

IPv4

Comunicaciones:
Licenciatura en Ciencias de la
Computación

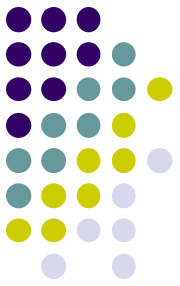
bulacio@cifasis-conicet.gov.ar





IPv4: Contenido

- Contexto
- Objetivo del IP (Cap 7)
- Datagrama - Cabeceras (Cap 7)
- Direcciones (Cap 4-Cap 10)
- Ruteo (Cap 8)
- ARP (Cap 5)
- ICMP (Cap 9)

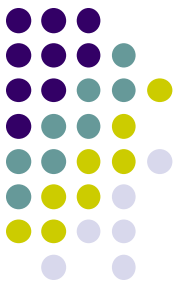


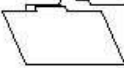

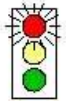

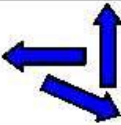
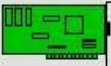

Bibliografía

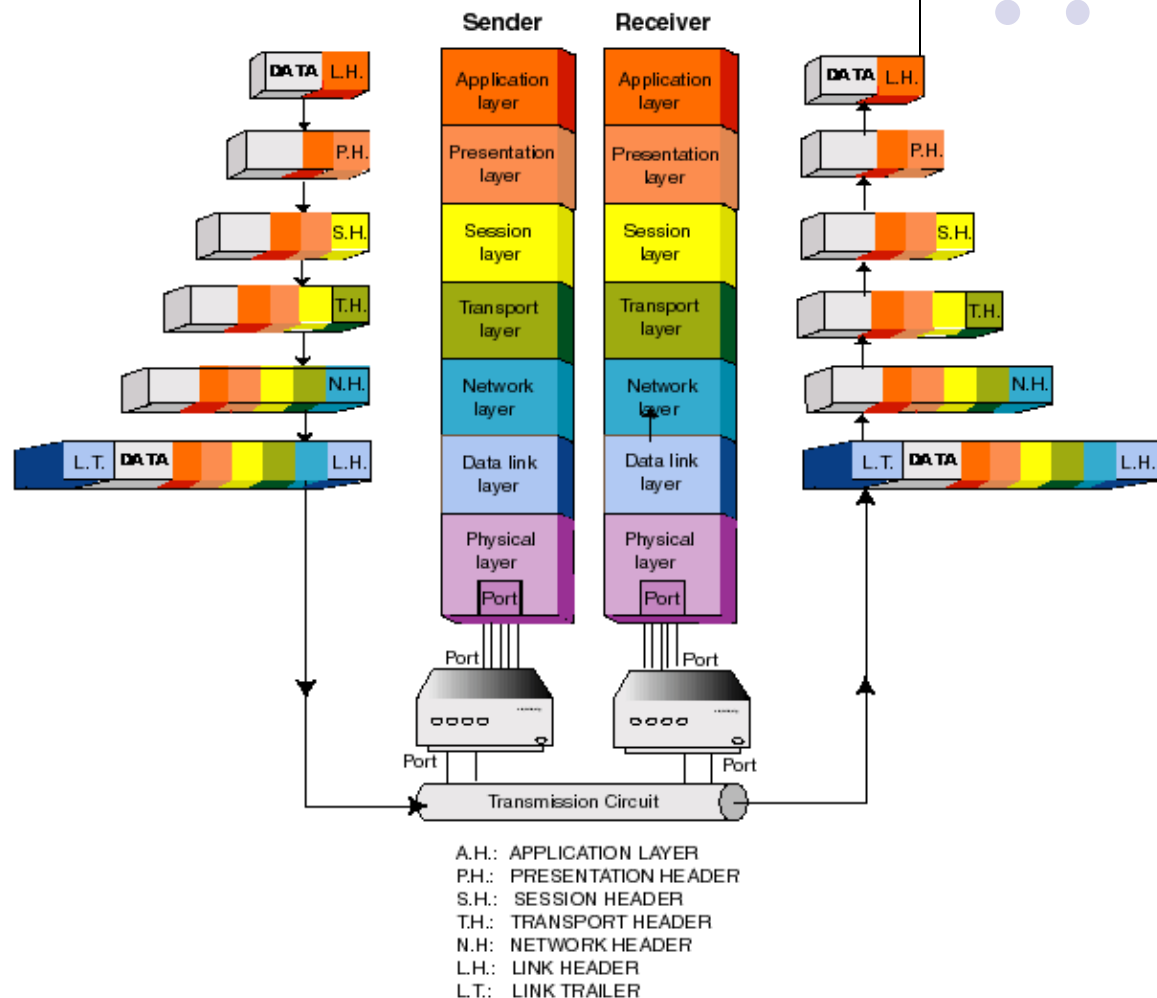
- TCP/IP Principios básicos, protocolos y arquitectura. D. Comer.
- TCP/IP Tutorial and Technical Overview, Redbooks (ibm.com/redbooks). A Rodriguez et al.
- RFCs



The OSI Seven-Layer Model



OSI MODEL		
7		Application Layer Type of communication: E-mail, file transfer, client/server.
6		Presentation Layer Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5		Session Layer Starts, stops session. Maintains order.
4		Transport Layer Ensures delivery of entire file or message.
3		Network Layer Routes data to different LANs and WANs based on network address.
2		Data Link (MAC) Layer Transmits packets from node to node based on station address.
1		Physical Layer Electrical signals and cabling.



Contexto: Comparación de modelos



OSI

TCP/IP

Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Física

Aplicación
Transporte
Internet
Host-red

Puerto: extremo-extremo

IP: Det. ruta

MAC: Dir físico

LLC. Acceso

Token ring-Ethernet

Hardware

Firmware

Software

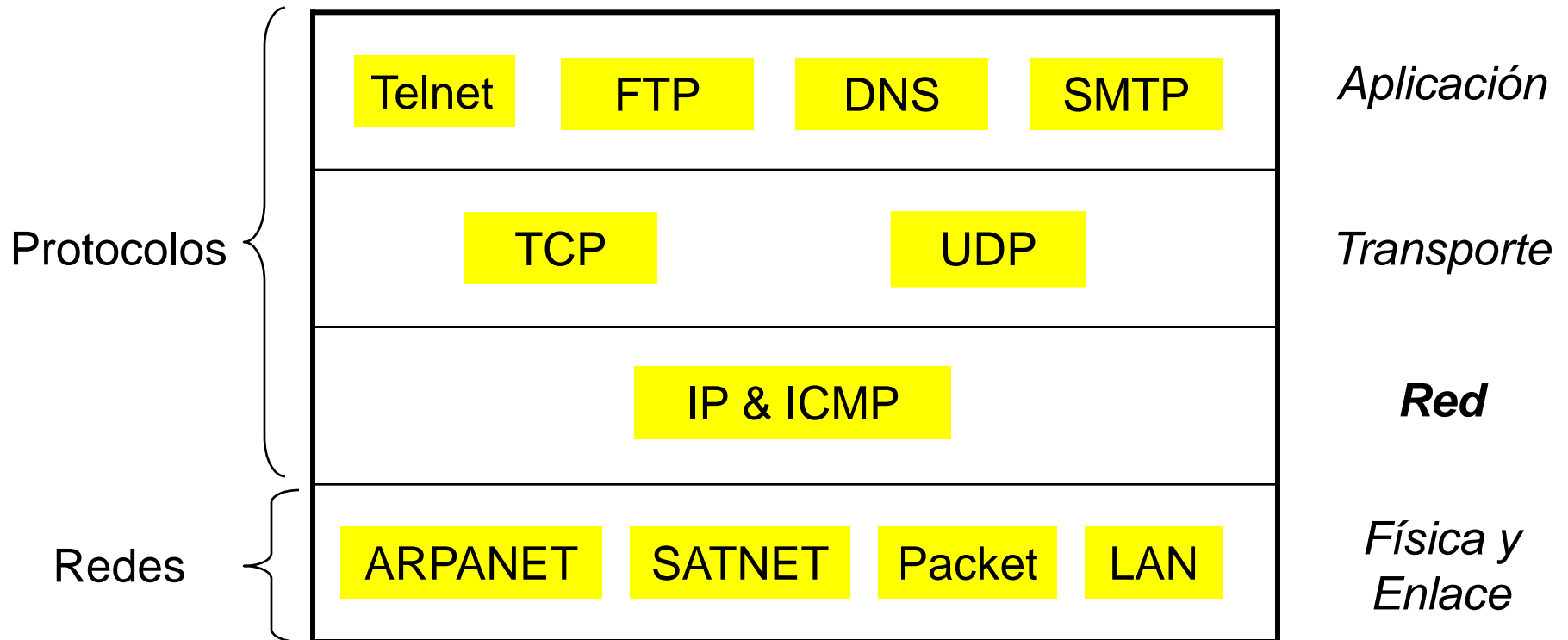
Sist. Operativo

Progr. de usuario

Contexto: Protocolos/redes de TCP/IP



Nombre de
Capa OSI



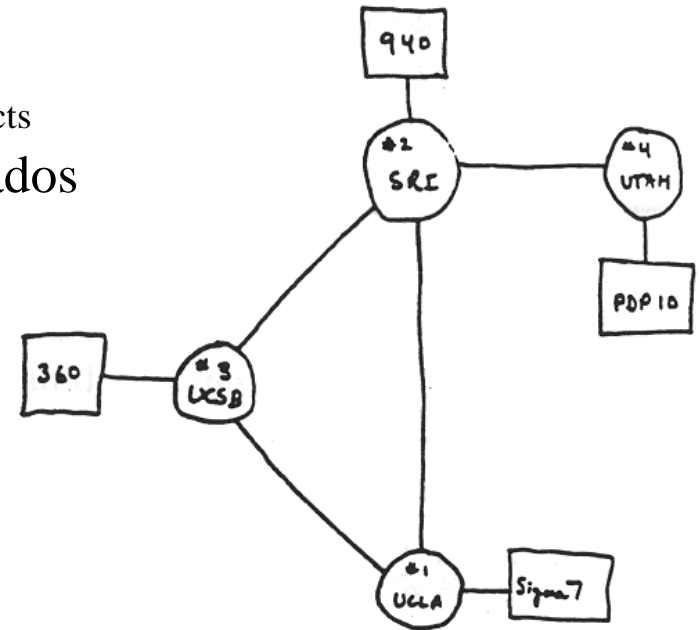
RFC: 791

Replaces: RFC 760

IENs 128, 123, 111,
80, 54, 44, 41, 28, 26

Internet

- **1969** – Inicio de ARPANET (Advanced Research Projects Agency Network): 4 computadoras con cables dedicados
- 1981 – Definición de IPv4 en la RFC 791
- 1983 – ARPANET adopta TCP/IP
- **1990** – Primeros estudios sobre el agotamiento de las direcciones
- 1993 – Internet comienza a ser explotada comercialmente



THE ARPA NETWORK

DEC 1969

4 NODES

FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

Objetivos del IP: RFC791 (1981)



- ✓ Transparencia en la red de redes...
- ✓ Protocolo IP, definiciones importantes:
 - Define la unidad básica para la transferencia de Datos: paquete o **DATAGRAMA**, que pasará a través de una red TCP/IP
 - El SW IP realiza la Función de Ruteo.
 - Reglas de entrega de paquetes *NO confinable*: Cómo procesar los paquetes; Cuándo generar los mensajes de error; Cuándo descartar los paquetes.

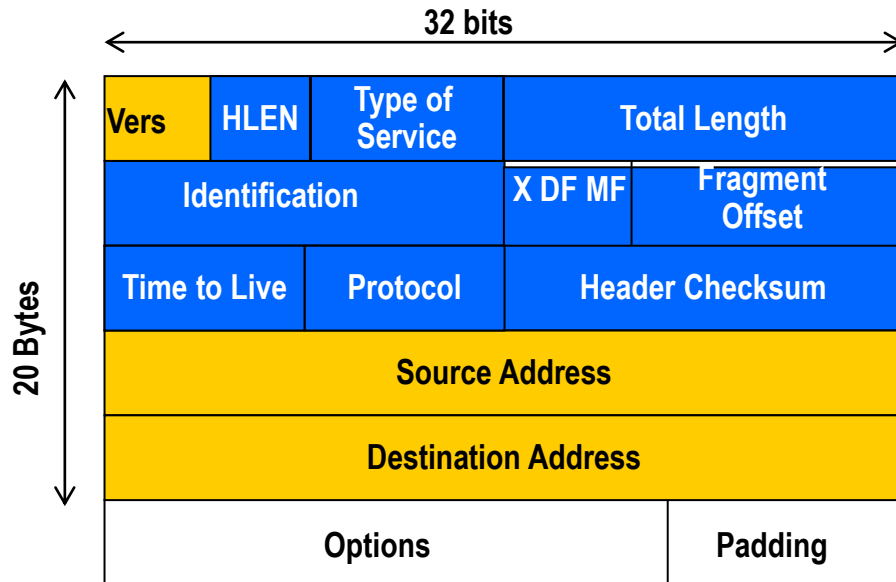
HEADER

Datos de usuario del datagrama

Cabecera IPv4: formato (C7)



IPv4

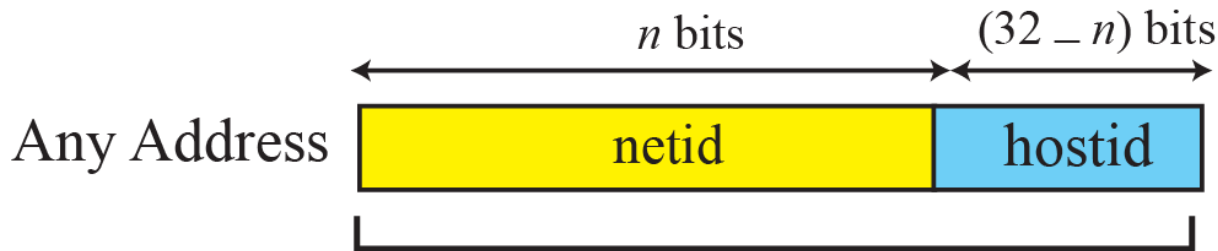


IPv4: 12 campos fijos que pueden tener opciones => cabecera de tamaño entre 20, $5 \cdot 32/8$, y 60 bytes

- Vers: 4.
- **Long. Cabecera (HLEN):** en palabras de 32 bits (mínimo 5, máximo 15)
- **Longitud total:** mide la cabecera + datos en octetos, máximo $2^{16} = 65535$ bytes.
- **Identificación, DF (Don't Fragment), MF, Desplaz. Fragmento:** campos de fragmentación en múltiplos de 8 bytes; x bit sin uso
- **Tiempo de vida:** contador de saltos hacia atrás (se descarta cuando es cero)
- **Checksum:** de la cabecera (no incluye los datos)



Direcciones IP (C4)



Class A: $n = 8$

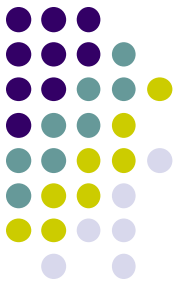
Class B: $n = 16$

Class C: $n = 24$



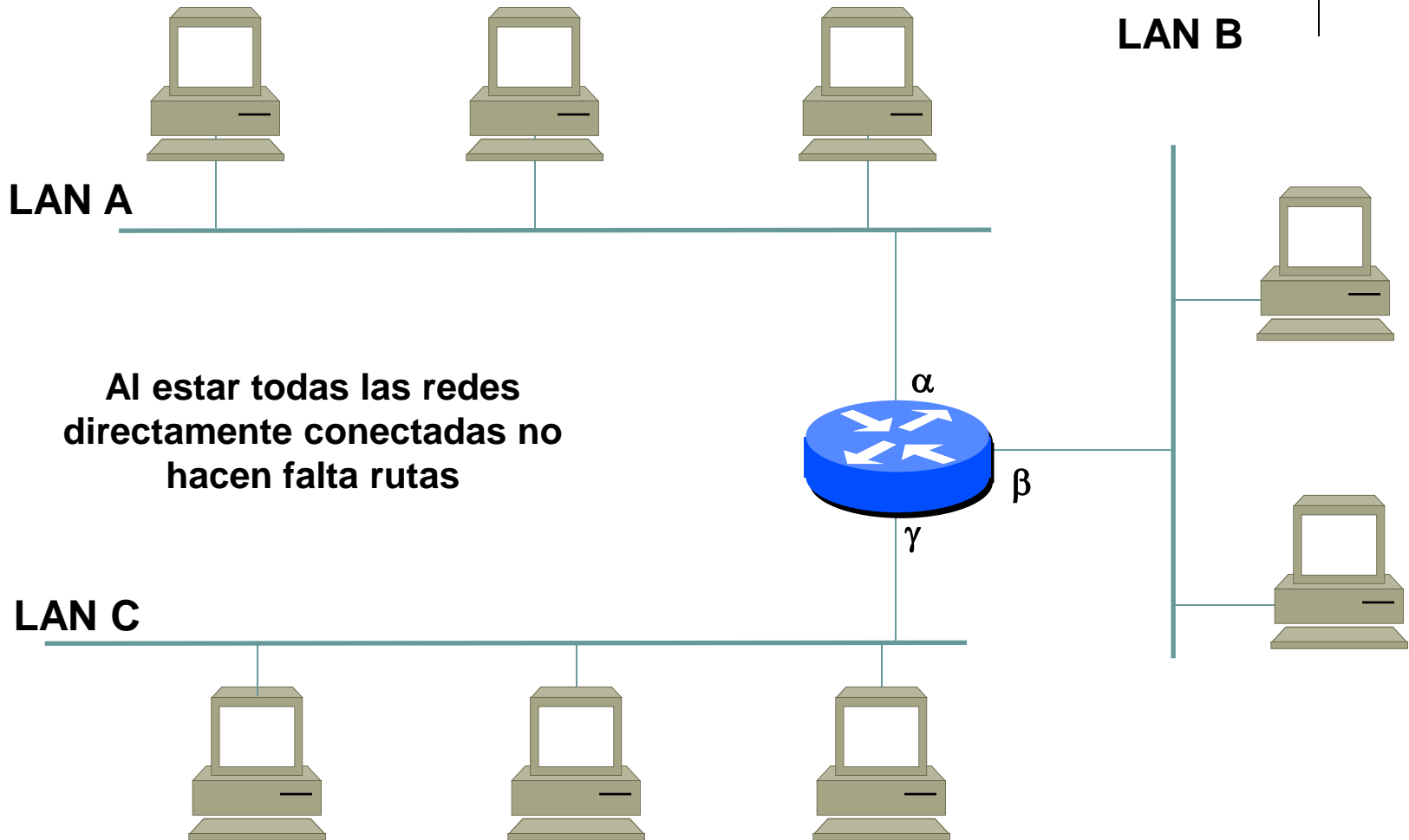


Dir IP: clase? Netid.hostid

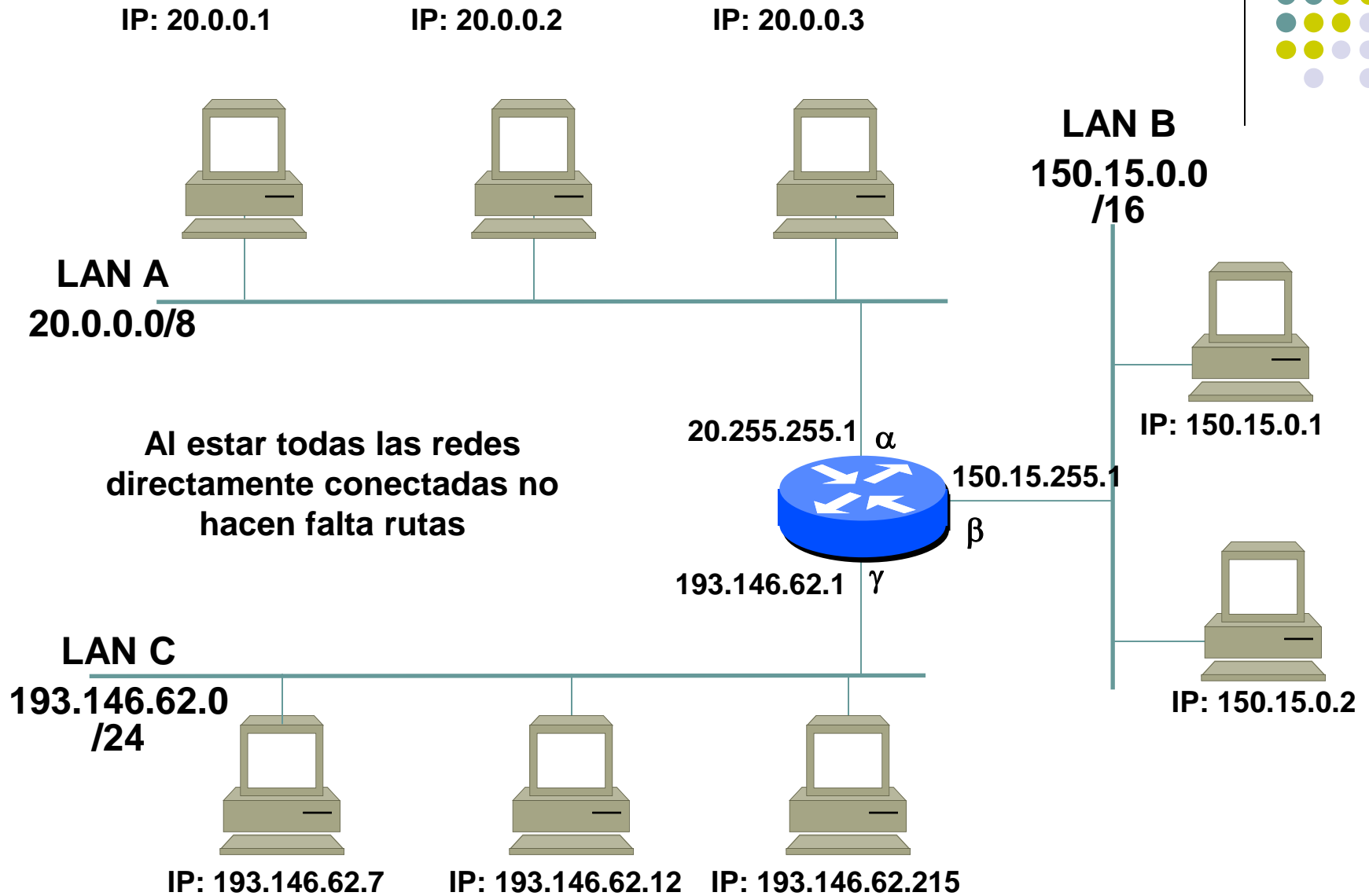


- 100000000.00001010.000000010. 00011110
- 110000000.01100100 .00001010. 001000001
- 177.100.18.5
- 119.18.45.0
- 209.240.80.77
- 199.155.77.56

Actividad 4: Router con tres LANs



Actividad 4: Router con tres LANs





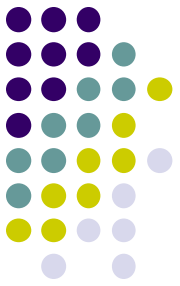
Direcciones IP especiales

netid	hostid	Significado	Ejemplo
todos 0		Este anfitrión. Permitida sólo en el arranque	0.0.0.0
todos 0	host	Anfitrión en esta red	0.0.0.10
red	host todos 0	Identifica una red	192.168.1.0
todos 1		Difusión limitada (red local)	255.255.255.255
red	host todos 1	Difusión a la red indicada	192.168.1.255
127	Nada (a menudo 1)	Loopback (mi propio host)	127.0.0.1



Escribir las direcciones de red y la dirección de difusión para cada red

Direcciones IP

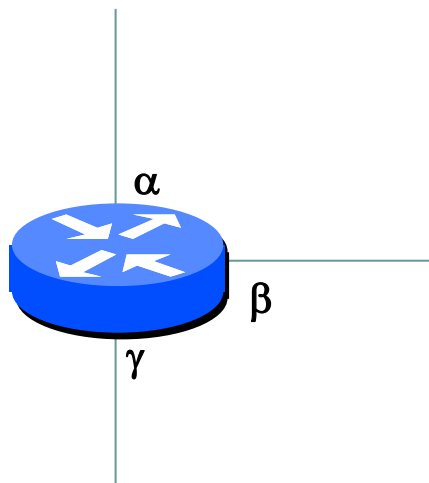


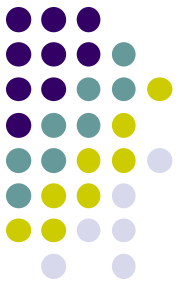
Clase	Formato (r=red, h=host)	Nro de redes	Nro de hosts por red	Rango de direcciones de redes	Máscara de subred (/long. Prefijo)
A	r.h.h.h	128-2 126	16777216 -2 16.777.214	0.0.0.0 - 127.0.0.0 1.0.0.0 -126.0.0.0	255.0.0.0 (/8)
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0 (/16)
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255. 0 (/24)
D	grupo	-	-	224.0.0.0 - 239.255.255.255	- (/4)
E	no válidas	-	-	240.0.0.0 - 255.255.255.255	- (/4)

Conmutación/Switching



- El paso de un **mensaje** de una **fuentes** a un **destino** implica muchas decisiones.
- Cuando un mensaje llega a un **dispositivo de conexión**, se debe tomar la decisión de seleccionar uno de los puertos de salida a través del cual envía el paquete: **conmutador**





Note

In circuit switching, the whole message is sent from the source to the destination without being divided into packets.

A good example of a circuit-switched network is the early telephone systems



Note

In packet switching, the message is first divided into manageable packets at the source before being transmitted. The packets are assembled at the destination.



PACKET SWITCHING

La capa de red de Internet está diseñada como conmutación de paquetes, servicio sin conexión.

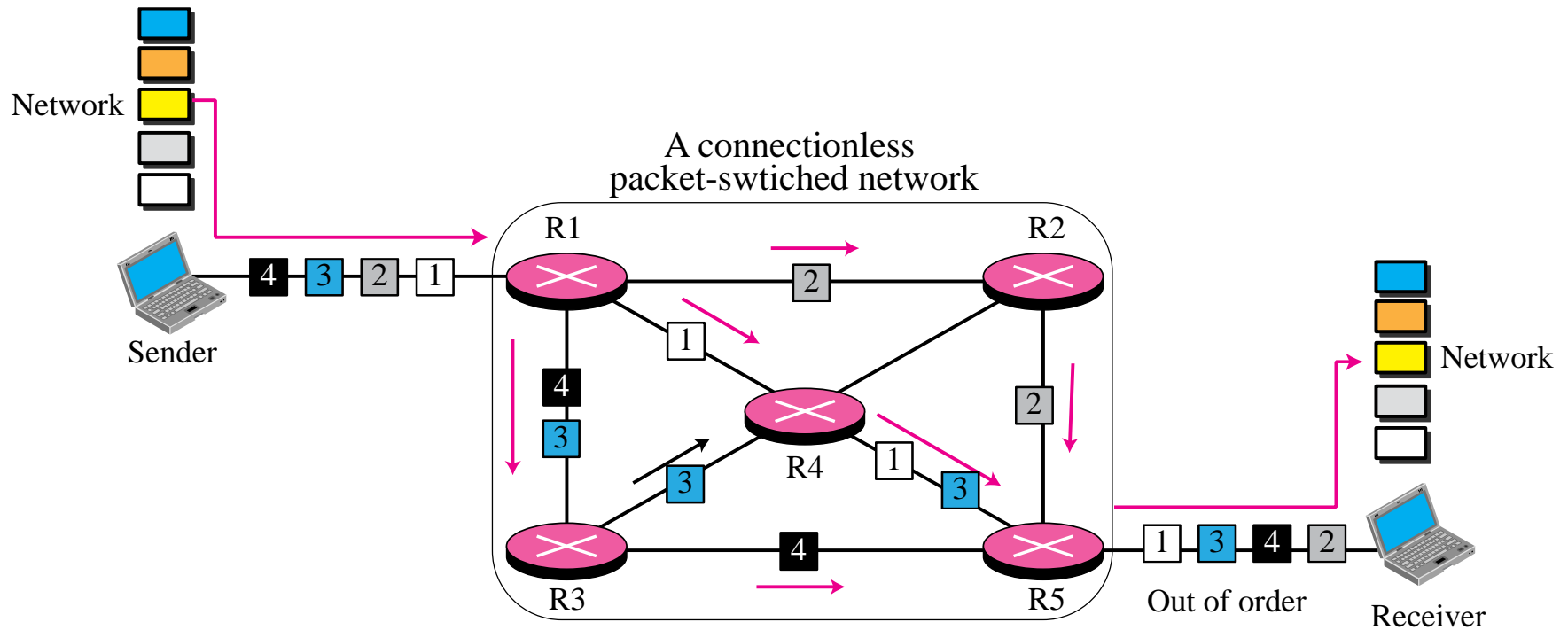
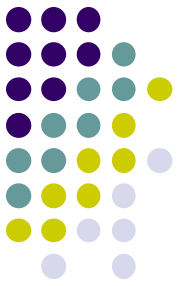
- El paquete en la fuente se **divide** en unidades manejables: **datagramas**.
- Los datagramas individuales se transfieren desde el origen al destino.
- Los datagramas recibidos se **ensamblan** en el **destino** para lograr el mensaje original.



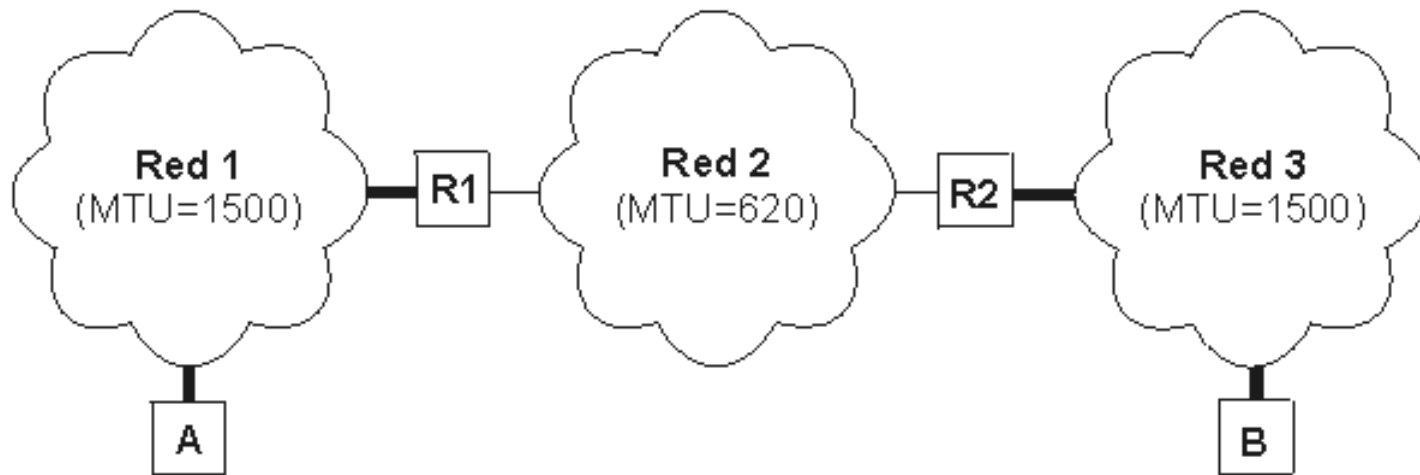
IP: Resumiendo...

- Conmutación de paquetes,
- Servicio sin conexión

IP: conmutación de paquetes, sin conexión

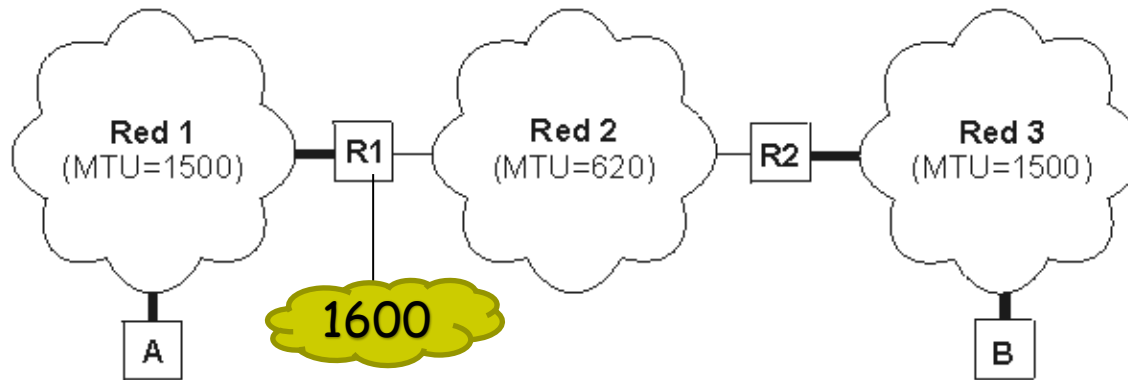


Ej. Tamaño de datagrama, MTU de red y fragmentación (7.7.4)



Ej: Realizar la fragmentación necesaria para el intercambio de datagramas entre A y B. Ver campos cabecera

Tamaño de datagrama, MTU de red y fragmentación (7.7.4)



ENCABEZADO DEL DATAGRAMA	Datos1 600 bytes	Datos2 600 bytes	Datos3 200 bytes
--------------------------	---------------------	---------------------	---------------------

ENCABEZADO DEL FRAGMENTO 1	Datos1
----------------------------	--------

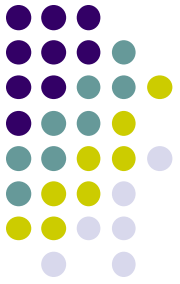
$ID_1 = ID_{ORIG}$
 $OFFSET_1 = 0$
 $MORE_1 = 1$

ENCABEZADO DEL FRAGMENTO 2	Datos2
----------------------------	--------

$ID_2 = ID_{ORIG}$
 $OFFSET_2 = (600 / 8)$
 $MORE_2 = 1$

ENCABEZADO DEL FRAGMENTO 3	Datos3
----------------------------	--------

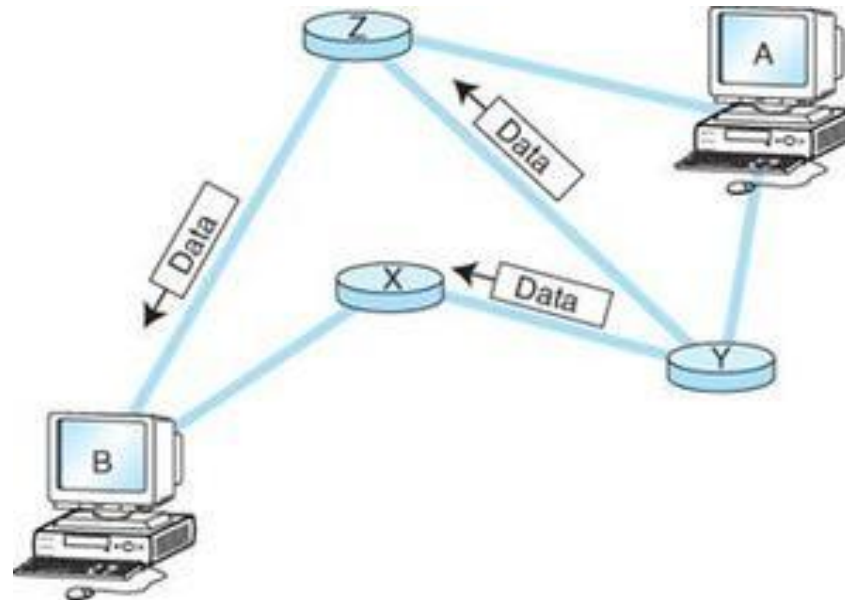
$ID_3 = ID_{ORIG}$
 $OFFSET_3 = OFFSET_2 + (600 / 8)$
 $MORE_3 = 0$



Ruteo

IP

Ruteo de datagramas (C8)



Ruteo: Proceso de selección de un camino para el envío de paquetes, y el ruter es el dispositivo que realiza la selección. Existen dos formas:

- 1) Entrega directa
- 2) Entrega indirecta

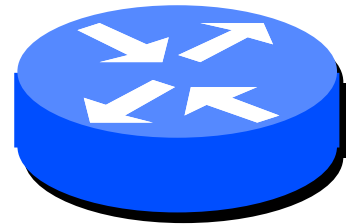
1. Ruteo: entrega directa

- La transmisión de datagramas entre hosts conectados a la **misma** red IP **no necesita routers**.
- El Tx encapsula el datagrama en trama física y envía el paquete directamente



2. Ruteo: entrega indirecta

- La transmisión de datagramas entre dos PCs conectadas a **diferentes** redes IP requiere el uso de **routers**.
- El Tx envía el datagrama a un **ruteador** de su red IP encapsulándolo en una trama física.





1. Ruteo: entrega directa

Cómo sabe el Tx si el destino está en su misma red?

Network addresses are the key (netid,0)

- El Tx compara:

Si: netid Tx = netid Dst



entrega directa

```
[R#show ip route]
C 10.0.0.0 is directly connected, Serial1/1/0
C 30.0.0.0 is directly connected, FastEthernet0/0
```



2. Ruteo: entrega indirecta

- El datagrama pasa de ruter a ruter hasta que llega a uno conectado directamente a la red destino
- ¿Cómo sabe un **host** a qué ruter enviar el datagrama?
- ¿Cómo saben los **ruters** la ruta por la que debe pasar el datagrama hasta llegar a la red destino?

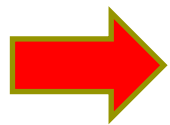
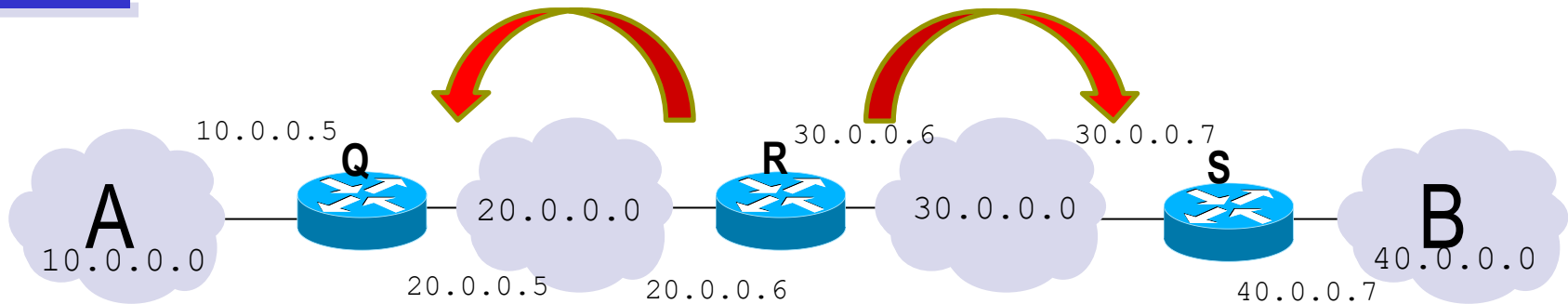
Los Hosts y los ruters usan **tablas de ruteo** que tienen una entrada por cada posible red IP destino indicando:

- a) que la entrega es directa, o
- b) la IP del ruter que constituye el sgte salto en la ruta hasta el destino



2. Ruteo: entrega indirecta

Ej.



Para alcanzar los host de
la Red (netid,0)

Entrega directa o siguiente salto

R

20.0.0.0

Directa

30.0.0.0

Directa

10.0.0.0

20.0.0.5

40.0.0.0

30.0.0.7

```
[R(config)#ip route 40.0.0.0 255.255.255.0 30.0.0.7]
```

Direcciones IPv4



Se terminan las direcciones... qué hacemos?
direcciones **públicas** vs **privadas**.

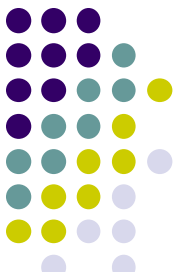
Direcciones IP privadas



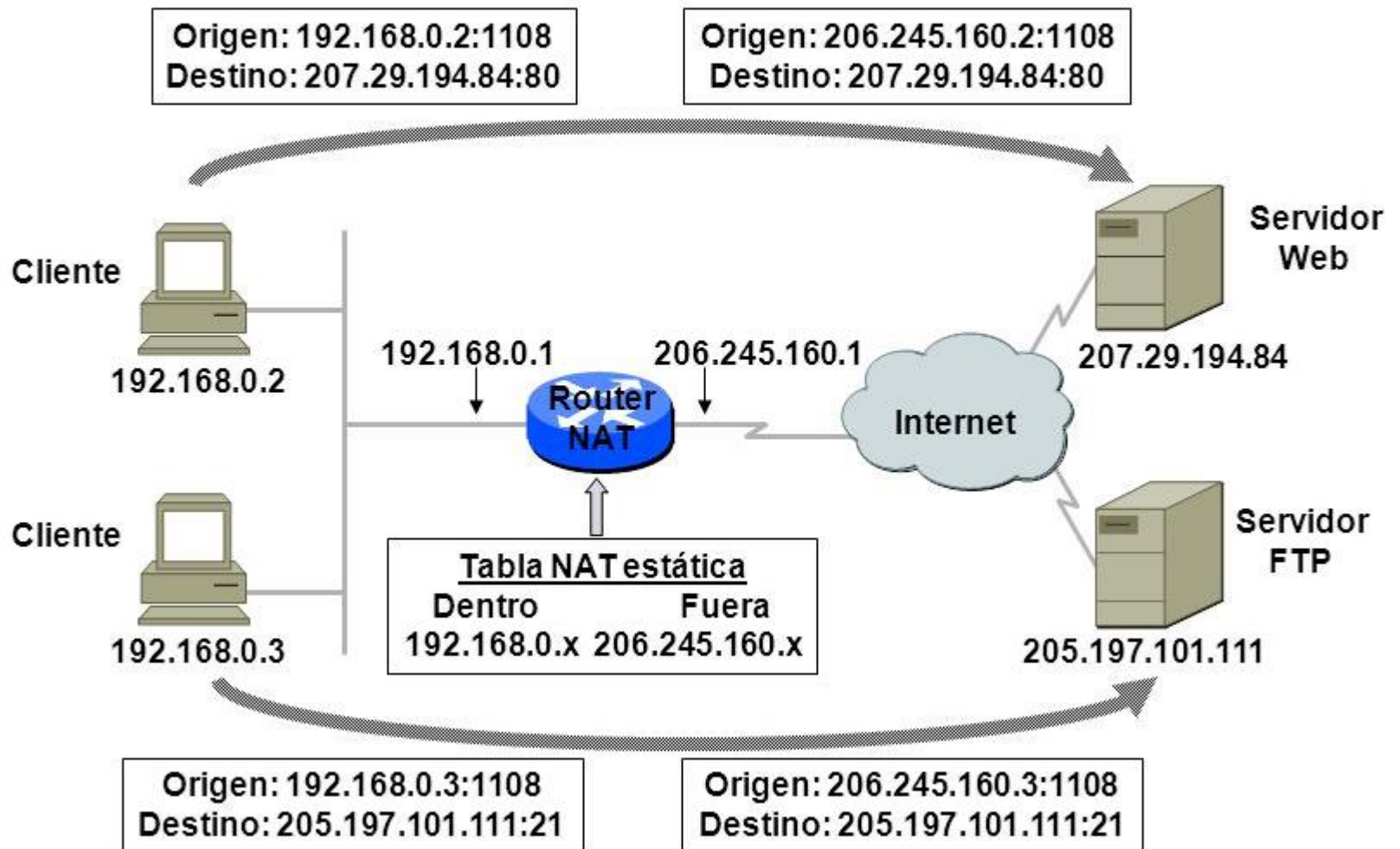
Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0



NAT



■ NAT básico estático

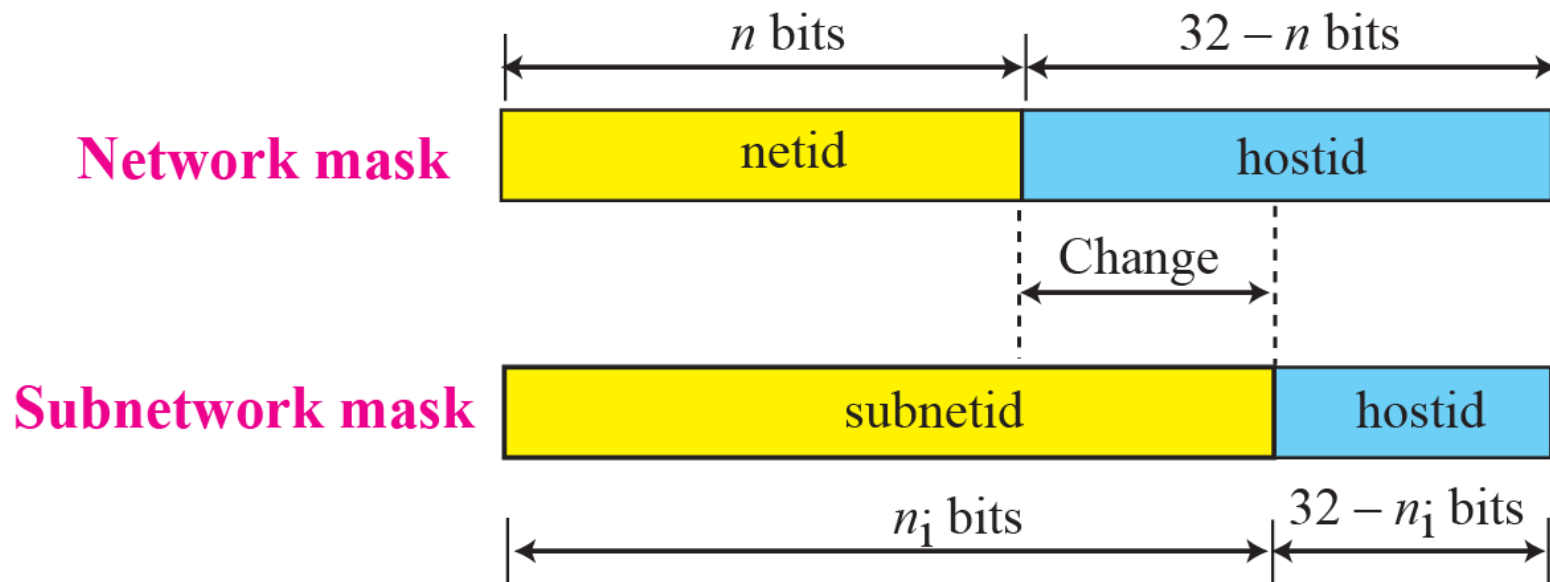


Extensión de direcciones: Subredes IP (C10)



Solución al problema del crecimiento:

- 'Robar' unos bits de la parte host para la subred.





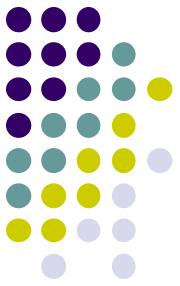
Direcciones IP especiales

netid	hostid	Significado	Ejemplo
todos 0		Este anfitrión. Permitida sólo en el arranque	0.0.0.0
todos 0	host	Anfitrión en esta red	0.0.0.10
red	host todos 0	Identifica una red	192.168.1.0
todos 1		Difusión limitada (red local)	255.255.255.255
red	host todos 1	Difusión a la red indicada	192.168.1.255
127	Nada (a menudo 1)	Loopback (mi propio host)	127.0.0.1



Escribir las direcciones de red y la dirección de difusión para cada red

Direcciones IP

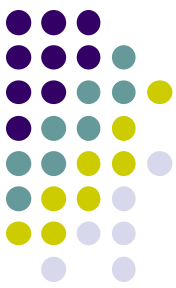


Clase	Formato (r=red, h=host)	Nro de redes	Nro de hosts por red	Rango de direcciones de redes	Máscara de subred (/long. Prefijo)
A	r.h.h.h	128-2 126	16777216 -2 16.777.214	0.0.0.0 - 127.0.0.0 1.0.0.0 -126.0.0.0	255.0.0.0 (/8)
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0 (/16)
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255. 0 (/24)
D	grupo	-	-	224.0.0.0 - 239.255.255.255	- (/4)
E	no válidas	-	-	240.0.0.0 - 255.255.255.255	- (/4)

Subnetting Clase C



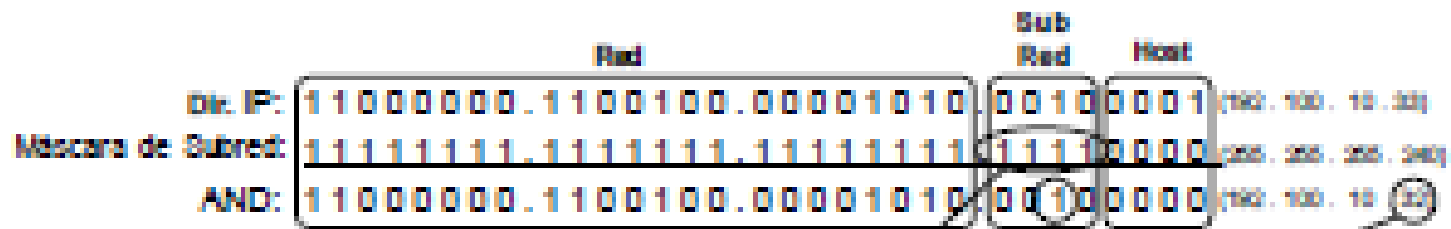
Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible



Dirección IP: 192 . 100 . 10 . 0

Máscara de Subred Adaptada: 255.255.255.240

Rangos de direcciones: 192.10.10.0 a 192.100.10.15
192.100.10.16 a 192.100.10.31
192.100.10.32 a 192.100.10.47
192.100.10.48 a 192.100.10.63
192.100.10.64 a 192.100.10.79
192.100.10.80 a 192.100.10.95
192.100.10.96 a 192.100.10.111
192.100.10.112 a 192.100.10.127
192.100.10.128 a 192.100.10.143
192.100.10.144 a 192.100.10.159
192.100.10.160 a 192.100.10.175
192.100.10.176 a 192.100.10.191
192.100.10.192 a 192.100.10.207
192.100.10.208 a 192.100.10.223
192.100.10.224 a 192.100.10.239
192.100.10.240 a 192.100.10.255



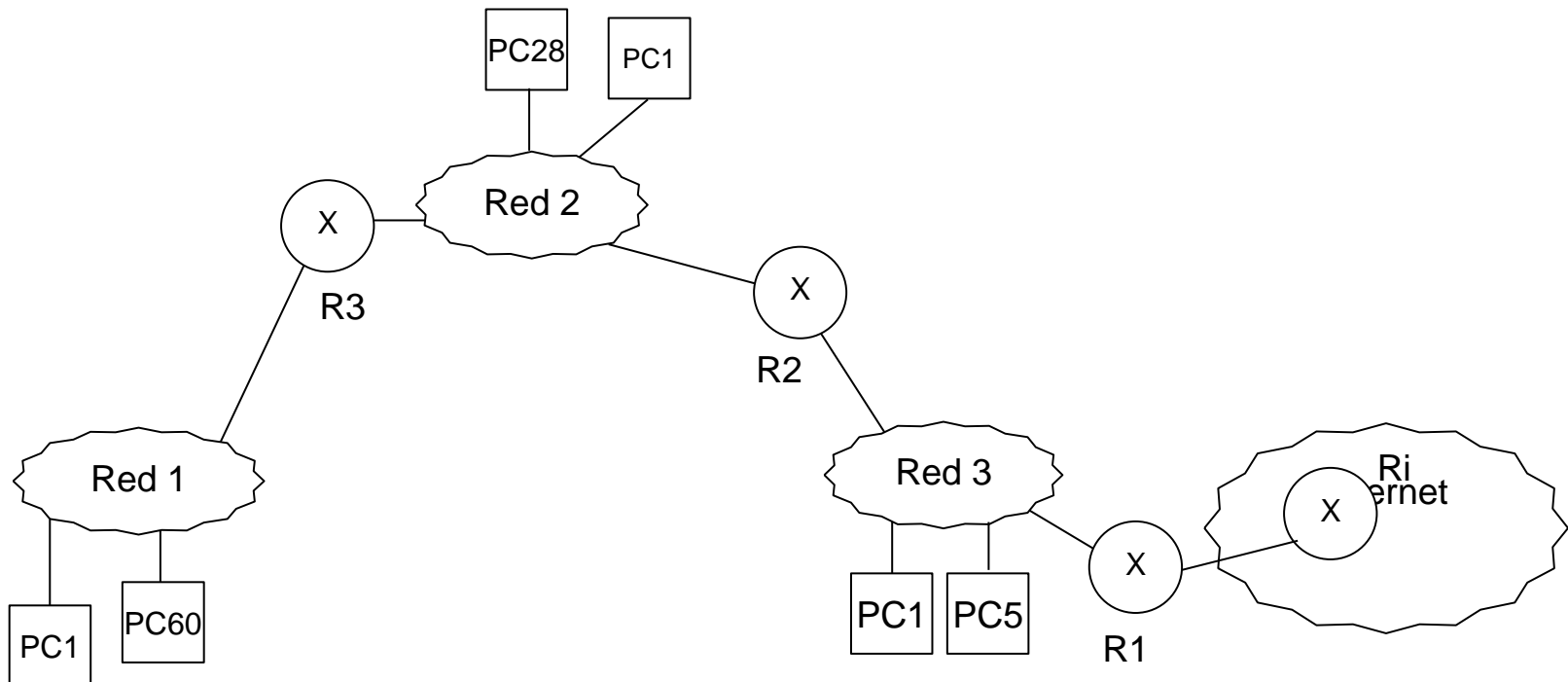
Se cogen 4 bits de la parte de host de la dirección para la máscara de subred adaptada.

La operación AND de los 4 bits que se han cogido mostrará cuál es el rango particular en el que cae la dirección IP.



2) Considere una organización con la siguiente red a la que el proveedor de Internet le asignó la red 190.100.10.0/24 a la empresa, que necesita direccionar 60 PCs en la Red 3, 28 PCs en la Red 2 y 5 PCs en la Red 1.

- Asignar IPs y máscaras detallando el razonamiento en binario.
- Realizar las tablas de ruteo de los tres routers.





Internet Control Message Protocol

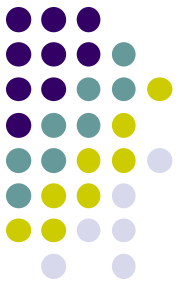
ICMP

ICMP: Cap 9 Comer-RFC 792



- En «**best effort delivery**» cada ruter es autónomo => el sistema trabaja bien si todos los dispositivos lo hacen, y si están de acuerdo con las rutas...
- En la realidad hay problemas ...

ICMP permite que los ruters/host envíen Mxs de error/control hacia otros ruters/hosts



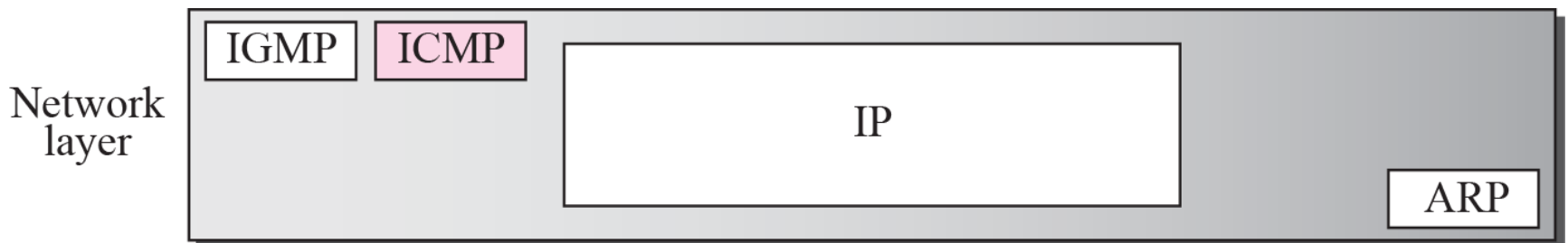
ICMP: Functions

Error:

- A node recognizing a transmission problem (TTL exceed, destination unreachable, etc.) generates ICMP messages;

Control:

- ICMP provides some useful diagnostics about network operation (ping, traceroute).



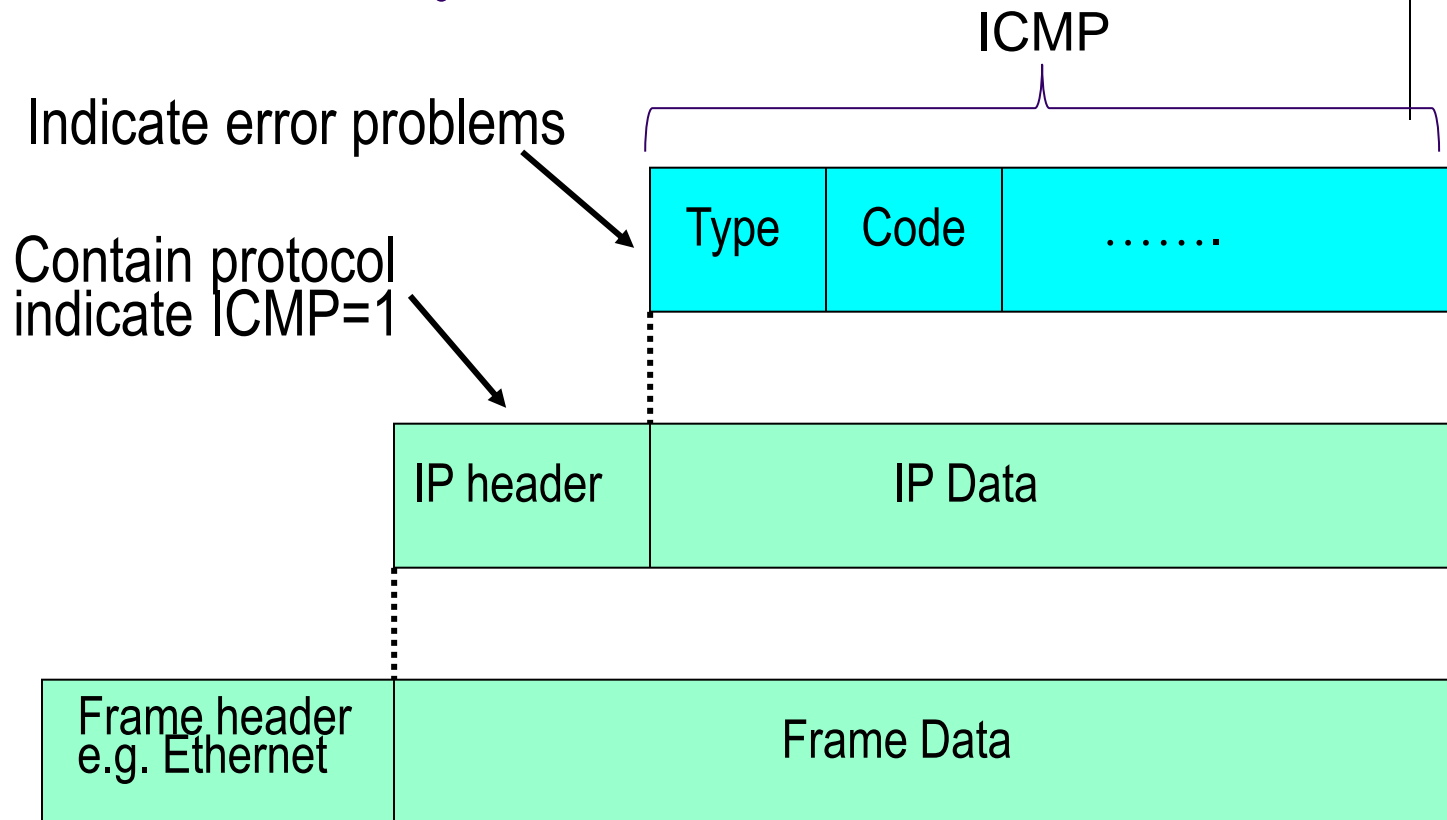


ICMP: Errores

- Cdo hay error, el ICMP reporta a la **fuelle original**. Esto se debe a que en la cabecera sólo se conocen las direcciones **fuelle original y último destino!!!**

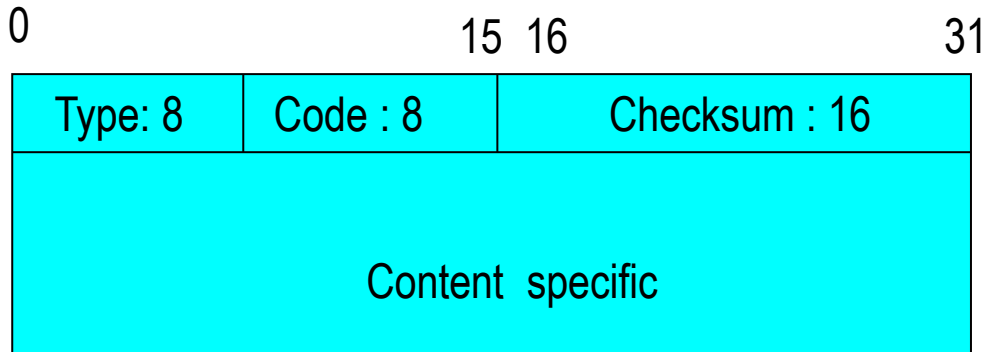


ICMP Encapsulation



OBS: Un Mx ICMP no puede generar Mxs de errores ICMP

ICMP: Mx



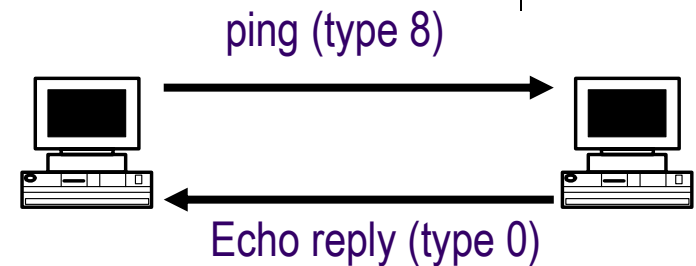
- **Type**: relevant ICMP message
- **Code**: more details information
- **Checksum**: covers ICMP header/data (not IP header)

<u>Campo de tipo</u>	<u>Tipo de mensaje ICMP</u>
0	Respuesta de eco (<i>Echo Reply</i>)
3	Destino inaccesible (<i>Destination Unreachable</i>)
4	Disminución del tráfico desde el origen (<i>Source Quench</i>)
5	Redireccionar (cambio de ruta) (<i>Redirect</i>)
8	Solicitud de eco (<i>Echo</i>)
11	Tiempo excedido para un datagrama (<i>Time Exceeded</i>)
12	Problema de Parámetros (<i>Parameter Problem</i>)
13	Solicitud de marca de tiempo (<i>Timestamp</i>)
14	Respuesta de marca de tiempo (<i>Timestamp Reply</i>)
17	Solicitud de máscara (<i>Addressmask</i>)
18	Respuesta de máscara (<i>Addressmask Reply</i>)

ICMP ping (echo request/reply)



Type = 0/8	code	checksum
identifier		Sequence number
Optional data		



```
C:\Users\pilar>ping 127.0.0.1
```

Haciendo ping a 127.0.0.1 con 32 bytes de datos:

Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

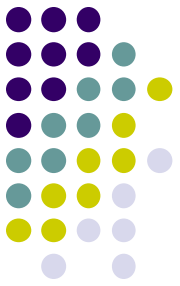
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms



Actividad 1

```
>ping localhost
>ping 127.x.x.x
>ping google.com
>ping 10,1,1,12
```

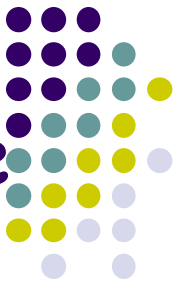
Realice ping con el gateway a internet (puerta de enlace)

```
>ipconfig
```

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

```
    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . :
fe80::241f:fefe:f21d:1ff9%11
    Dirección IPv4. . . . . : 192.168.96.36
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.96.1
```



ICMP type 3 Destination Unreachable

- Cdo un **ruter** no puede direccionar/entregar un datagrama, envía un ICMP type 3 con code descriptivo a la **fuelle original**.
- IP header + primeros 64 bits del datagrama original para dar información de causa del problema

Type = 3	code	checksum
unused		
IP header + 64 bits of original data		

0 = red inaccesible; lo envía cualquier ruter del camino
1 = "host" inaccesible; lo envía el último ruter
2 = protocolo inaccesible;
3 = puerto inaccesible;
4 = se necesitaba fragmentación pero DF estaba activado;
5 = fallo en la ruta de origen.

ICMP type 4 Source Quench



- Un host/ruter envían un ICMP de **disminución de tasa de origen** a la **fuentes original** cuando detecta congestionamiento (los datagramas llegan demasiado rápido)
- Un host que reciba un ICMP 4 para el destino D, disminuye la velocidad de envío a D hasta que deja de recibir los ICMPs. Luego comienza a aumentar gradualmente.

Type = 4	code	checksum
Unused (must be 0)		
IP header + 64 bits of original data		

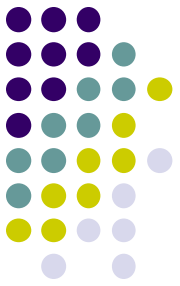
ICMP type 5 Route Change Request



- Usado por un ruter *directamente* conectado al host fuente para solicitarle que cambie de ruta (also called ICMP redirect)

Type = 5	Code (0-3)	checksum
Router IP address (a more suitable router)		
IP header + 64 bits of original data		

Actividad 2: Traceroute Command



Para verificar rutas a un destino.

Linux:

```
user@localhost:/# traceroute www.google.com
```

```
C:\Users\Usuario>tracert google.com
```

Traza a la dirección google.com [173.194.42.9]
sobre un máximo de 30 saltos:

1	1 ms	1 ms	<1 ms	192.168.96.1
2	*	*	*	Tiempo de espera agotado para esta solicitud.
3	6 ms	5 ms	5 ms	168.96.199.92
4	7 ms	7 ms	6 ms	rnoc5.BUENOS-AIRES.innova-red.net [168.96.0.5]
5	*	*	*	Tiempo de espera agotado para esta solicitud.
6	69 ms	119 ms	8 ms	209.85.251.86
7	11 ms	8 ms	8 ms	209.85.251.194
8	8 ms	7 ms	9 ms	eze03s05-in-f9.1e100.net [173.194.42.9]

Traza completa.

- usually probes each hop 3 times
- a lost message or a router that doesn't respond with denote with an " * "



ICMP type 11: tiempo excedido

Type = 11	Code (0-1)	checksum
NO USADO (DEBE SER 0)		
IP header + 64 bits of original data		

- Cada vez que el TTL llega a 0; Code=0
- Cada vez que el tiempo de reensamblado llega a 0; Code=1



ICMP: Solicitando IX

- Marca de hora (type 13/14): la máquina Rx envía un timestamp a quien lo solicitó. Ej., Sincronización, cálculo de viaje redondo, ...
- Obtención máscara: un host puede solicitarlo a los routers



Address Resolution Protocol: 2 entidades se pueden comunicar si conocen sus direcciones físicas

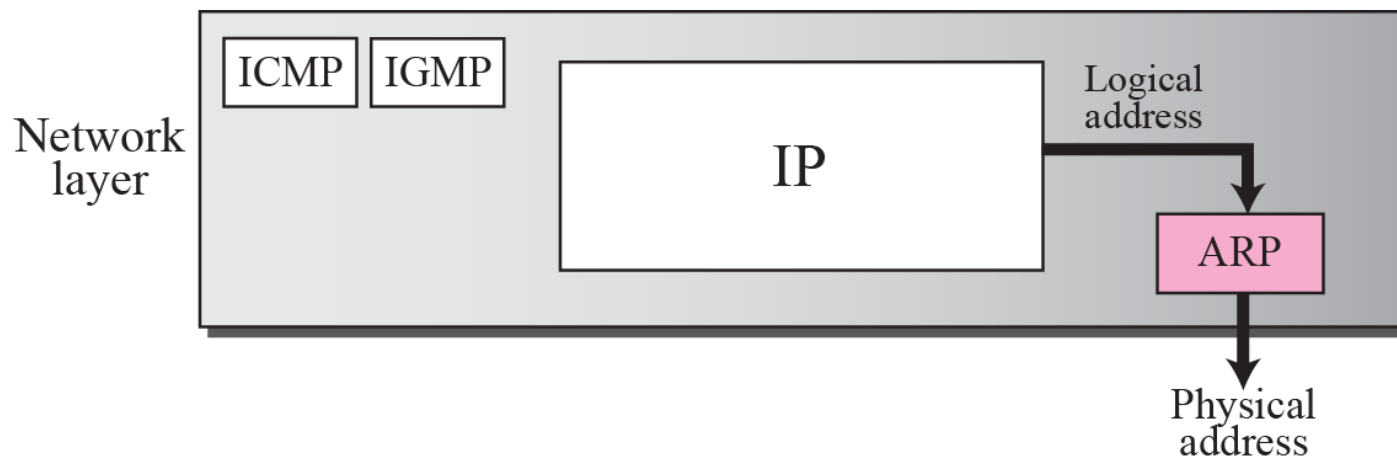
ARP RFC 826

ARP Cap 5 Comer, RFC 826

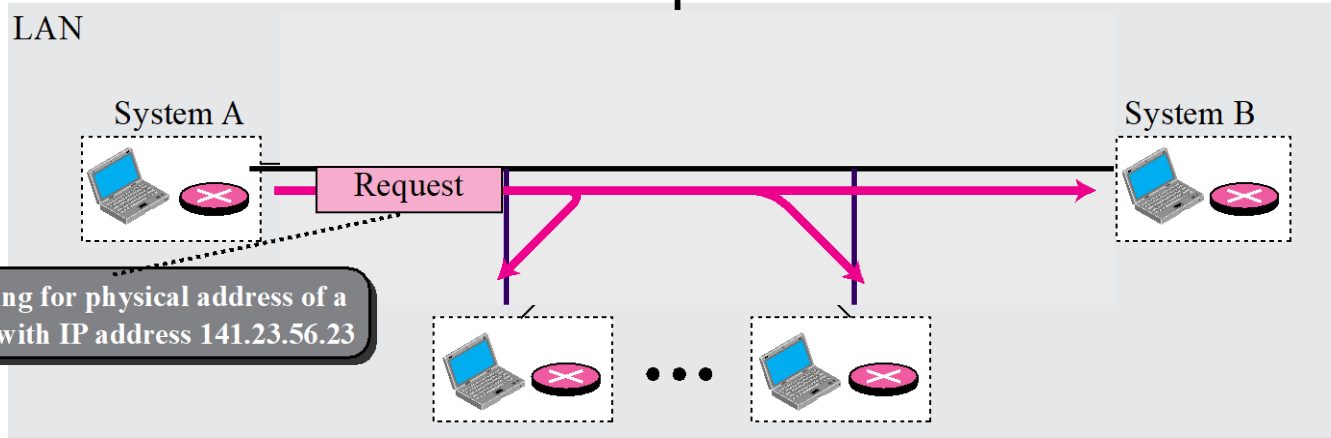


Usado para mapear dinámicamente dir. IPs en dir. físicas (MACs) dentro de la misma red...

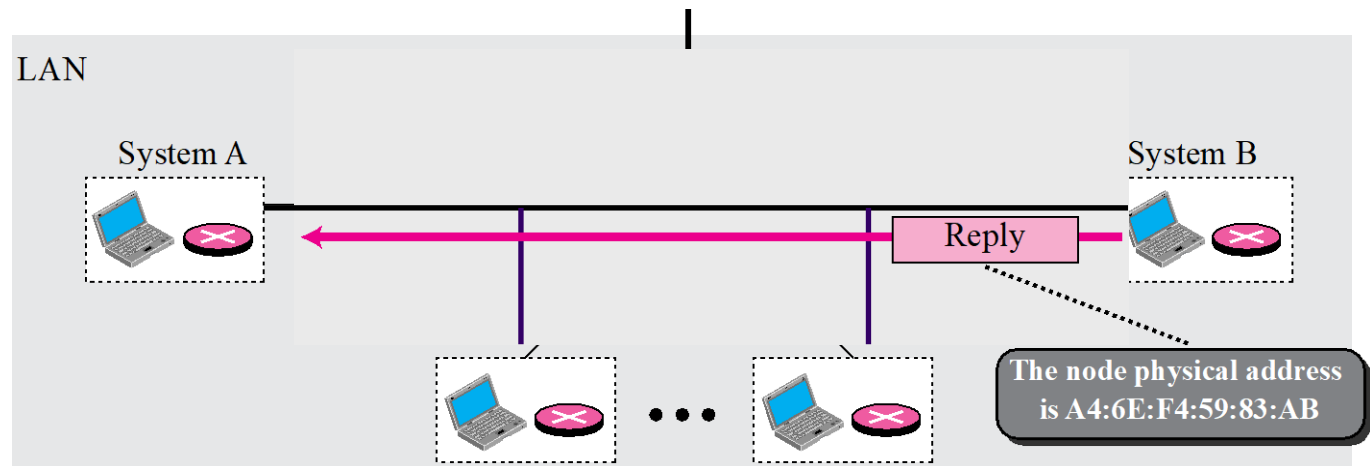
- Sabiendo la IP de destino, Cómo determina su dirección MAC?



ARP operation



a. ARP request is multicast



b. ARP reply is unicast



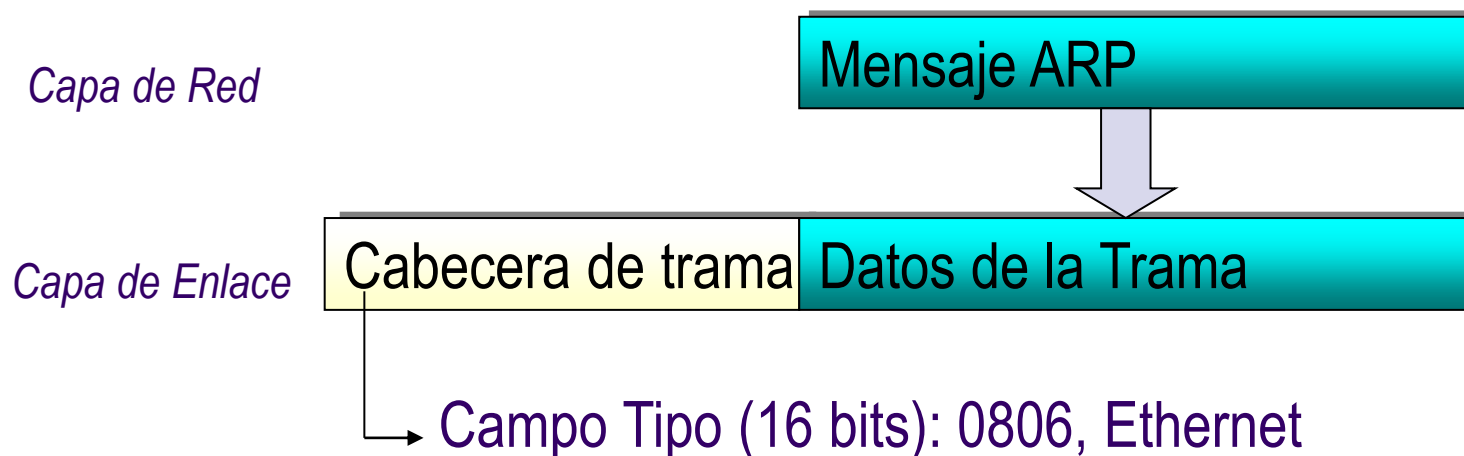
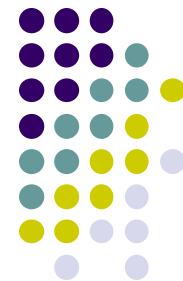
Note

*An ARP request is broadcast;
an ARP reply is unicast.*

Note

*El Tx incluye en cada difusión ARP su
propia IP y MAC para que los receptores
actualicen su memoria intermedia.*

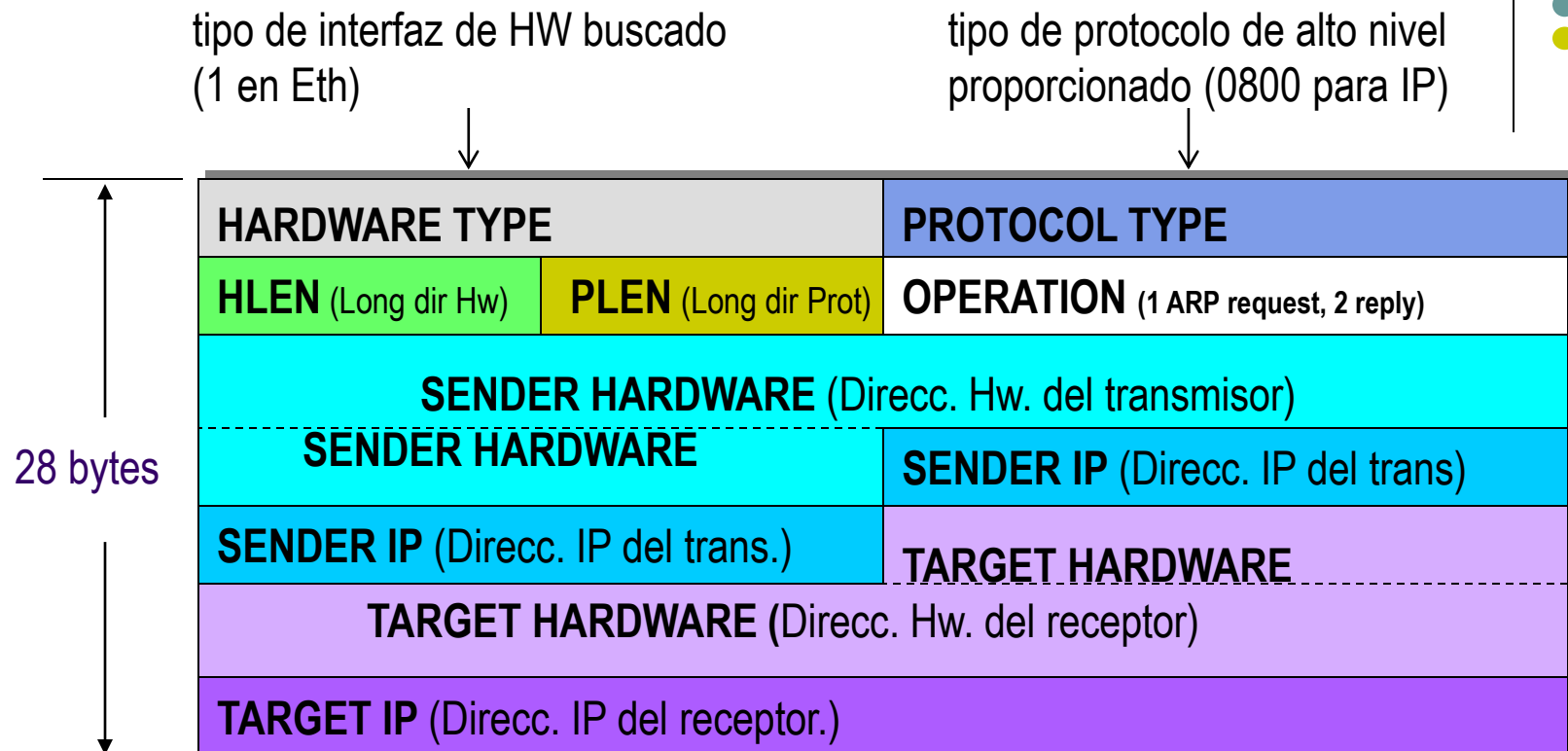
Encapsulation of ARP packet into the frame



Note

El mensaje ARP se encapsula directamente en la trama física


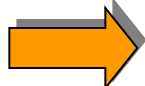



Cabecera ARP



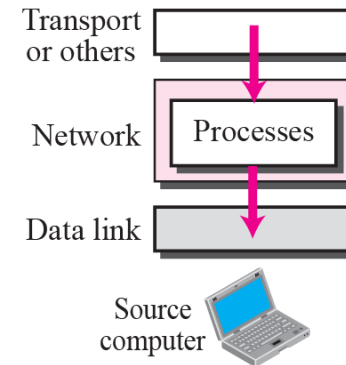
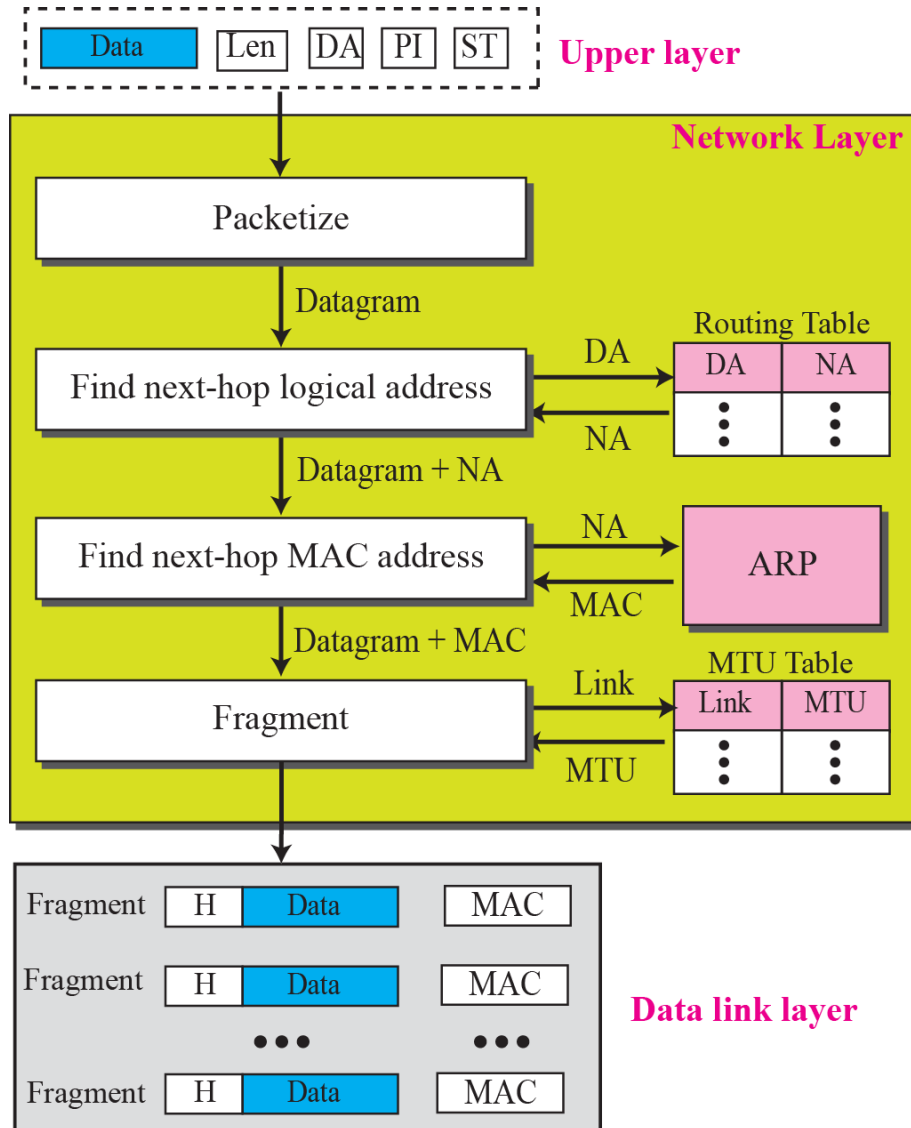
HLEN, PLEN => permiten que ARP se use con redes arbitrarias, ya que estas especifican las longitudes de las direcciones de HW y lógicas o del protocolo de alto nivel

Implantación de ARP



-  ARP realiza:
 -  Transformación de dirección IP en dirección física.
 -  Responde solicitudes.
-  Al inicio se realiza una consulta de una memoria intermedia ARP para ver si existe dirección física del destino. Si no, envía requerimiento ARP.
-  Cuando una consulta ARP llega, extrae dirección IP y dirección física del transmisor. Si no existe esta información en su memoria intermedia lo almacenará.

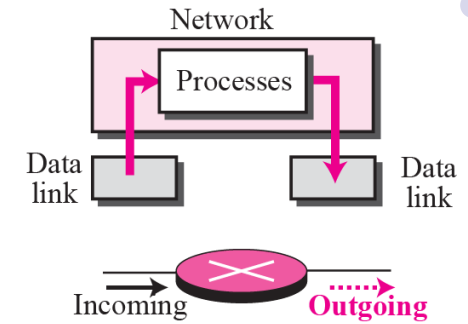
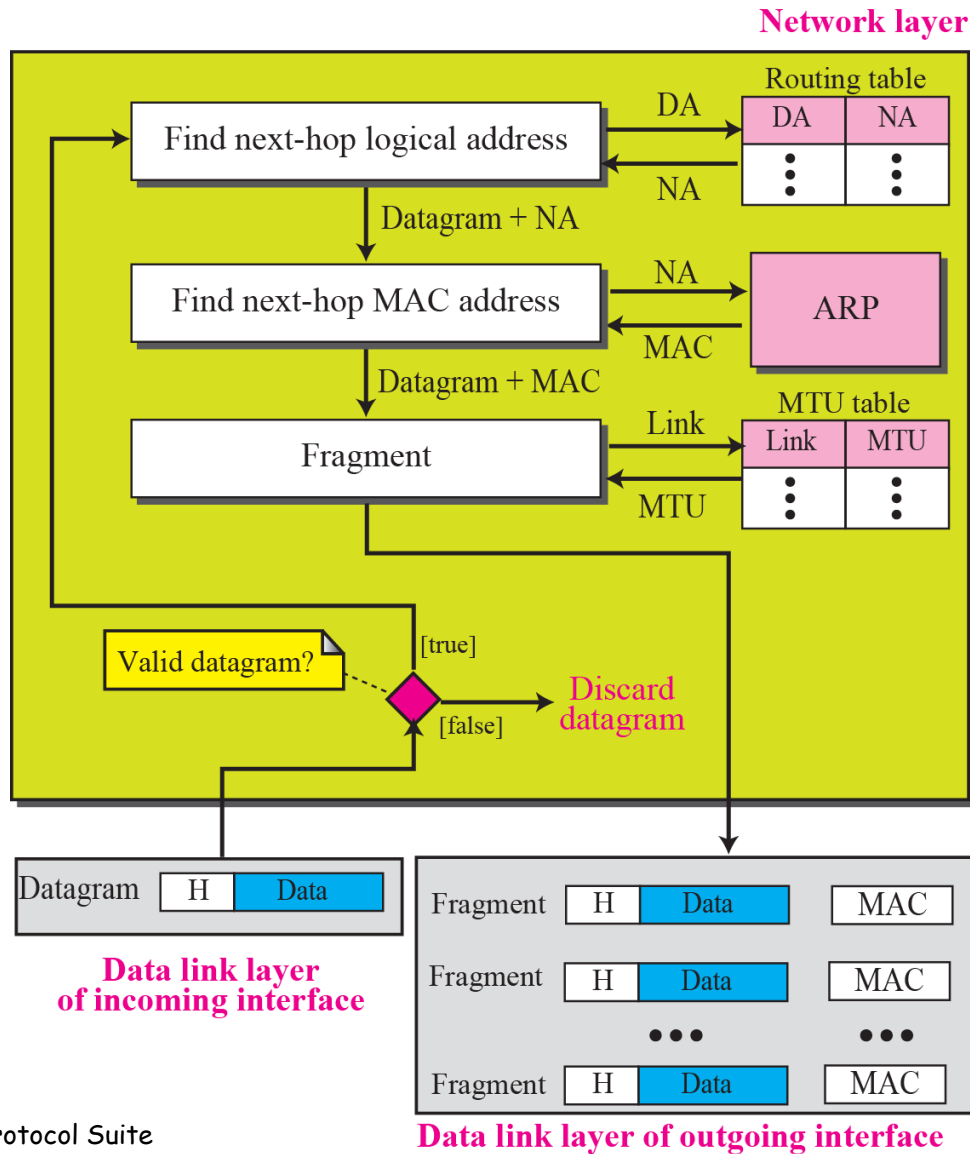
Services provided at the source computer



Legend

Data	Upper layer data
DA	Destination logical address
SA	Source logical address
PI	Protocol ID
ST	Service type
NA	Next-hop logical address
MAC	Next-hop MAC address
MTU	Maximum Transfer Unit
H	Datagram header
Len	Length of data

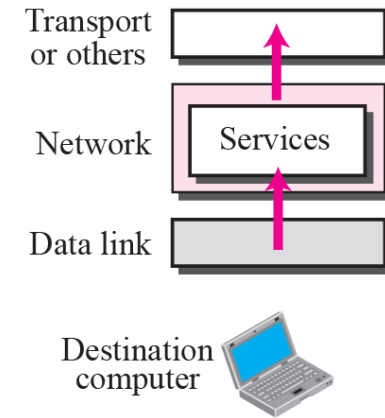
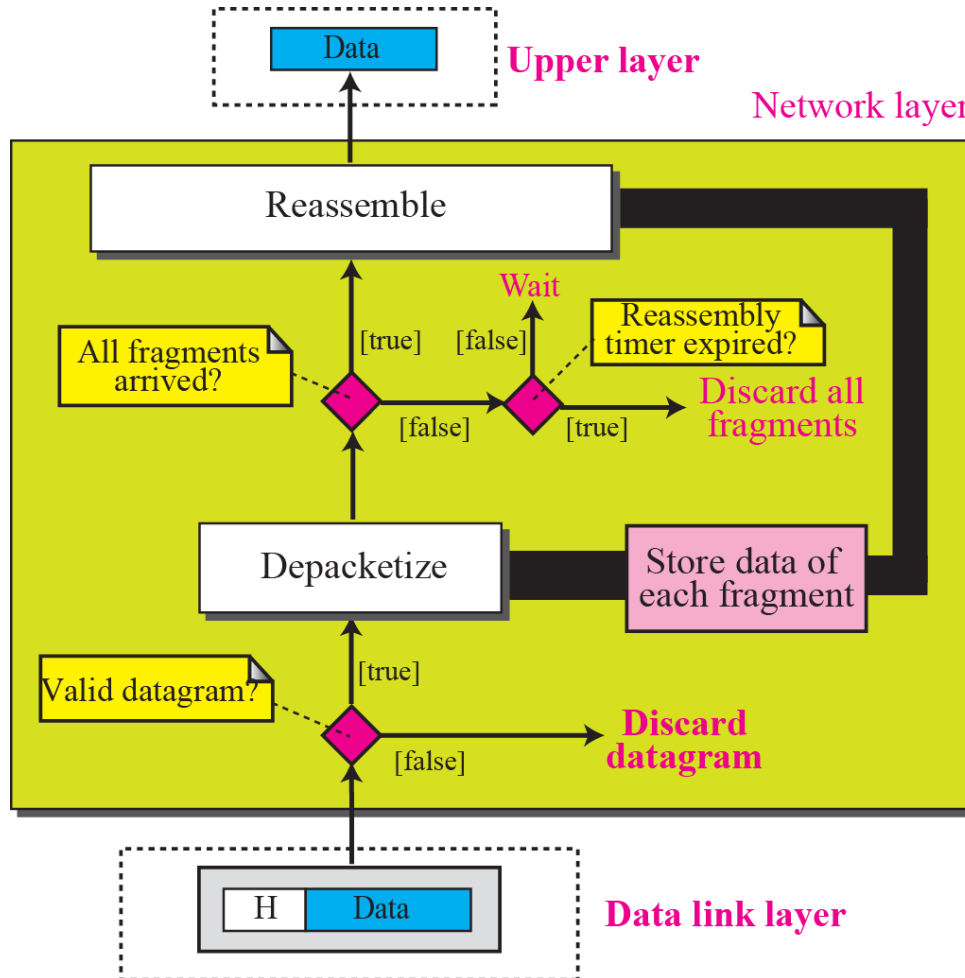
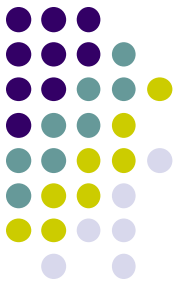
Processing at each router



Legend

Data	Upper layer data
DA	Destination logical address
NA	Next-hop logical address
MAC	Next-hop MAC address
MTU	Maximum Transfer Unit
H	Datagram header

Processing at the destination computer



Legend

Data	Data of upper layer
H	Datagram header

