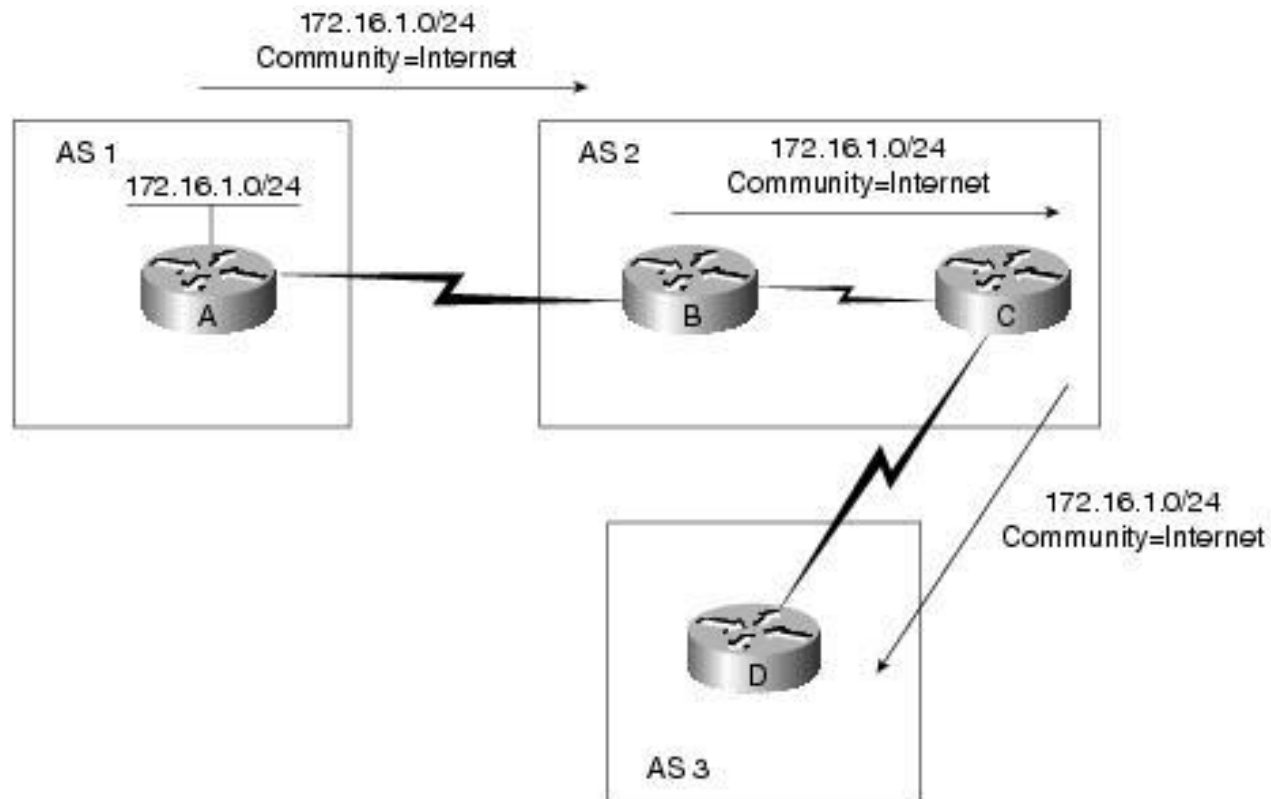
BGP: ATRIBUTOS



BGP: ATRIBUTOS



BGP: ATRIBUTOS



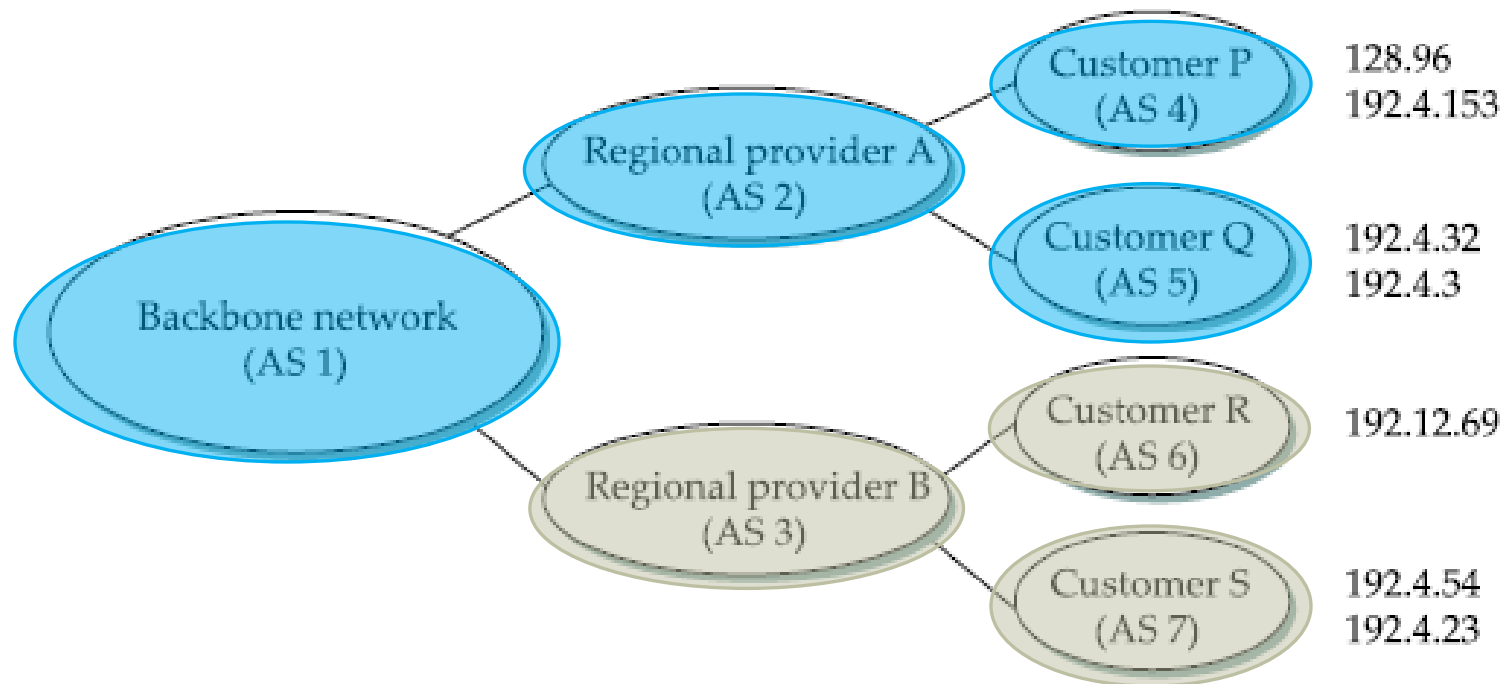
BGP: FUNCIONAMIENTO GENERAL

- Asuma que los proveedores son AS de tránsito y los clientes son *stubs*.
- Un BGP speaker para el AS del proveedor A (AS 2) debe ser capaz de anunciar alcanzabilidad para los números asignados a los clientes P y Q.

BGP: FUNCIONAMIENTO GENERAL

- Ejemplo:
- Las redes 128.96, 192.4.153, 192.4.32, y 192.4.3 pueden ser alcanzadas desde AS 2.
- El *backbone* puede anunciar esto después de recibir el anuncio del AS 2.
- Las redes 128.96, 192.4.153, 192.4.32, and 192.4.3 pueden ser alcanzados por el camino AS 1, AS 2
- Las redes 192.12.69, 192.4.54, y 192.4.23 pueden ser alcanzadas por el camino AS 1, AS 3.

BGP: FUNCIONAMIENTO GENERAL



BGP: FUNCIONAMIENTO GENERAL

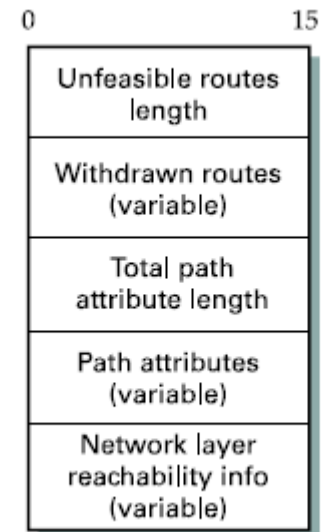
- Prevenir loops:
- Se anuncia el camino completo en los mensajes de enrutamiento.
- Por ejemplo, un anuncio recibido por AS 2 de AS 3 contiene un camino (AS 3, AS 1, AS 2).

BGP: CONSIDERACIONES

- ◉ Un determinado AS sólo anuncia rutas que considera suficiente buenas por sí mismo:
 - ◉ de acuerdo a sus propias políticas locales
- ◉ Un BGP speaker no tiene la obligación de anunciar cualquier ruta a un destino, incluso si tiene una:
 - ◉ un AS puede aplicar una política de no facilitar el tránsito.
 - ◉ puede negarse a anunciar las rutas de los prefijos que no son contenida dentro de ese AS.

BGP: CONSIDERACIONES

- Un *BGP speaker* puede cancelar caminos previamente anunciados:
 - withdrawn route*.



Mensaje de actualización

BGP: CONSIDERACIONES

- Las rutas que son anunciadas siguen el formato:
 - Prefijo
 - Longitud
- Ejemplo:
 - 192.4.16/20

VISTA DE RUTAS USANDO
<http://bgp.he.net>



HURRICANE ELECTRIC
INTERNET SERVICES




Search

AS19192 Universidad Central de Venezuela

Quick Links

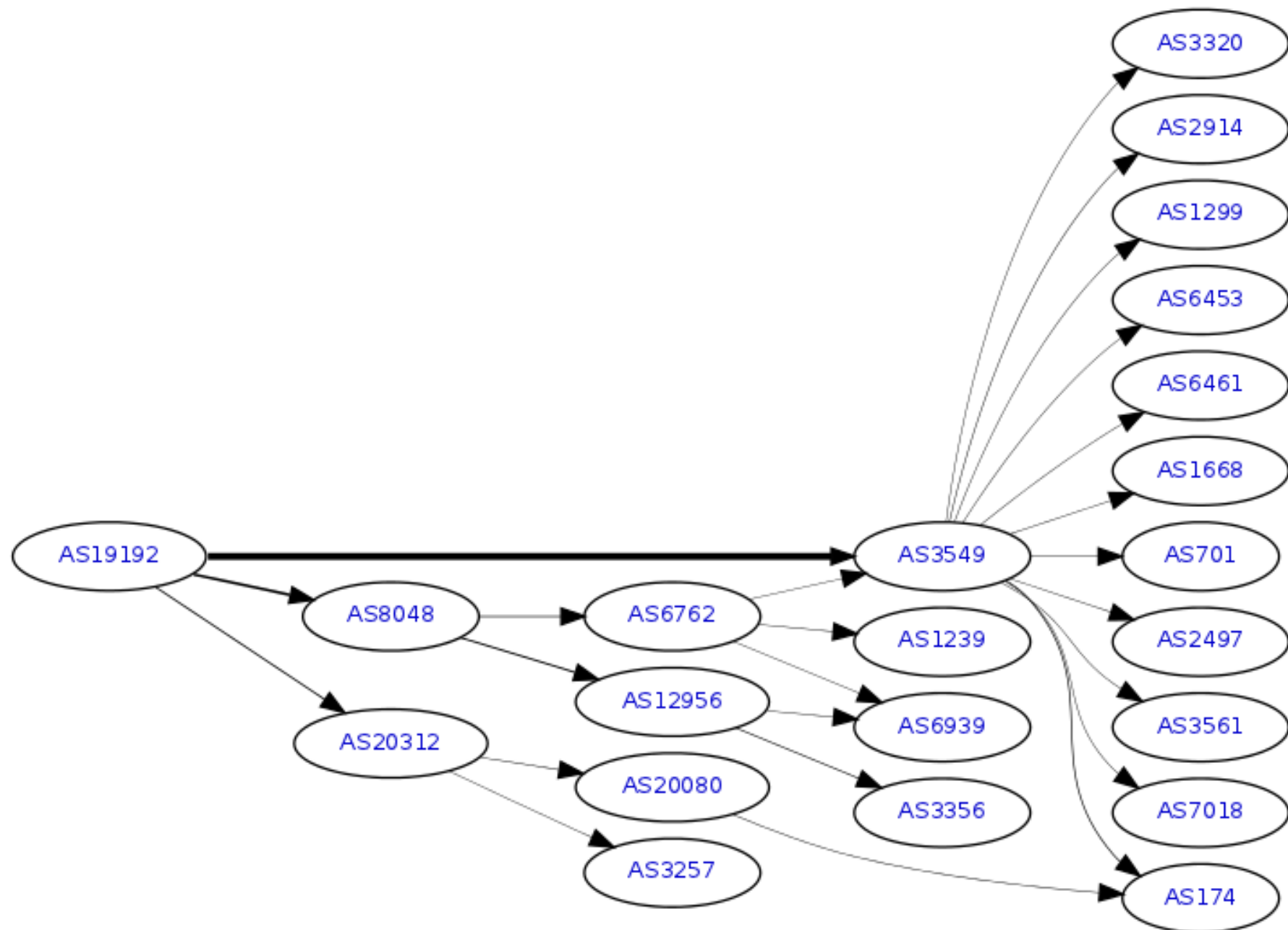
[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Bogon Routes](#)
[World Report](#)
[Multi Origin Routes](#)
[DNS Report](#)
[Top Host Report](#)
[Internet Statistics](#)
[Looking Glass](#)
[Free IPv6 Tunnel](#)
[IPv6 Certification](#)
[IPv6 Progress](#)
[Going Native](#)
[Contact Us](#)

[AS Info](#) [Graph v4](#) [Graph v6](#) [Prefixes v4](#) [Prefixes v6](#) [Peers v4](#) [Peers v6](#) [Whois](#) [IRR](#)

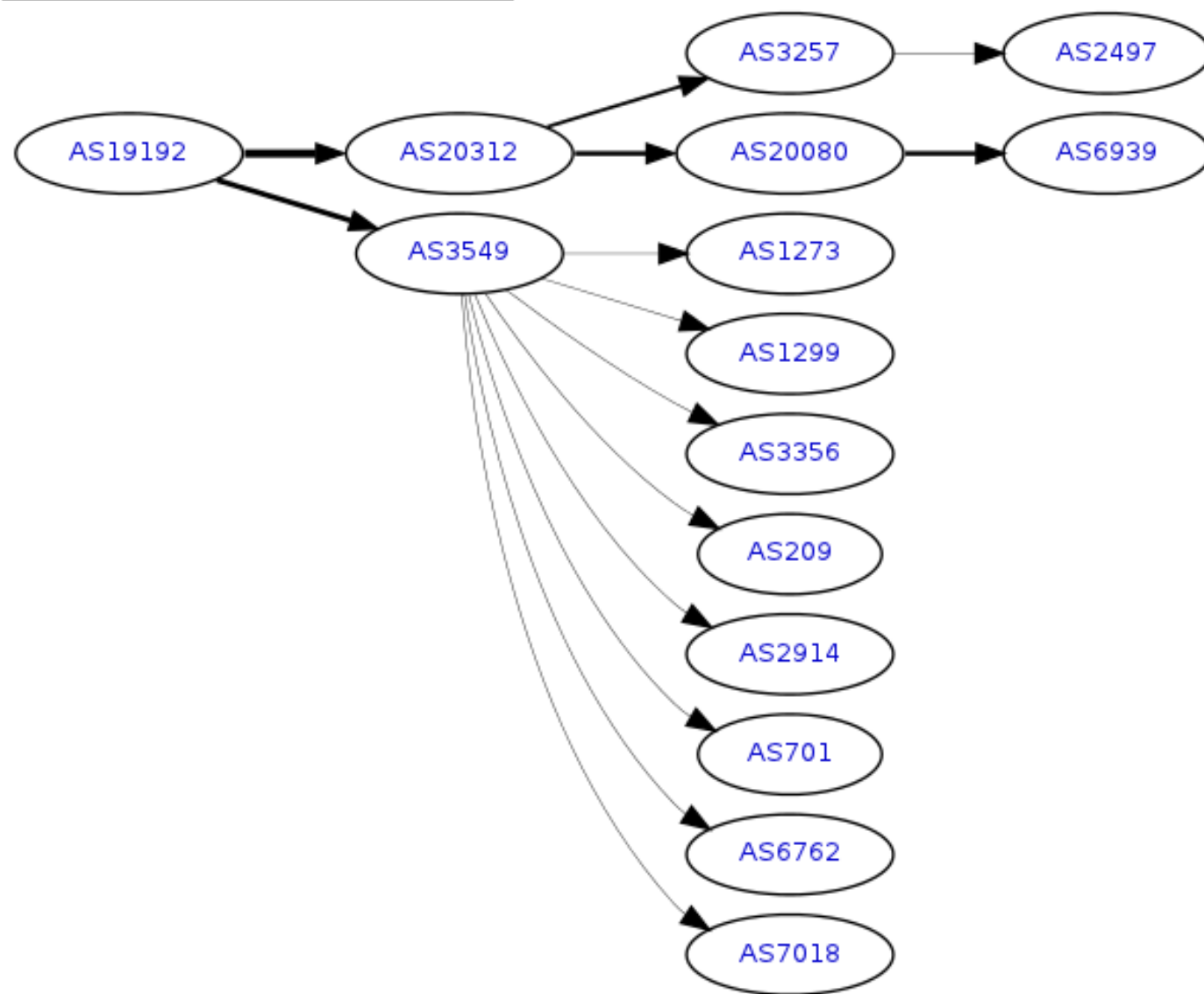
Prefix	Description
150.185.64.0/19	Early registration addresses 
190.169.0.0/16 	Universidad Central de Venezuela 

Updated 17 Jun 2012 06:52 PST © 2012 Hurricane Electric




AS19192 IPv4 Route Propagation



AS19192 IPv6 Route Propagation






AS Info Graph v4 Graph v6 Prefixes v4 Prefixes v6 Peers v4 Peers v6 Whois IRR

Rank	Description	IPv6	Peer
1	Level 3 Communications, Inc. (GBLX) 	X	AS3549
2	CANTV Servicios, Venezuela 		AS8048
3	Fundación Centro Nacional de Innovación Tecnológica (CENIT) 	X	AS20312
4	Fundación Centro Nacional de Innovación Tecnológica (CENIT) 	X	AS27807

Updated 17 Jun 2012 06:52 PST © 2012 Hurricane Electric

[AS Info](#)[Graph v4](#)[Graph v6](#)[Prefixes v4](#)[Prefixes v6](#)[Peers v4](#)[Peers v6](#)[Whois](#)[IRR](#)

Rank	Description	IPv4	Peer
1	Fundación Centro Nacional de Innovación Tecnológica (CENIT) 	X	AS20312
2	Level 3 Communications, Inc. (GBLX) 	X	AS3549
3	Fundación Centro Nacional de Innovación Tecnológica (CENIT) 	X	AS27807

Updated 17 Jun 2012 06:52 PST © 2012 Hurricane Electric