Capa de Red

Redes de Computadores

FIEC04705

Sesión 13

Agenda

- Terminología
- Ejercicios de Subnetting
- ARP
- IPv6

Terminología

Terminología

- **ICMP** - Internet Control Message Protocol: Un protocolo en la suite TCP/IP que maneja mensajes de error y de control.
- **RFC** - Request for Comments es un documento publicado por la Internet Engineering Task Force (IETF) describiendo métodos, comportamiento, investigaciones, u otras innovaciones aplicables al Internet y sistemas conectados al Internet.

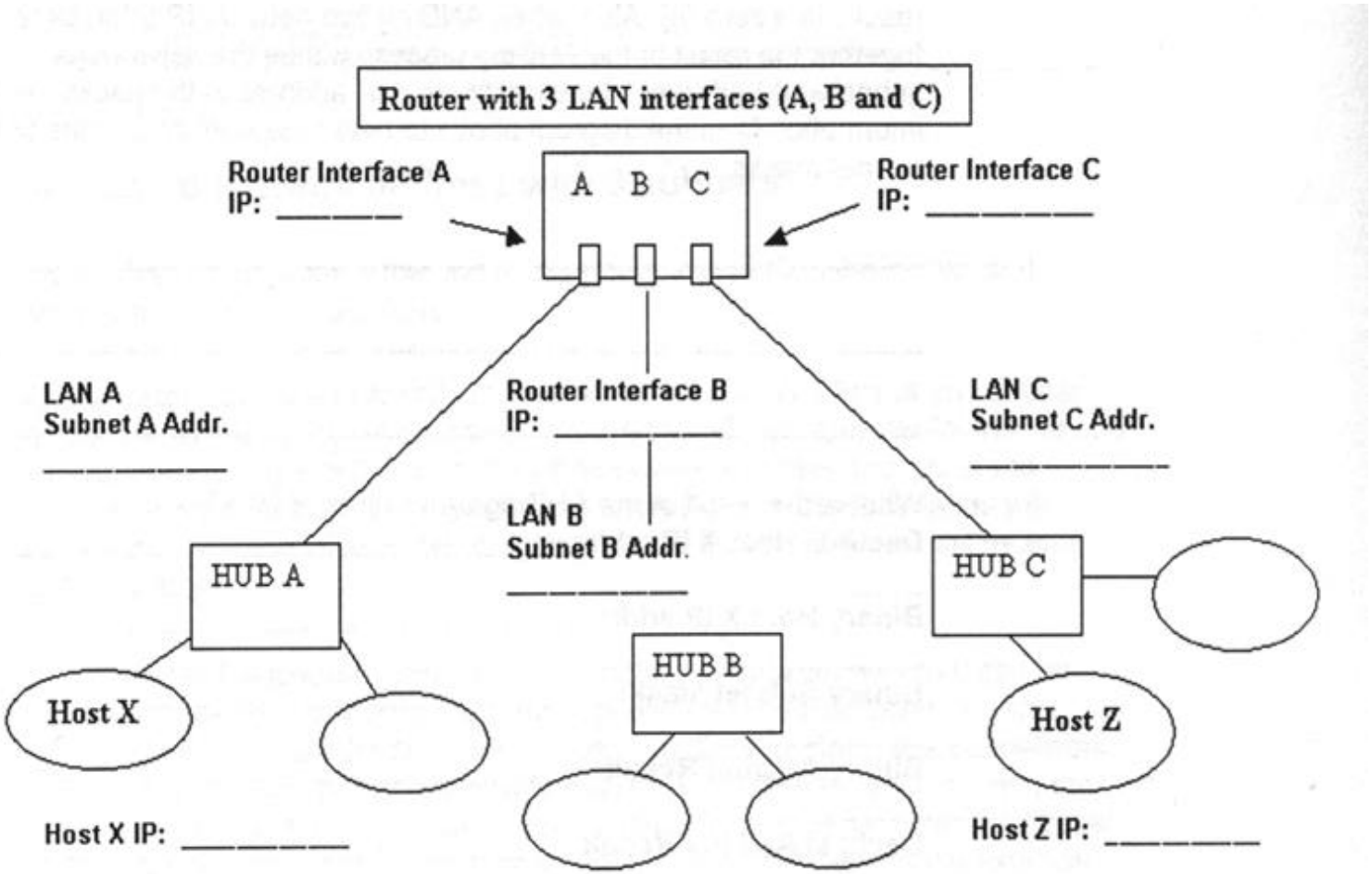
Terminología

- **NAT** - Network Address Translation: Una tecnología que permite a una red privada utilizar un conjunto de redes privadas para comunicación interna y un conjunto de direcciones globales de Internet para comunicaciones externas.
- **IGMP** - Internet Group Management Protocol: Un protocolo en la suite TCP/IP que maneja el multicasting.

Subnetting: Ejercicio #1

- A una organización se le asigna el bloque 130.56.0.0/16. El administrador requiere crear una subred para cada uno de los 1024 departamentos en la organización.
  - Especifique la máscara de subred
  - Especifique el número de direcciones de host en cada subred
  - Especifique la primera y última dirección de host en la primera subred
  - Especifique la primera y última dirección de host en la última subred
  - Si se toman las tres primeras subredes: A, B y C, como se indica en la figura, llene en los espacios en blanco las direcciones IP y de red correctas.

Subnetting: Ejercicio #1



Subnetting: Ejercicio # 2

- Dada la dirección IP *172.18.71.2* y la máscara de subred *255.255.248.0*, obtenga la dirección de red y la dirección de broadcast de la subred de este host.

Subnetting: Ejercicio # 3

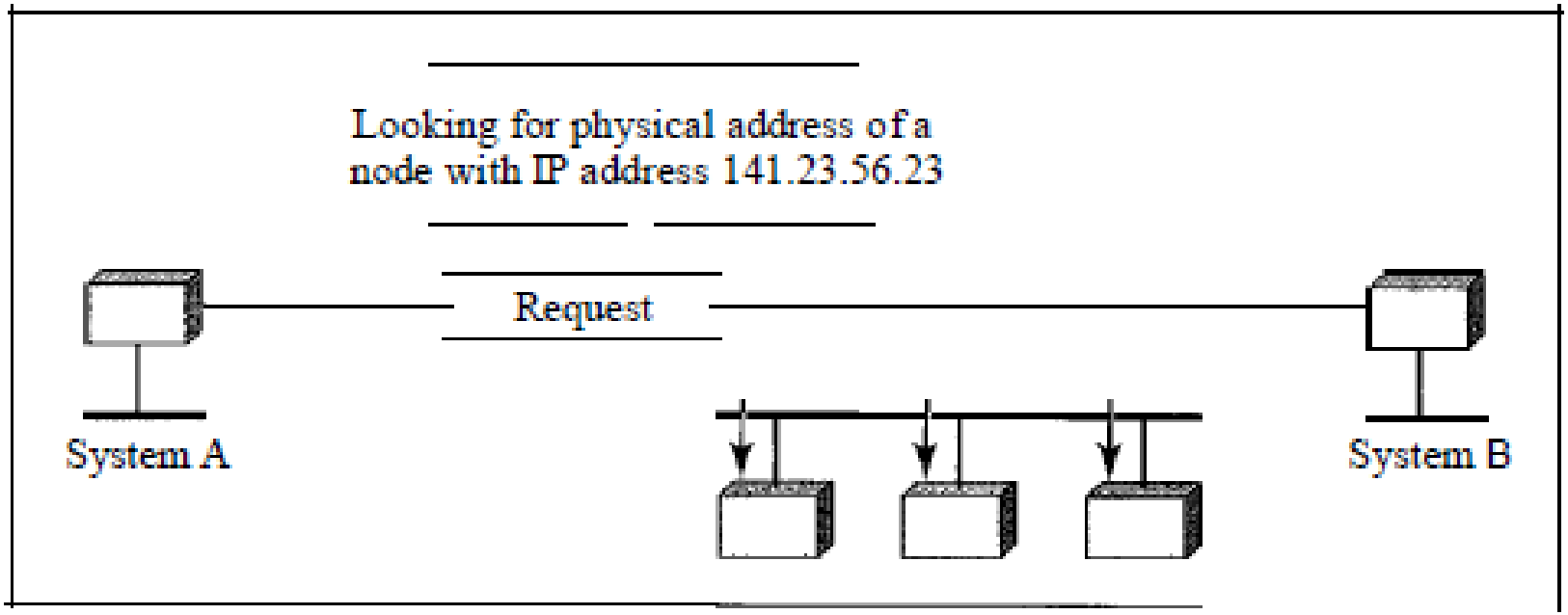
- Determine si la dirección *212.10.14.63 / 27* es una dirección de host, red, broadcast o inválida.

Subnetting: Ejercicio # 4

- Considere la dirección *10.6.165.0* y la máscara *255.255.224.0*. Muestre el rango de direcciones de hosts disponibles en la subred.

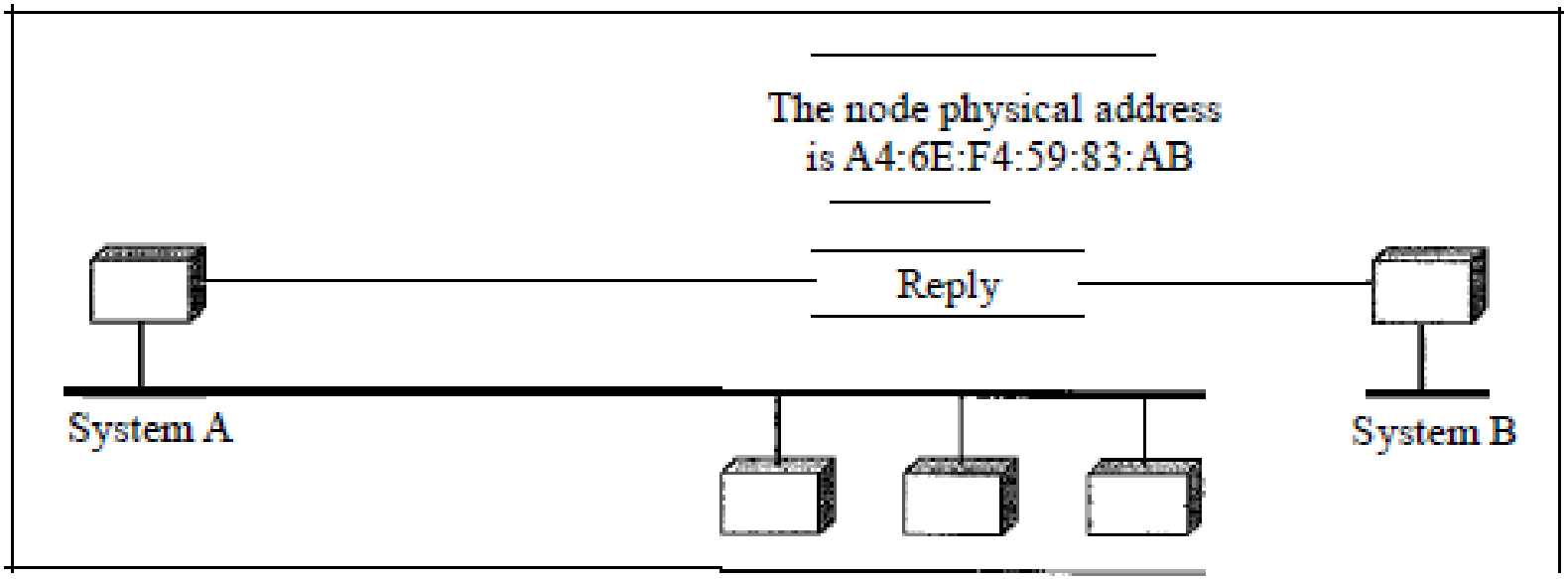
Mapeo de direcciones

Mapeo de direcciones



a. ARP request is broadcast

Mapeo de direcciones



b. ARP reply is unicast

Address Resolution Protocol (ARP)

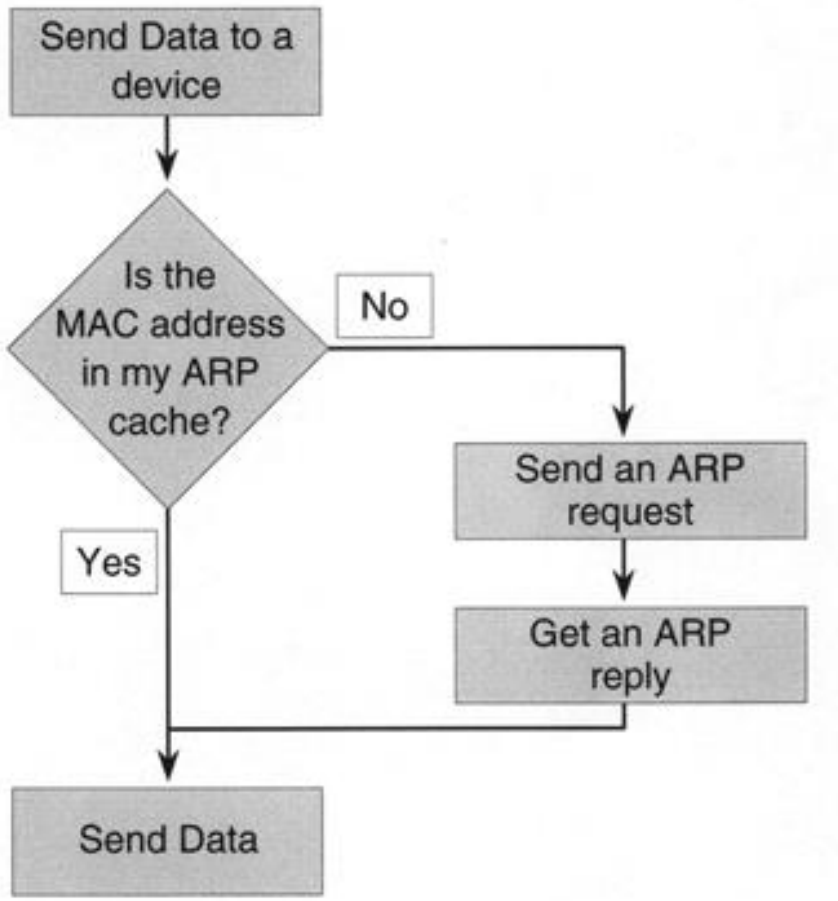
ARP

- Un paquete de datos debe contener una dirección MAC de destino y una dirección IP de destino. Luego que los dispositivos determinan las direcciones IP de los dispositivos de destino, ellos agregan la dirección MAC de destino a los paquetes de datos.
- Diferentes técnicas para determinar las direcciones MAC: Address Resolution Protocol (ARP), uno de ellos (RFC 826).

ARP

- Cada computadora en la red mantiene su propia tabla ARP la cual mapea direcciones IP a las correspondientes direcciones MAC. Las tablas ARP están en la memoria caché de cada dispositivo.

ARP


Send Data to a device
Is the MAC address in my ARP cache?
No
Yes
Send an ARP request
Get an ARP reply
Send Data

ARP

- Host *A* wants to know the hardware address associated with IP address I_b of host *B*
- *A* broadcasts a special message to all the hosts on the same physical link
- Host *B* answers with a message containing its own link-level address
- *A* keeps the answer in its cache (for some time, e.g., 20 minutes)
- When *A* sends its request, *A* includes its own IP address in the request
  - As an optimization, the receiver of the ARP request may cache the requester mapping

Mensaje ARP

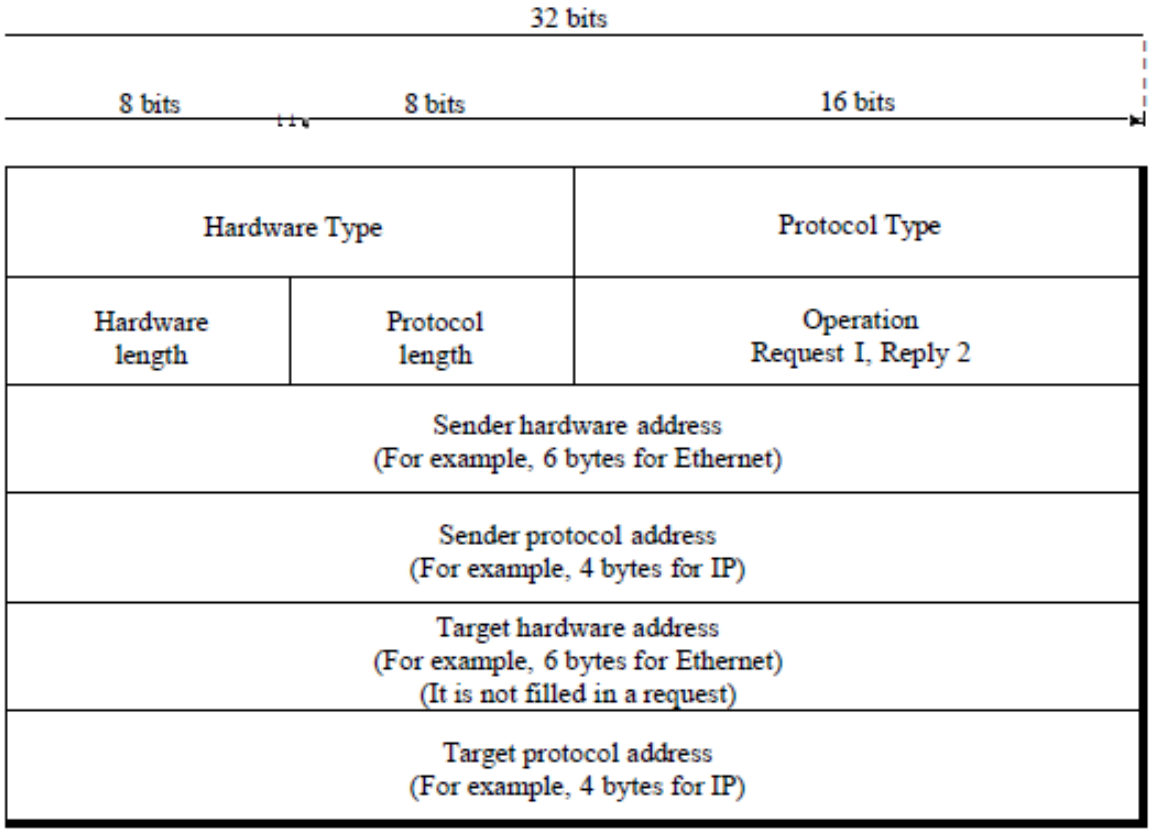
Hw type	Proto type	Hw size	Proto size	Op	Sender Ether	Sender IP	Target Ether	Target IP

- Mapping information
  - Hardware (2 bytes) [Typically: Ethernet]
  - Protocol (2 bytes) [Typically: IP]
  - Hardware size (1 byte)
  - Protocol size (1 byte)

  Typically: 0x0001, 0x0800, 6, 4
- Op: type of message (1: request; 2: response)
- Sender Ethernet/IP: sender data
- Target Ethernet/IP: target data
  - Target Ethernet is all 0s in request

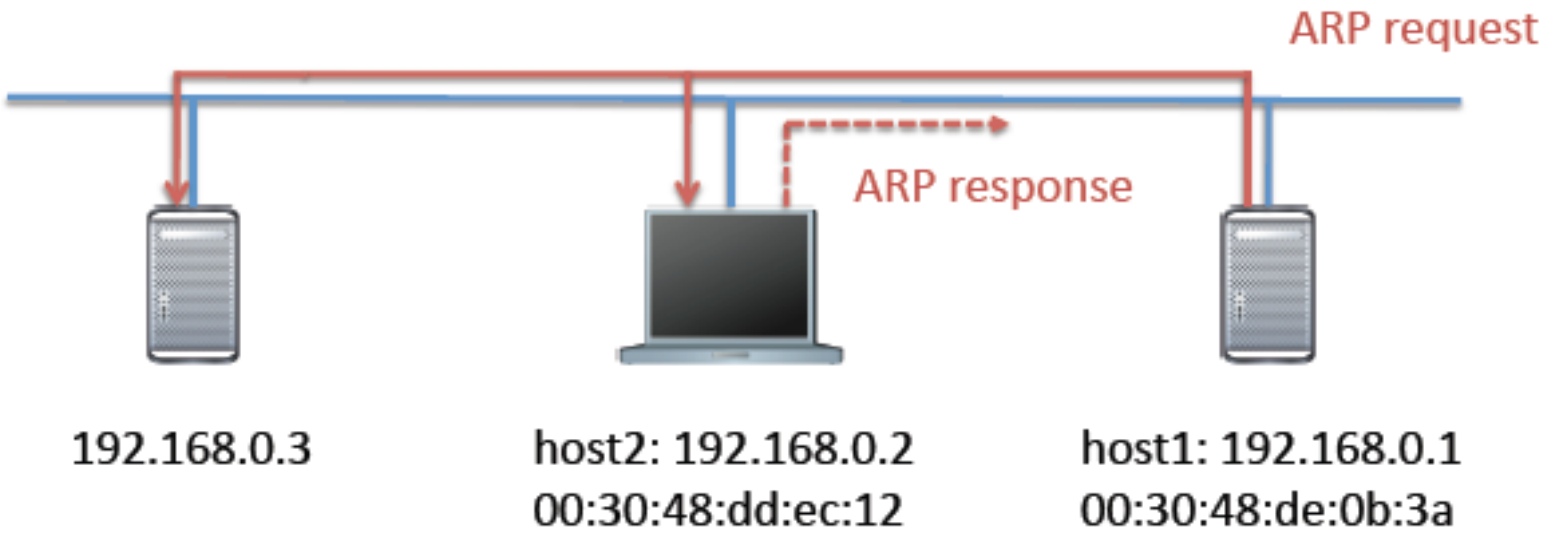
ARP

Figure 21.2 *ARP packet*



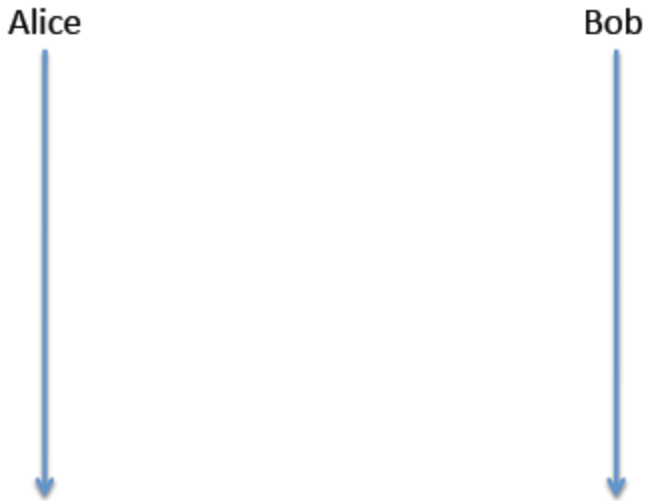
Tráfico ARP

```
host1# arp –n
host1# ping –c 1 192.168.0.2
04:21:16.312430 ARP, Request who-has 192.168.0.2 tell 192.168.0.1, length 28
04:21:16.312500 ARP, Reply 192.168.0.2 is-at 00:30:48:dd:ec:12, length 46
04:21:16.312506 IP 192.168.0.1 > 192.168.0.2: ICMP echo request, id 16976, seq 1, length 64
04:21:16.312577 IP 192.168.0.2 > 192.168.0.1: ICMP echo reply, id 16976, seq 1, length 64
host1# arp –n
192.168.0.2        ether   00:30:48:dd:ec:12   C                 eth0
Host2# arp –n
192.168.0.1        ether   00:30:48:de:0b:3a   C                 eth0
```



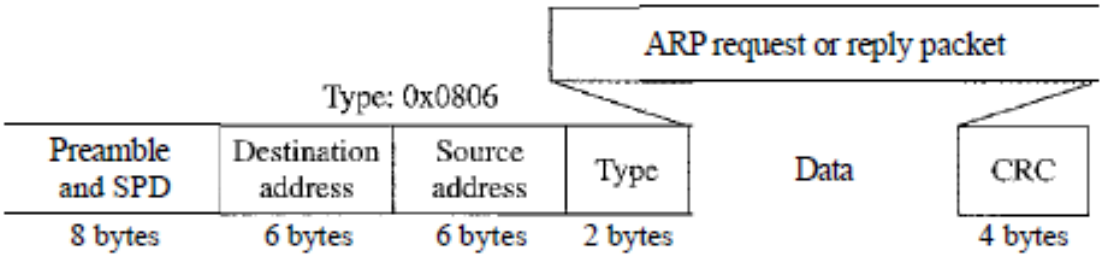
ARP

- Alice (192.168.1.1) desea enviar un datagrama IP a Bob (192.168.1.2). ¿Qué sucede?

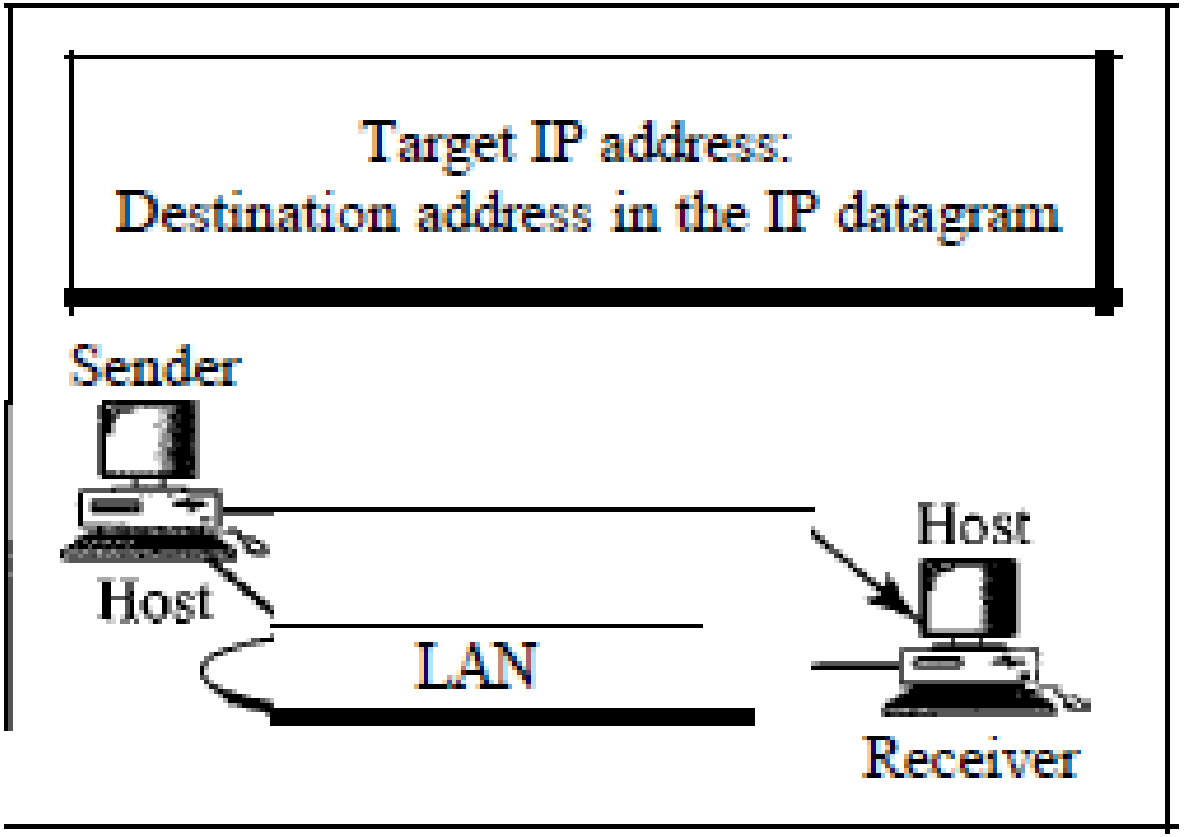


ARP

Figure 21.3 *Encapsulation of ARP packet*

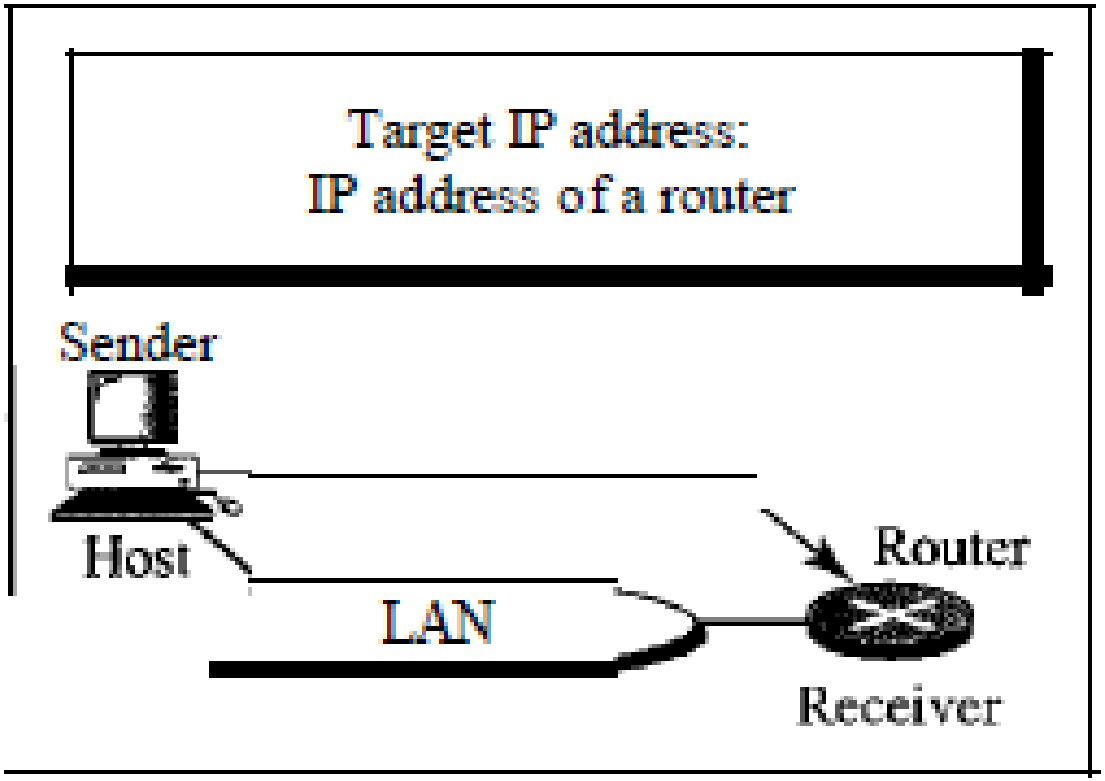


ARP: Caso 1



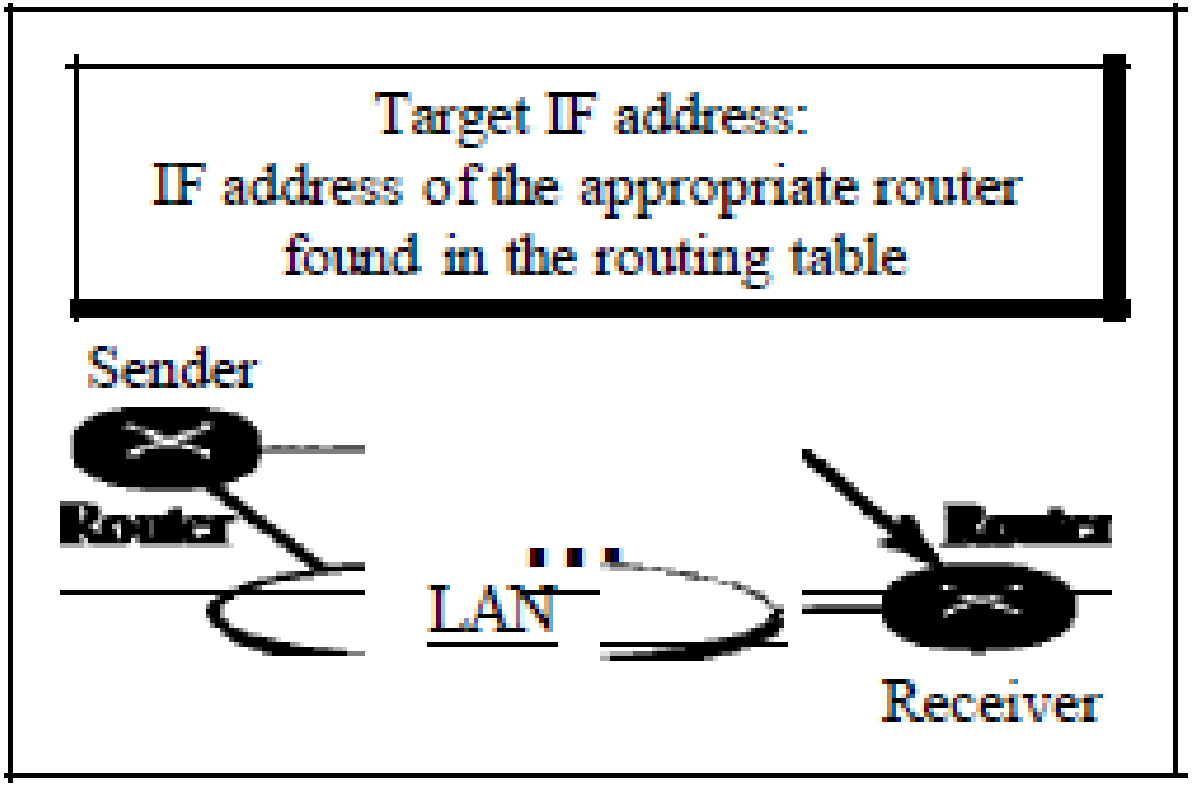
Case 1. A host has a packet to send to another host on the same network.

ARP: Caso 2



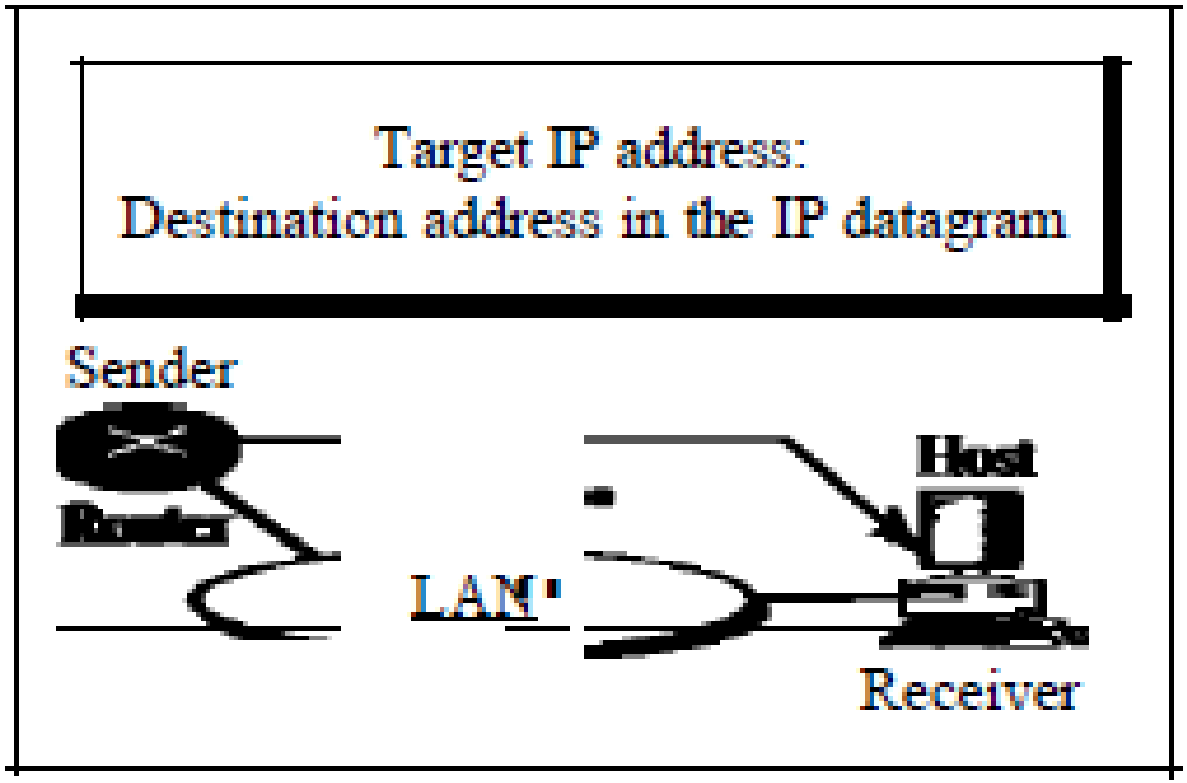
Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.

ARP: Caso 3



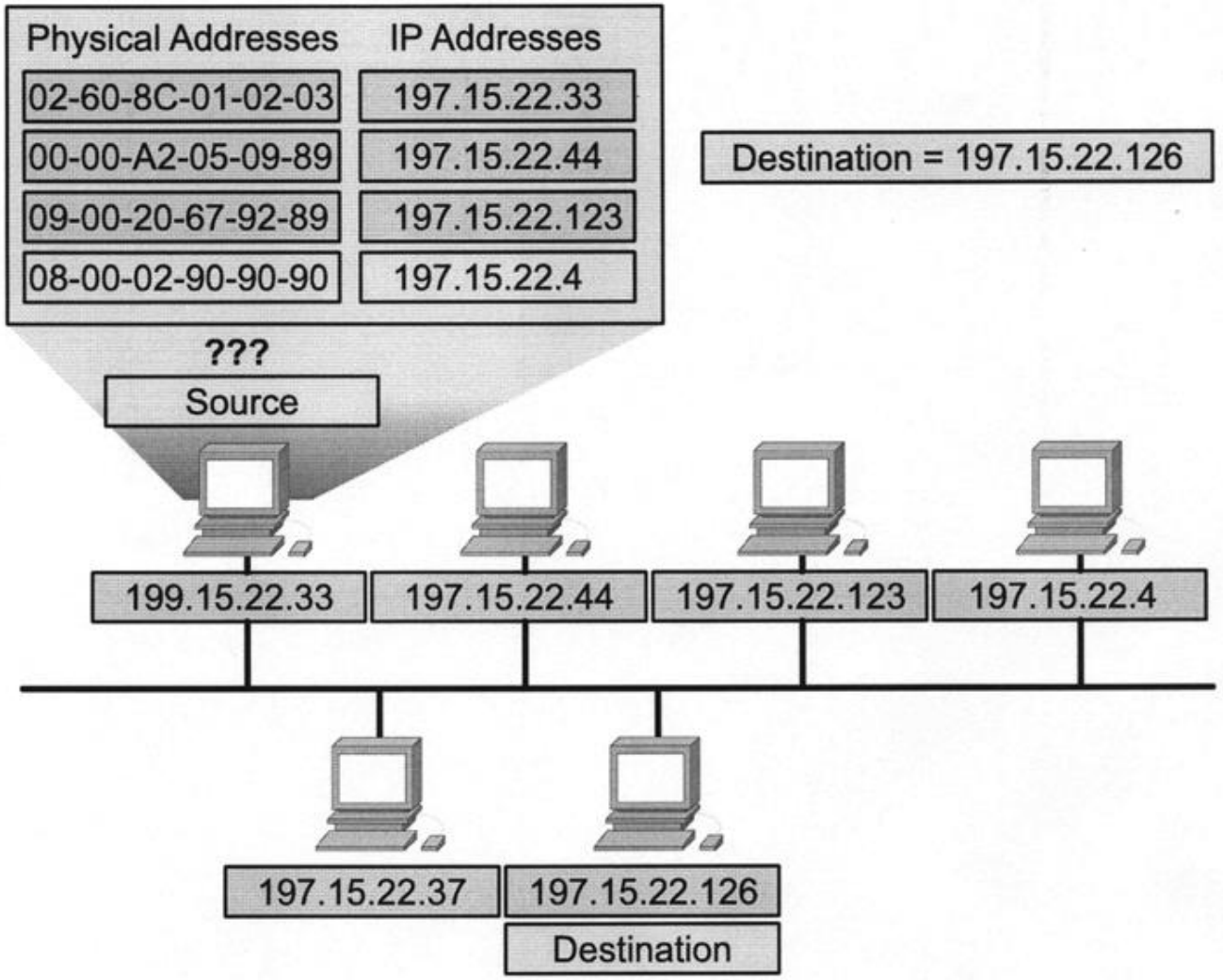
Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

ARP: Caso 4

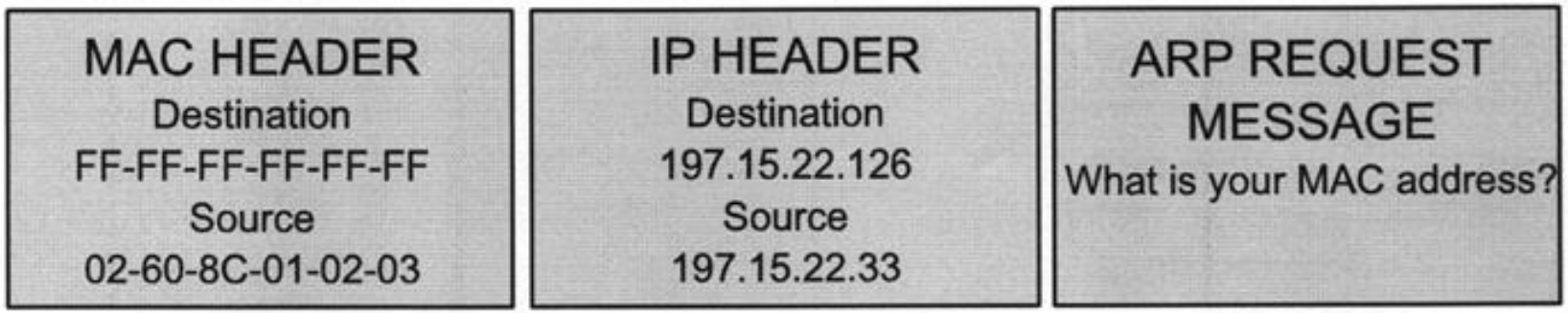


Case 4. A router receives a packet to be sent to a host on the same network.

ARP con subnet



ARP con subnet



ARP: Comunicación entre subredes

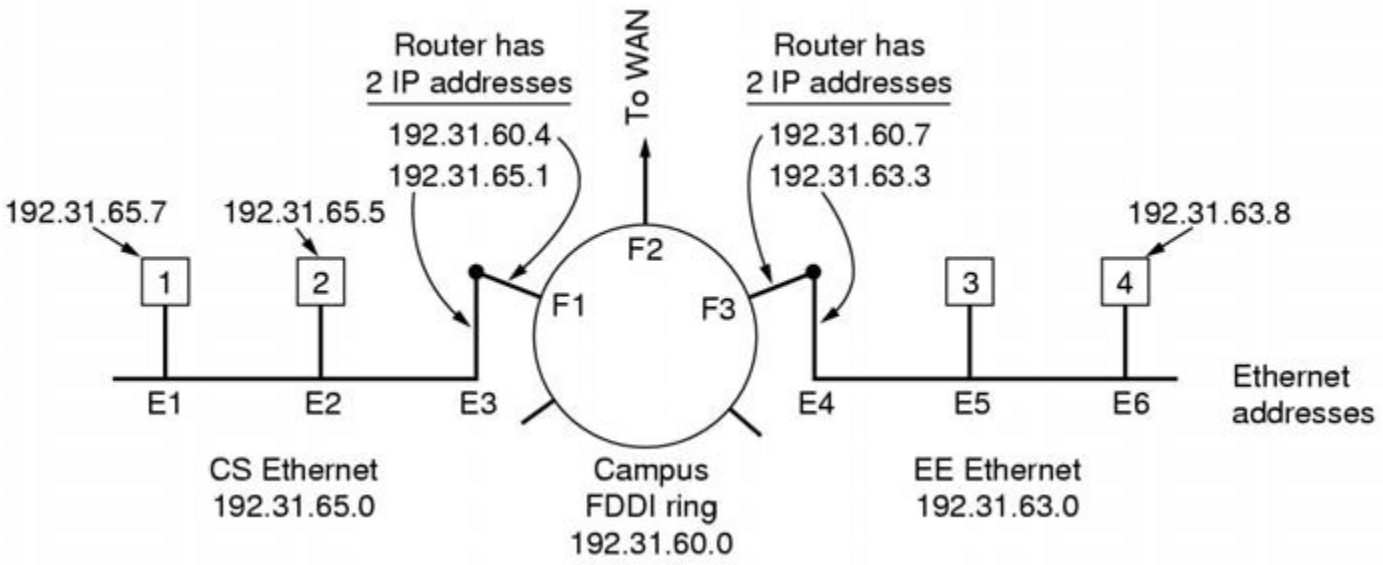
1. **Usando un gateway por defecto**.
   - La dirección IP de la interface en el router que conecta al segmento de red en el cual se encuentra el host de origen.
   - El host de origen compara la dirección IP del destino y si no se encuentra en la misma subred, envía el requerimiento ARP al gateway por defecto (usando la dirección MAC del router)

ARP: Comunicación entre subredes

2. **Proxy ARP:**
   - El router es configurado para responder a los requerimientos ARP para redes remotas.

- En ambos casos, el router luego reenvía el paquete en un frame destinado al router remoto (en el ejemplo de la figura usando la dirección MAC FDDI)

ARP: Comunicación entre subredes

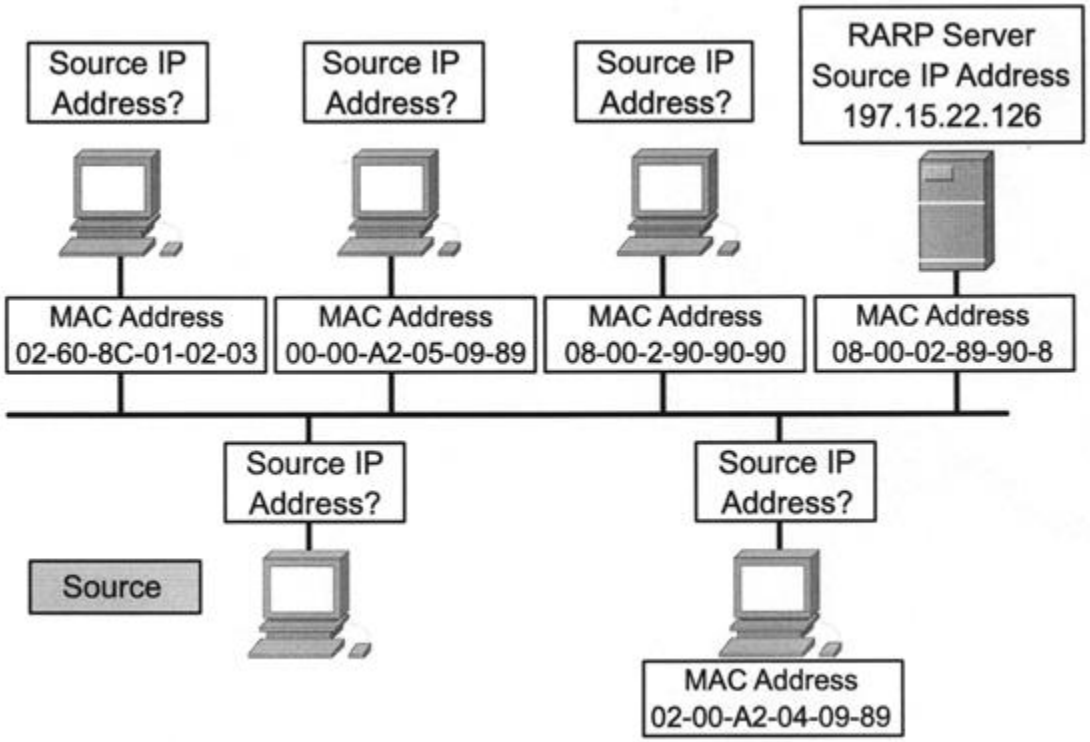


Asignación de direcciones IP

Asignando direcciones IP

- Principalmente, existen dos métodos para asignar direcciones IP:
  - **Direccionamiento estático**: cada dispositivo individual está configurado manualmente con una dirección IP
  - **Direccionamiento dinámico**:
    - Reverse ARP (RARP, RFC 903). Problema: Un servidor RARP es requerido en cada red (routers no reenvían MAC broadcasts)
    - BOOTP (RFC, 951, 1048, 1084): usa mensajes UDP (Capa 4) los cuales son reenviados por routers.

Asignando direcciones IP



IPv6

Deficiencias del IPv4

1. A pesar de las soluciones a corto plazo, tales como subnetting, classless addressing y NAT, **el agotamiento de IPs es un problema a largo plazo en el Internet**.
2. Internet requiere transmisión de audio y video en tiempo real. Este tipo de transmisión requiere una estrategia para minimizar el retardo y la reservación de recursos.
3. **No provee encriptación ni autenticación** de datos, lo cual es requerido para ciertas aplicaciones.

IPv6

- Para superar estas deficiencias, IPv6 (Internetworking Protocol, version 6), también conocido como IPng (Internetworking Protocol, next generation), fue propuesto y es ahora un standard.
- La longitud y formato de las direcciones IP fueron modificados.
- Protocolos relacionados, tales como ICMP fueron modificados.
- Otros protocolos, tales como ARP, RARP, IGMP, fueron eliminados o incluidos en el protocolo ICMPv6

Ventajas de IPv6

1. Mayor espacio de dirección: **128 bits** de longitud.
2. Formato de cabecera mejorado: se **acelera** el proceso de **ruteo** porque la mayoría de las opciones no requieren ser chequeadas por los routers.
3. Nuevas opciones: para **funcionalidades** adicionales.
4. Diseñado para permitir la **extensión** del protocolo: de ser requerido por nuevas tecnologías o aplicaciones
5. Soporte para **asignación** de recursos: se ha agregado un mecanismo (flow label) que permite a los recursos requerir un manejo especial de paquetes.
6. Soporte para mayor **seguridad**: encriptación y autenticación.

Puntos para recordar

- Mensajes ARP
- IPv6

Próxima Sesión

- Algoritmos de ruteo