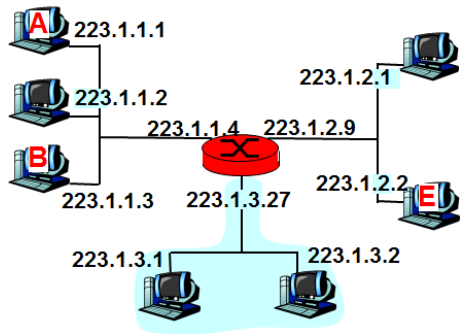
Redes de Datos II
Protocolo IP – Arquitectura

Luis Marrone

LINTI–UNLP

15 de septiembre de 2020



Contenidos

Contenidos

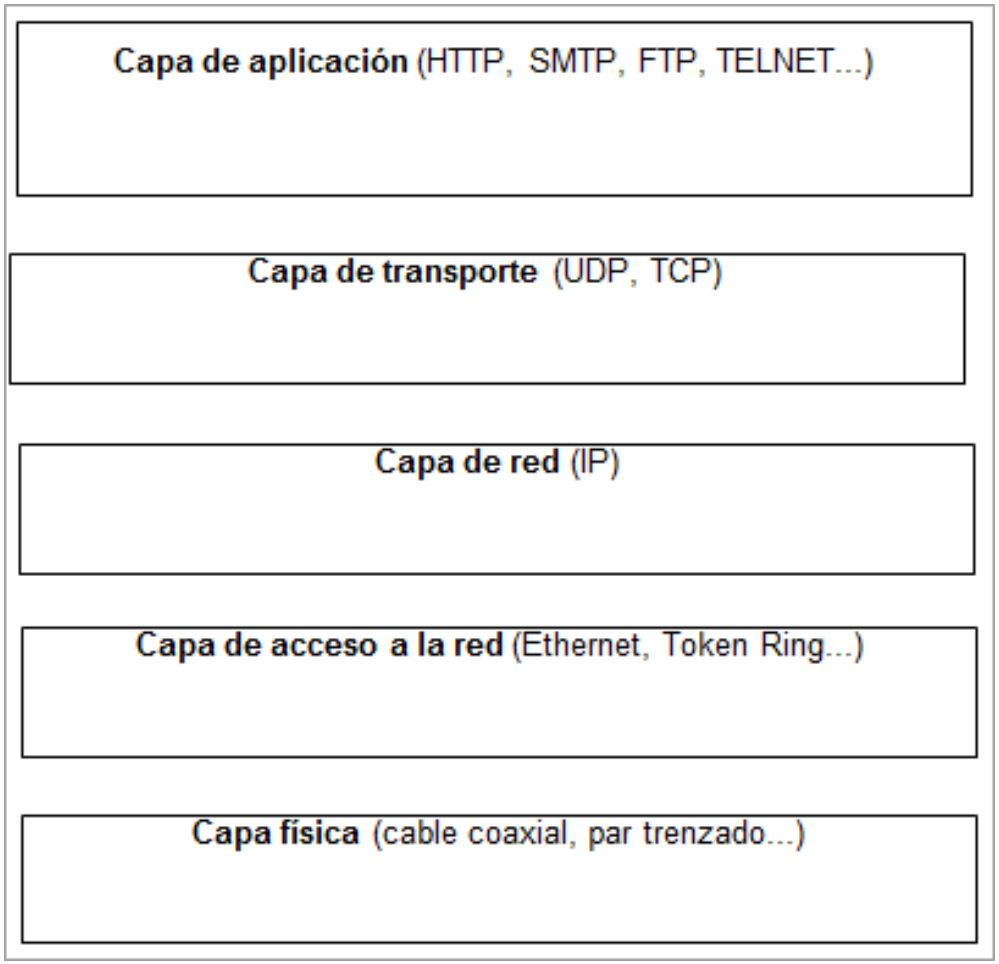
Contenidos

Contenidos

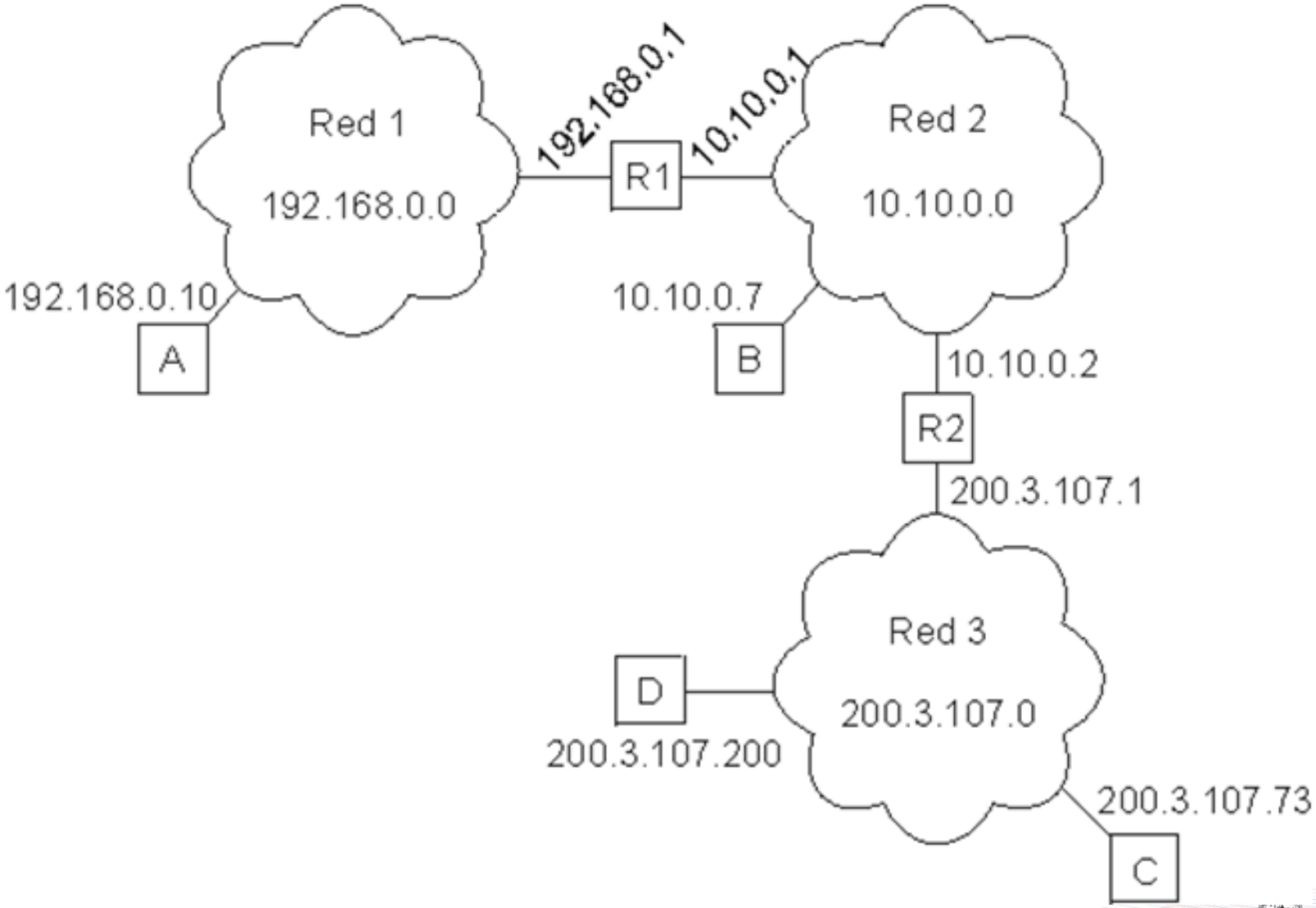
Contenidos

Estamos en:

Modelo TCP/IP



Capa de Red


Red 1
192.168.0.0
192.168.0.1
R1
10.10.0.1
Red 2
10.10.0.0
192.168.0.10
A
10.10.0.7
B
10.10.0.2
R2
200.3.107.1
Red 3
200.3.107.0
D
200.3.107.200
200.3.107.73
C

Estándares IP v4

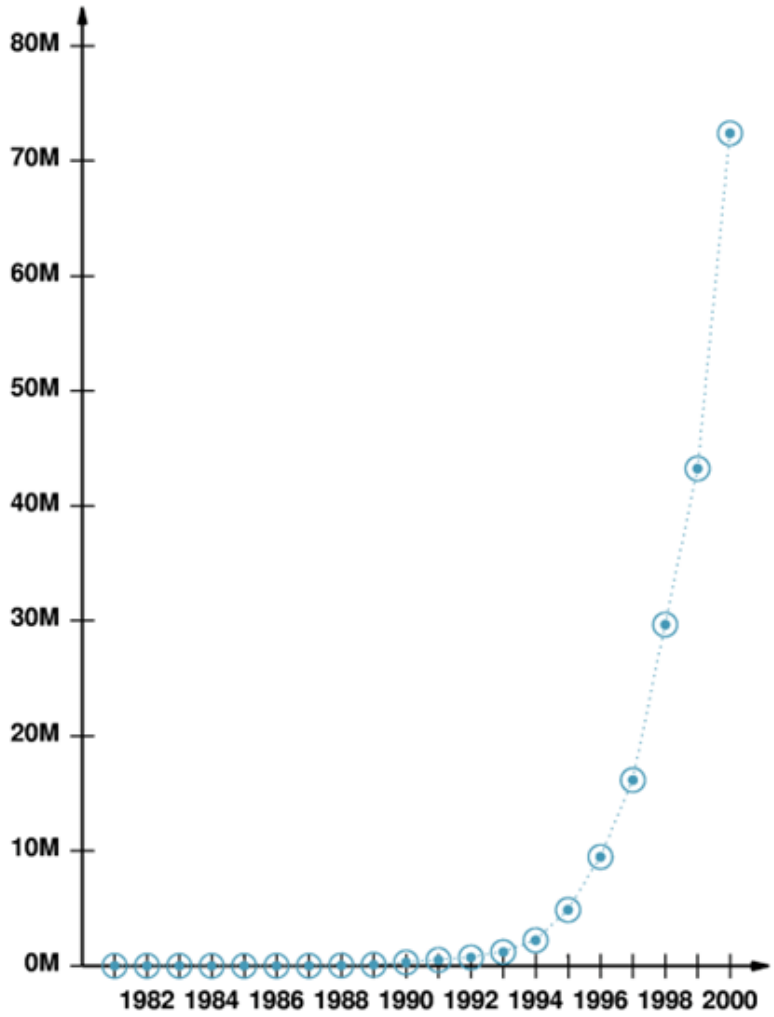
Number	Title	Author or Ed.	Date	More Info (Obs&Upd)	Status
STD0005 RFC0791	**Internet Protocol**	J. Postel	Sep-01-1981	Obsoletes RFC760	STANDARD
STD0005 RFC0792	**Internet Control Message Protocol**	J. Postel	Sep-01-1981	Obsoletes RFC777, Updated by RFC950	STANDARD
STD0005 RFC0919	**Broadcasting Internet Datagrams**	J.C. Mogul	Oct-01-1984		STANDARD
STD0005 RFC0922	**Broadcasting Internet datagrams in the presence of subnets**	J.C. Mogul	Oct-01-1984		STANDARD
STD0005 RFC0950	**Internet Standard Subnetting Procedure**	J.C. Mogul, J. Postel	Aug-01-1985	Updates RFC792	STANDARD
STD0005 RFC1112	**Host extensions for IP multicasting**	S.E. Deering	Aug-01-1989	Obsoletes RFC988, RFC1054, Updated by RFC2236	STANDARD

Internet

- ✓ Proyecto DARPA a comienzos de los 70s.
- ✓ Introduce el concepto de conmutación de paquetes.
- ✓ Introduce el concepto de arquitectura abierta

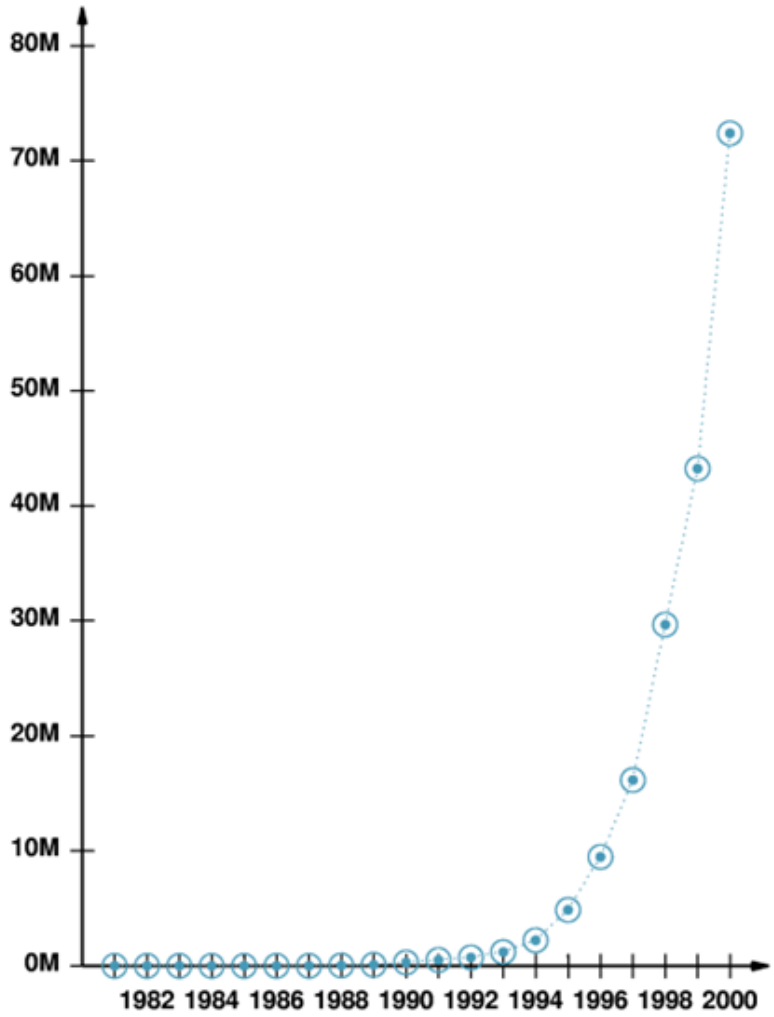
Internet

- ✓ Crecimiento exponencial.
- ✓ Servicios de alto valor agregado.

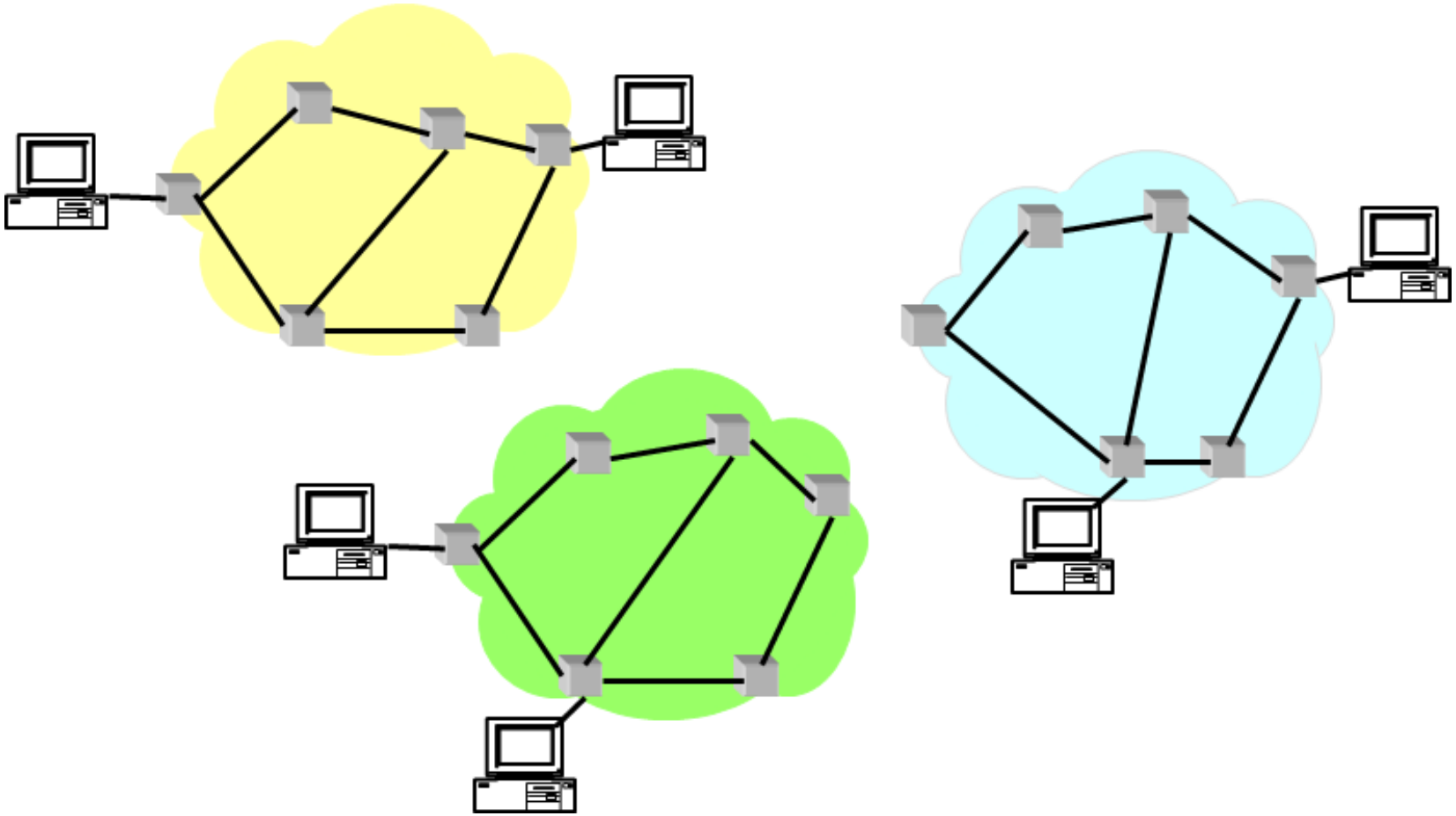


Internet

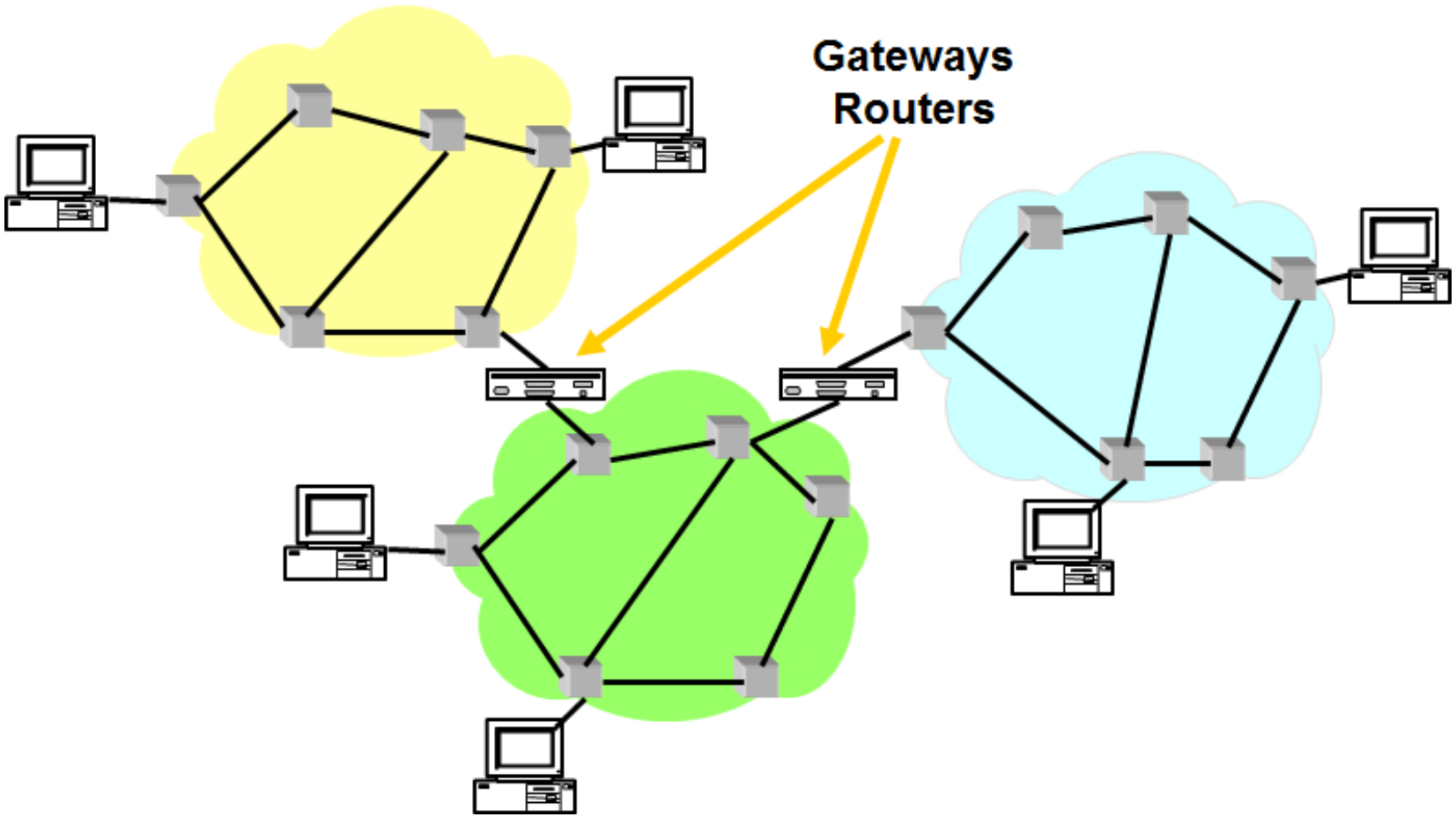
- ✓ Crecimiento exponencial.
- ✓ Servicios de alto valor agregado.



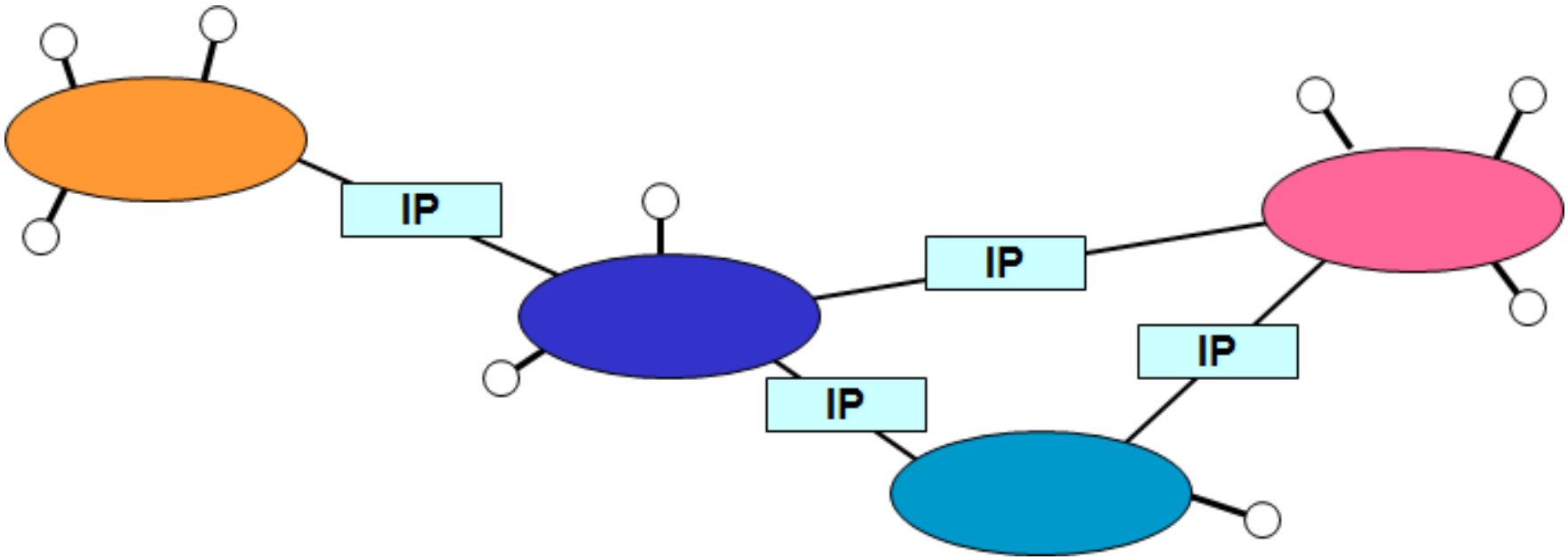
Contexto de IP



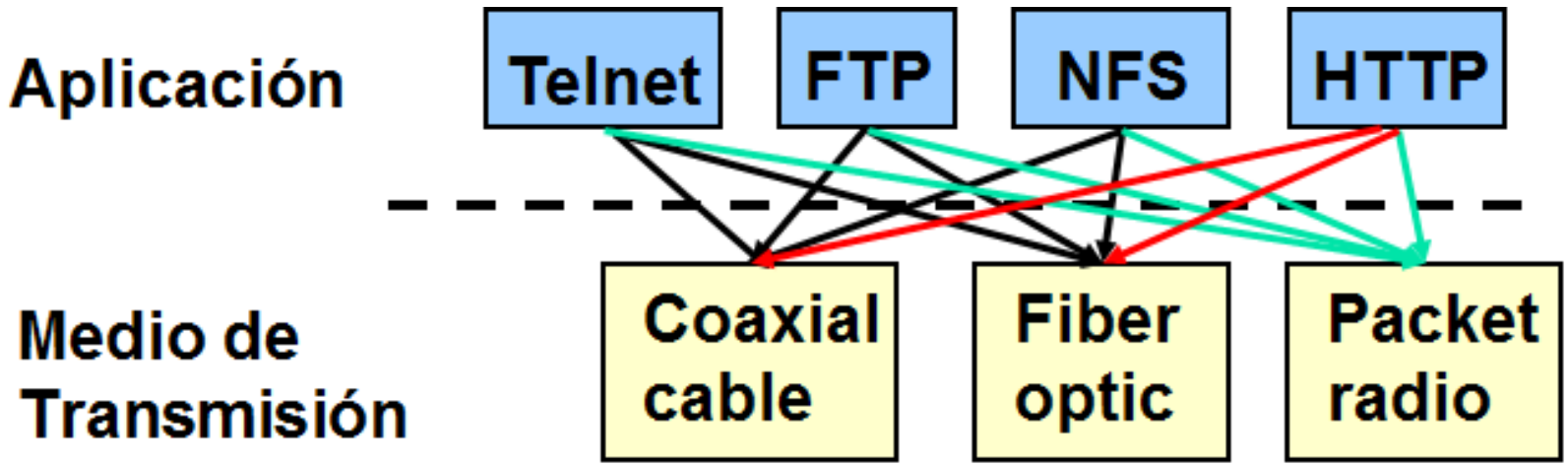
Contexto de IP



Solución IP

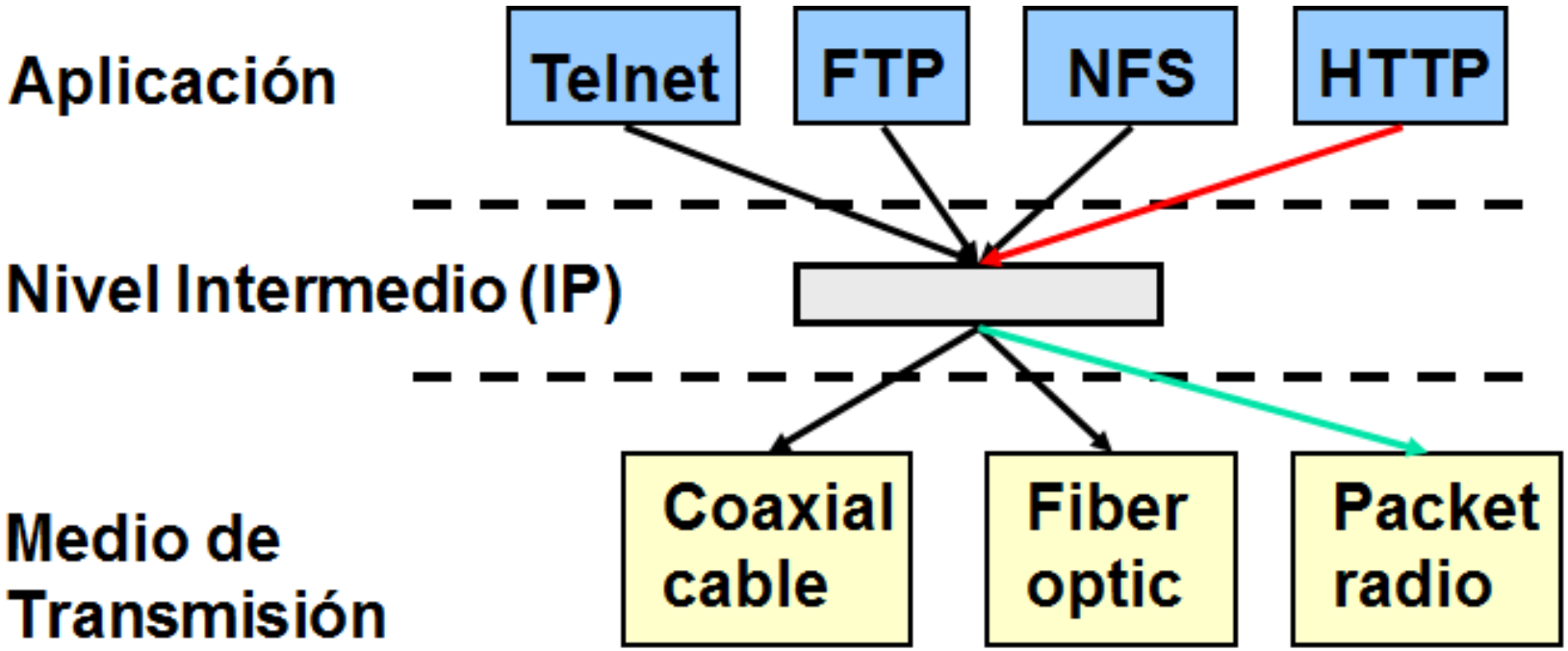


Antes de IP



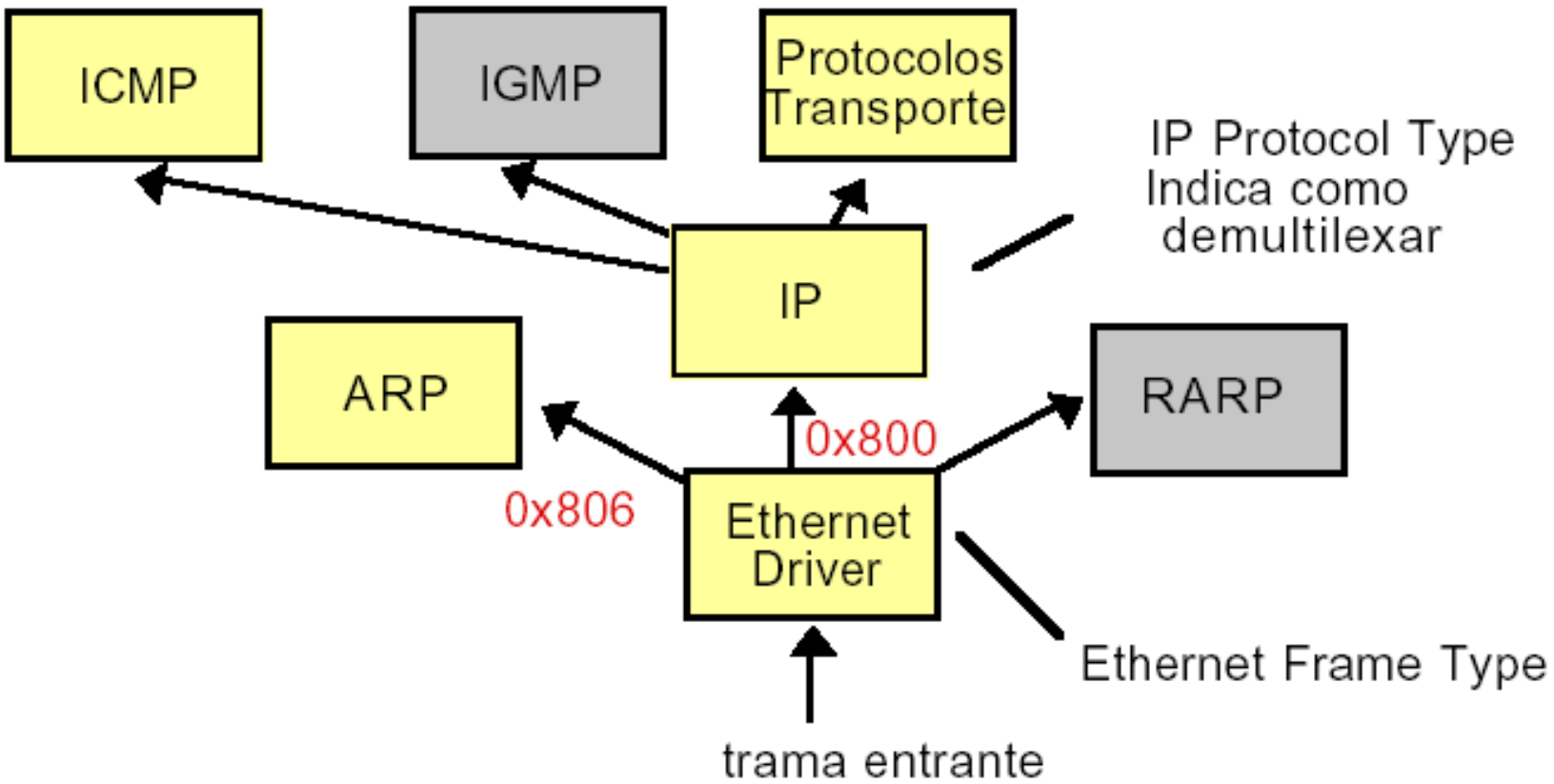
Cada nueva aplicación debía rediseñarse acorde con la nueva tecnología.

Con IP



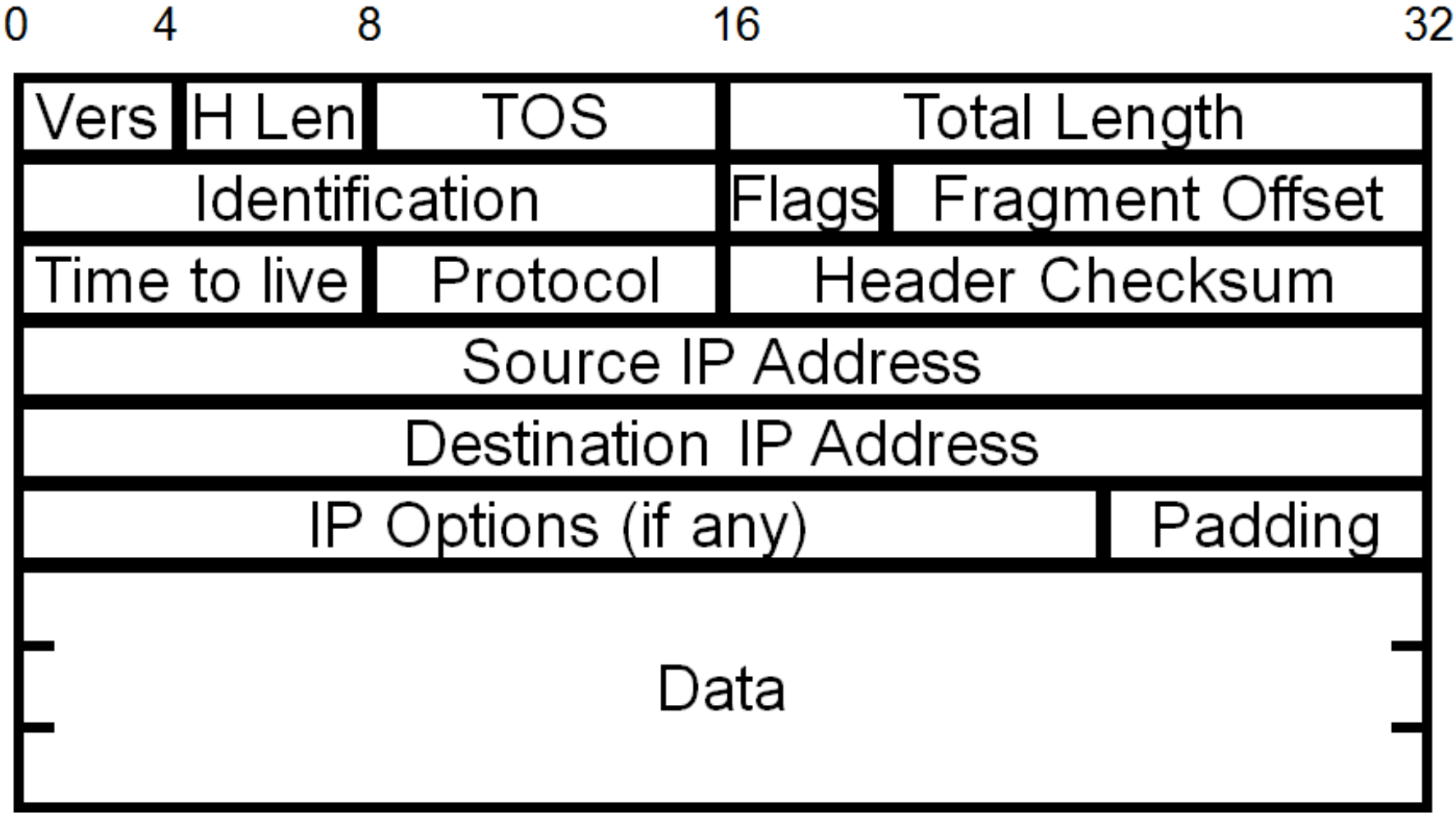
Se requiere un solo mapping de la aplicación/red a IP.

Familia de Protocolos

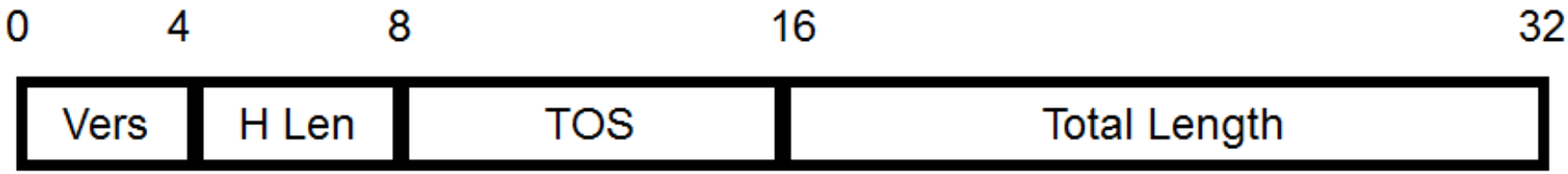


Estamos en:

Estructura del Datagrama IP

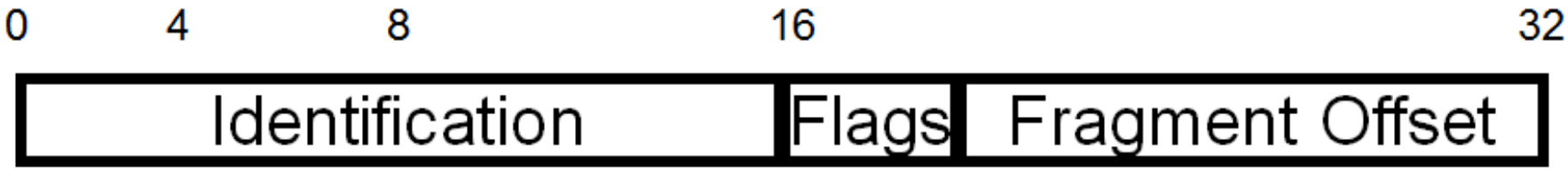


Primer Palabra



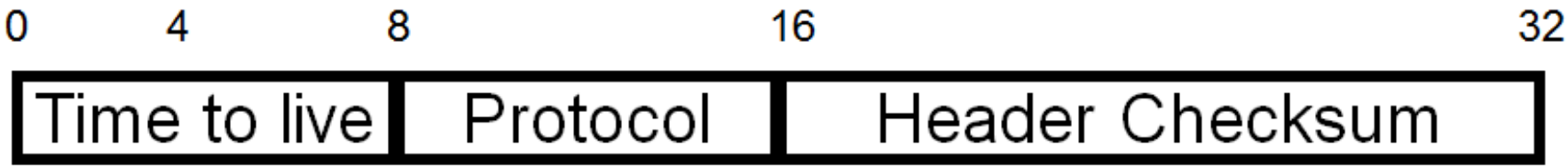
- ✓ Version(4 bits)
- ✓ H Len (4 bits) : longitud del encabezamiento en palabras de 32 bits.
- ✓ TOS (8 bits) : confiabilidad, prioridad, retardo y throughput.
- ✓ Total Length (16 bits) : Longitud total del datagrama en bytes.

Segunda Palabra: Fragmentación



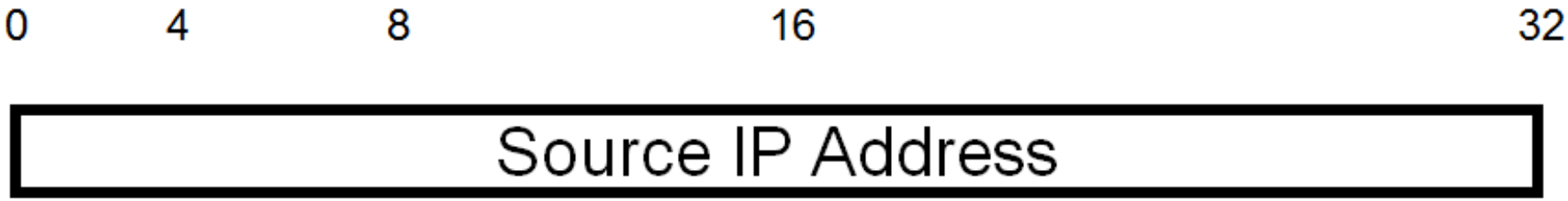
- ✓ Identification(16 bits): único para todos los segmentos del mismo datagrama.
- ✓ Flags(3 bits):
  - X(Sin asignar)
  - D (Don't fragment)
  - M (More fragments
- ✓ Fragment offset(13 bits): ubicación del segmento dentro del datagrama. En unidades de 8 bytes.

Tercer Palabra

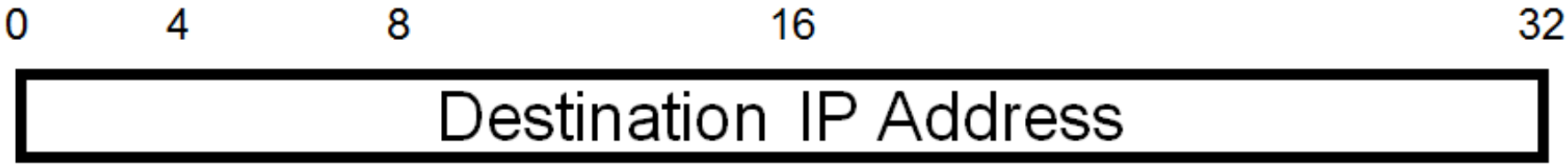


- ✓ Time To Live(8 bits):se decrementa por cada salto.
- ✓ Protocol(8 bits):indica el protocolo que contiene el campo de datos.
- ✓ Header Checksum(16 bits):control de errores del header.

Cuarta-Quinta Palabras

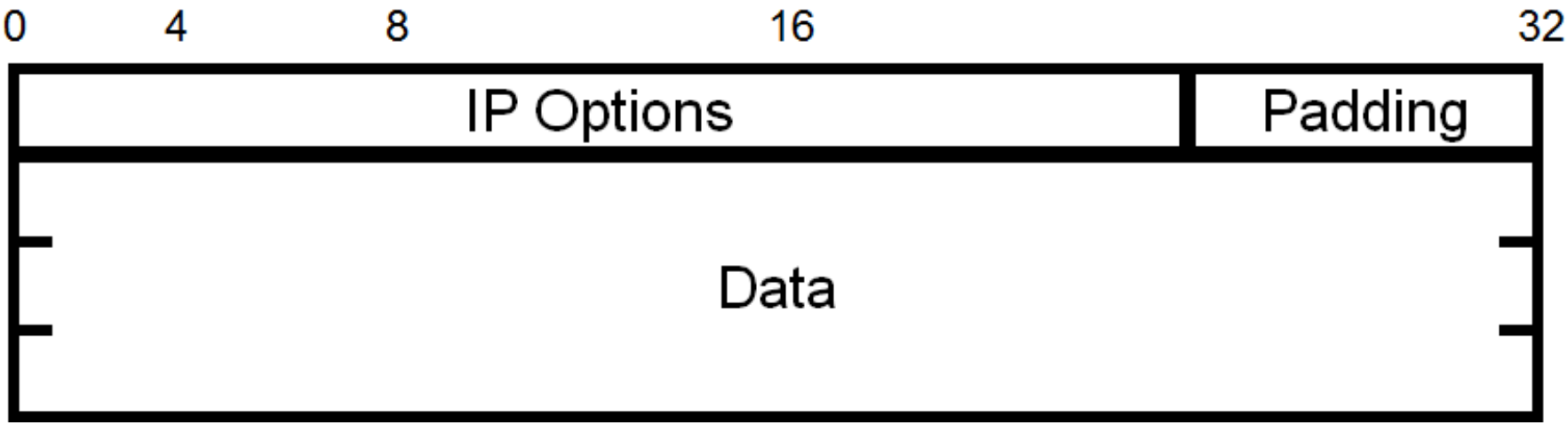


- ✓ Source IP Address(32 bits):dirección del host origen.



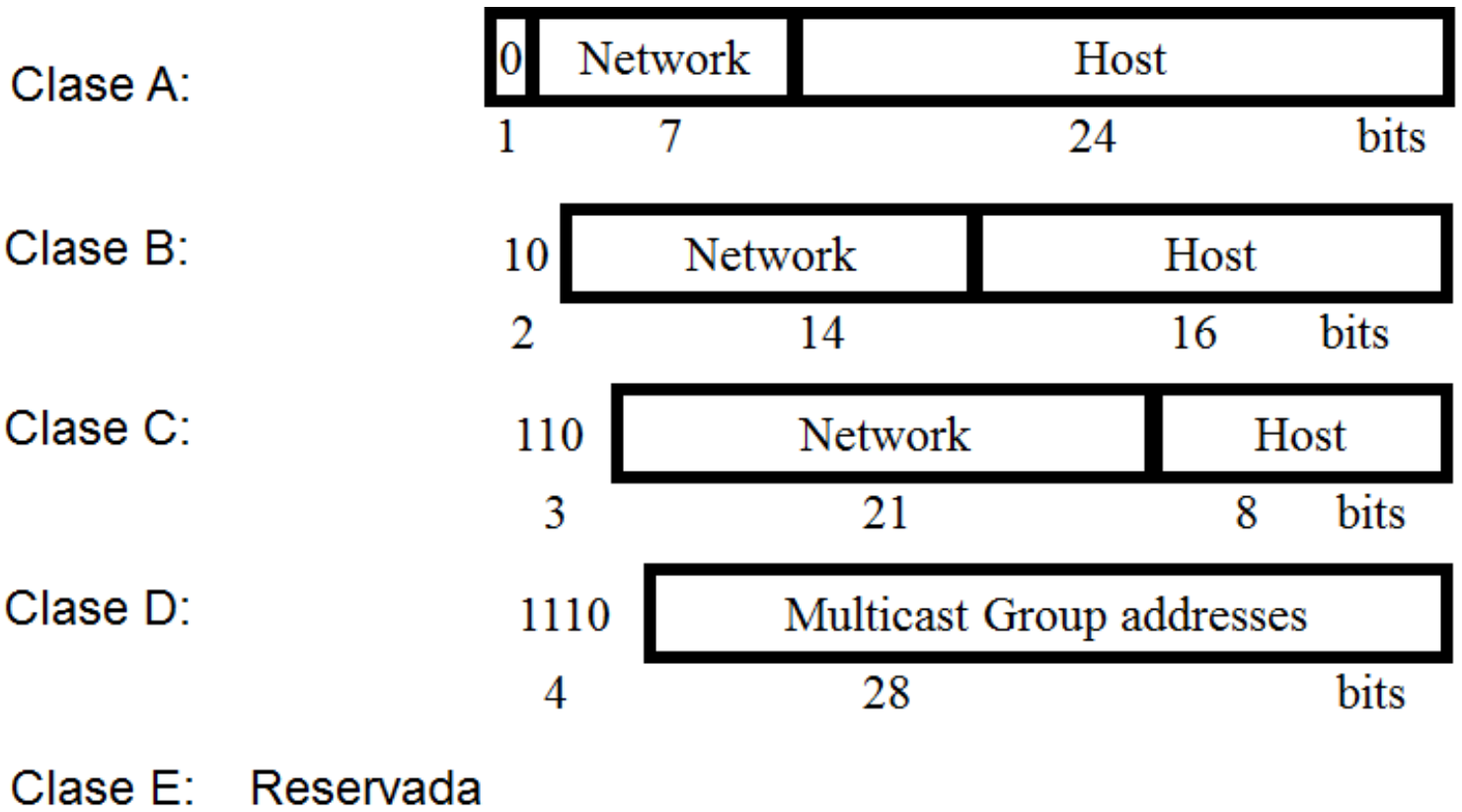
- ✓ Destination IP Address(32 bits):dirección del host destino

Opciones



- ✓ Opciones:longitud variable. Seguridad, source route, echo, etc.
- ✓ Padding:longitud variable. Completa header en palabras de 32 bits.
- ✓ Data/Payload:longitud variable en múltiplos de 8 bits. Data + header $\leq$ 65.536 bytes.

Direcciones IP



Tipos de Direcciones

- ✓ Unicast: Identifican a un único host/interfaz. 123.13.2.45.
- ✓ Broadcast: Identifican a todos los hosts de una red. Los bits del campo de host en uno: 123.255.255.255
- ✓ Multicast: Identifican a un grupo de hosts/interfaces. 224.0.0.0 a la 239.255.255.255.
- ✓ Anycast: Más que un tipo de dirección es un direccionamiento. Identifica a un grupo de hosts/interfaces y logra que llegue a uno de ellos según el protocolo de ruteo. La dirección se toma del espacio de las direcciones unicast.

Tipos de Direcciones

- ✓ Unicast: Identifican a un único host/interfaz. 123.13.2.45.
- ✓ Broadcast: Identifican a todos los hosts de una red. Los bits del campo de host en uno: 123.255.255.255
- ✓ Multicast: Identifican a un grupo de hosts/interfaces. 224.0.0.0 a la 239.255.255.255.
- ✓ Anycast: Más que un tipo de dirección es un direccionamiento. Identifica a un grupo de hosts/interfaces y logra que llegue a uno de ellos según el protocolo de ruteo. La dirección se toma del espacio de las direcciones unicast.

Tipos de Direcciones

- ✓ Unicast: Identifican a un único host/interfaz. 123.13.2.45.
- ✓ Broadcast: Identifican a todos los hosts de una red. Los bits del campo de host en uno: 123.255.255.255
- ✓ Multicast: Identifican a un grupo de hosts/interfaces. 224.0.0.0 a la 239.255.255.255.
- ✓ Anycast: Más que un tipo de dirección es un direccionamiento. Identifica a un grupo de hosts/interfaces y logra que llegue a uno de ellos según el protocolo de ruteo. La dirección se toma del espacio de las direcciones unicast.

Tipos de Direcciones

- ✓ Unicast: Identifican a un único host/interfaz. 123.13.2.45.
- ✓ Broadcast: Identifican a todos los hosts de una red. Los bits del campo de host en uno: 123.255.255.255
- ✓ Multicast: Identifican a un grupo de hosts/interfaces. 224.0.0.0 a la 239.255.255.255.
- ✓ Anycast: Más que un tipo de dirección es un direccionamiento. Identifica a un grupo de hosts/interfaces y logra que llegue a uno de ellos según el protocolo de ruteo. La dirección se toma del espacio de las direcciones unicast.

Direcciones especiales

- ✓ Los bits del campo de hosts en 0 identifican la red. 123.0.0.0.
- ✓ Los bits del campo de hosts en 1 es la dirección broadcast de la red correspondiente. 123.255.255.255
- ✓ Loopback. Red 127.0.0.0. Los datagramas con este destino no se transmiten a la red. Produce un loopback dentro del host que la emite.

Direcciones especiales

- ✓ Los bits del campo de hosts en 0 identifican la red. 123.0.0.0.
- ✓ Los bits del campo de hosts en 1 es la dirección broadcast de la red correspondiente. 123.255.255.255
- ✓ Loopback. Red 127.0.0.0. Los datagramas con este destino no se transmiten a la red. Produce un loopback dentro del host que la emite.

Direcciones especiales

- ✓ Los bits del campo de hosts en 0 identifican la red. 123.0.0.0.
- ✓ Los bits del campo de hosts en 1 es la dirección broadcast de la red correspondiente. 123.255.255.255
- ✓ Loopback. Red 127.0.0.0. Los datagramas con este destino no se transmiten a la red. Produce un loopback dentro del host que la emite.

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

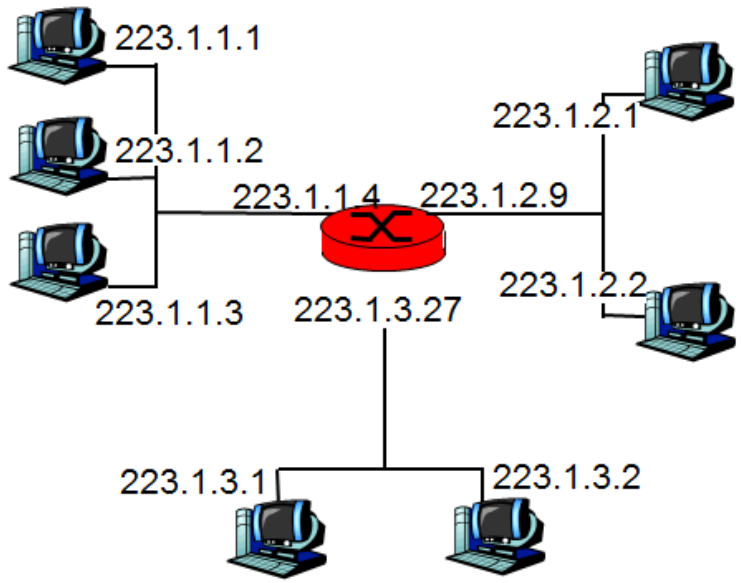
Direcciones Privadas

- ✓ Comúnmente utilizadas en Intranets
- ✓ Redes autónomas sin conexión a Internet
- ✓ Los routers de acceso a Internet las filtran
- ✓ RFC 1918
- ✓ Clase A:
  - 10.0.0.0
- ✓ Clase B:
  - 172.16.0.0 – 172.31.0.0
- ✓ Clase C
  - 192.168.0.0 – 192.168.255.0

Estamos en:

Introducción

- Dirección IP : Identificador de 32-bit para el host e interfaz del router
- Interfaz: conexión entre el host, router y enlace físico.
- Los hosts en la misma red tienen el mismo network ID



223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Direccionamiento Directo

- ✓ Origen y destino en la misma red.
- ✓ El origen detecta que el destino está en la misma red.
- ✓ Encuentra la dirección MAC del destino.
- ✓ Si no lo encuentra acude a ARP
- ✓ Envía el datagrama IP encapsulado en la trama MAC.
- ✓ En todo el proceso las direcciones IP no cambian.

Direccionamiento Directo

- ✓ Origen y destino en la misma red.
- ✓ El origen detecta que el destino está en la misma red.
- ✓ Encuentra la dirección MAC del destino.
- ✓ Si no lo encuentra acude a ARP
- ✓ Envía el datagrama IP encapsulado en la trama MAC.
- ✓ En todo el proceso las direcciones IP no cambian.

Direccionamiento Directo

- ✓ Origen y destino en la misma red.
- ✓ El origen detecta que el destino está en la misma red.
- ✓ Encuentra la dirección MAC del destino.
- ✓ Si no lo encuentra acude a ARP
- ✓ Envía el datagrama IP encapsulado en la trama MAC.
- ✓ En todo el proceso las direcciones IP no cambian.

Direccionamiento Directo

- ✓ Origen y destino en la misma red.
- ✓ El origen detecta que el destino está en la misma red.
- ✓ Encuentra la dirección MAC del destino.
- ✓ Si no lo encuentra acude a ARP
- ✓ Envía el datagrama IP encapsulado en la trama MAC.
- ✓ En todo el proceso las direcciones IP no cambian.

Direccionamiento Directo

- ✓ Origen y destino en la misma red.
- ✓ El origen detecta que el destino está en la misma red.
- ✓ Encuentra la dirección MAC del destino.
- ✓ Si no lo encuentra acude a ARP
- ✓ Envía el datagrama IP encapsulado en la trama MAC.
- ✓ En todo el proceso las direcciones IP no cambian.

Direccionamiento Directo

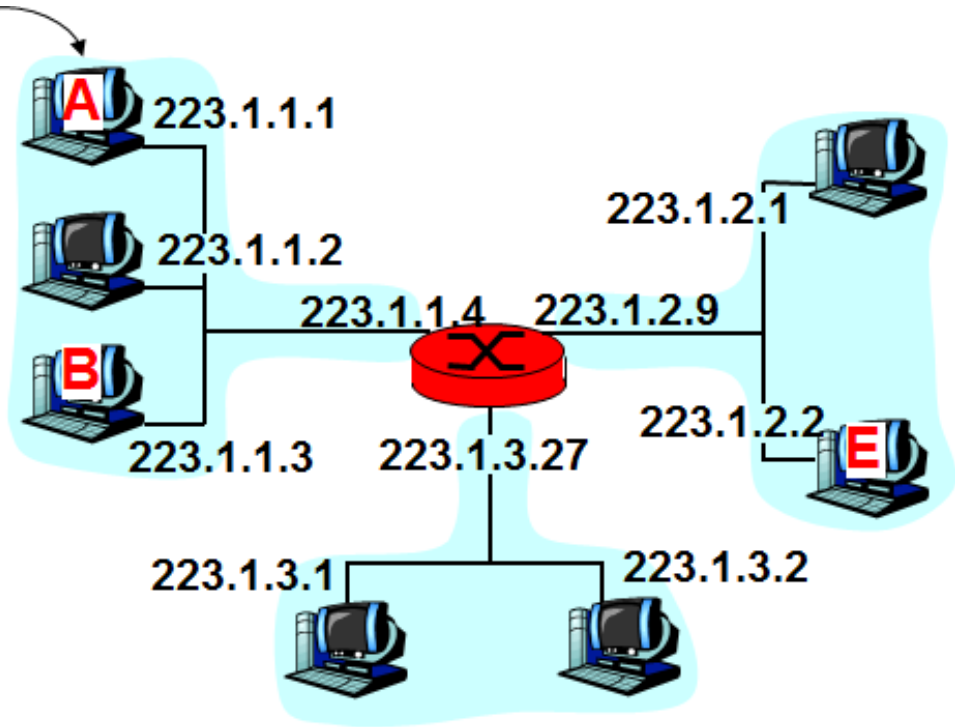
- ✓ Origen y destino en la misma red.
- ✓ El origen detecta que el destino está en la misma red.
- ✓ Encuentra la dirección MAC del destino.
- ✓ Si no lo encuentra acude a ARP
- ✓ Envía el datagrama IP encapsulado en la trama MAC.
- ✓ En todo el proceso las direcciones IP no cambian.

Direccionamiento Directo - Ejemplo

Tabla de ruteo en A

Dest.	Próx. rout	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2

camp head	223.1.1.1	223.1.1.3	data



Protocolo Auxiliar: ARP

- ✓ El host origen envía un mensaje broadcast preguntando: ¿Cuál es el MAC address del destino IP?
- ✓ El host cuyo address IP destino coincide responde: El MAC address de mi dirección IP es: xx:xx:xx:xx:xx:xx

Protocolo Auxiliar: ARP

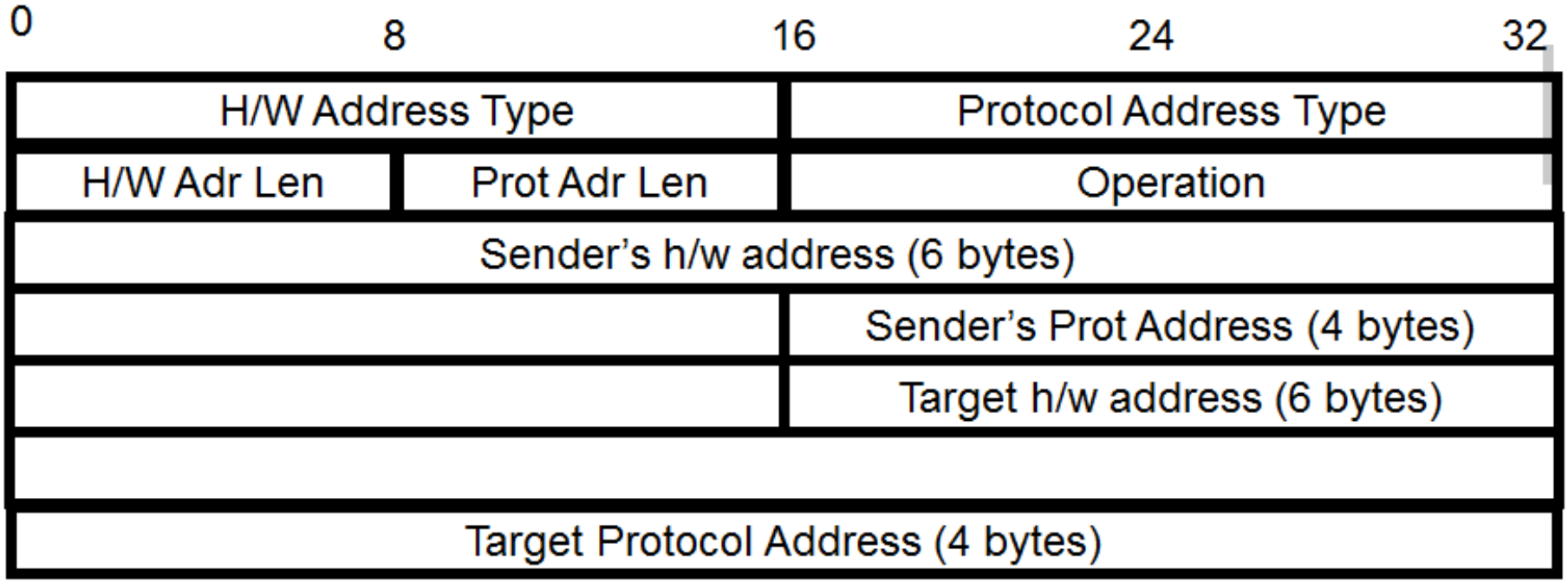
- ✓ El host origen envía un mensaje broadcast preguntando: ¿Cuál es el MAC address del destino IP?

- ✓ El host cuyo address IP destino coincide responde: El MAC address de mi dirección IP es: xx:xx:xx:xx:xx:xx

Datos ARP

- ✓ RFC 826 - STD 37
- ✓ Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware - D. Plummer - Noviembre 1982
- ✓ Actualizado por RFC 5227, RFC 5494
- ✓ El EtherType para ARP es 0x0806

Formato del mensaje ARP



- Hardware address Type : Tipo de protocolo del nivel 2.
- Protocol address Type : Tipo de protocolo de nivel 3 (IP= 0800)16).
- Operation : 1= request, 2= response.

Direccionamiento Indirecto

- ✓ Origen y destino en diferentes redes.
- ✓ El origen detecta que el destino está en otra red.
- ✓ Encuentra el default gateway (router).
- ✓ Envía el datagrama IP encapsulado en la trama MAC con la dirección MAC del default gateway.

Direccionamiento Indirecto

- ✓ Origen y destino en diferentes redes.
- ✓ El origen detecta que el destino está en otra red.
- ✓ Encuentra el default gateway (router).
- ✓ Envía el datagrama IP encapsulado en la trama MAC con la dirección MAC del default gateway.

Direccionamiento Indirecto

- ✓ Origen y destino en diferentes redes.
- ✓ El origen detecta que el destino está en otra red.
- ✓ Encuentra el default gateway (router).
- ✓ Envía el datagrama IP encapsulado en la trama MAC con la dirección MAC del default gateway.

Direccionamiento Indirecto

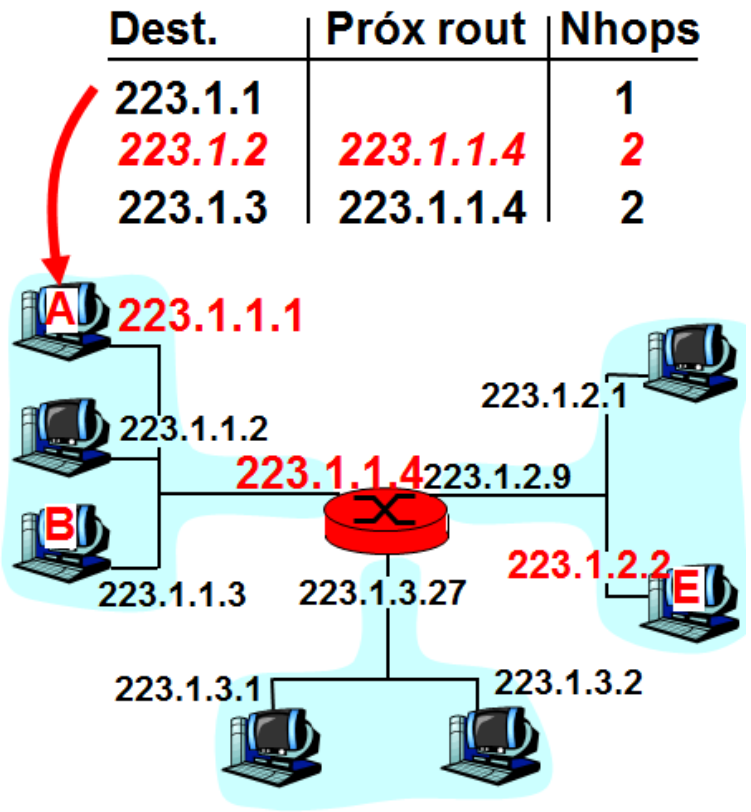
- ✓ Origen y destino en diferentes redes.
- ✓ El origen detecta que el destino está en otra red.
- ✓ Encuentra el default gateway (router).
- ✓ Envía el datagrama IP encapsulado en la trama MAC con la dirección MAC del default gateway.

Direccionamiento Indirecto - 1

A le envía un datagrama a E:

- Tabla de ruteo: próximo salto a E es: 223.1.1.4
- El nivel MAC envía el datagrama al router 223.1.1.4
- El datagrama llega a 223.1.1.4

. . .

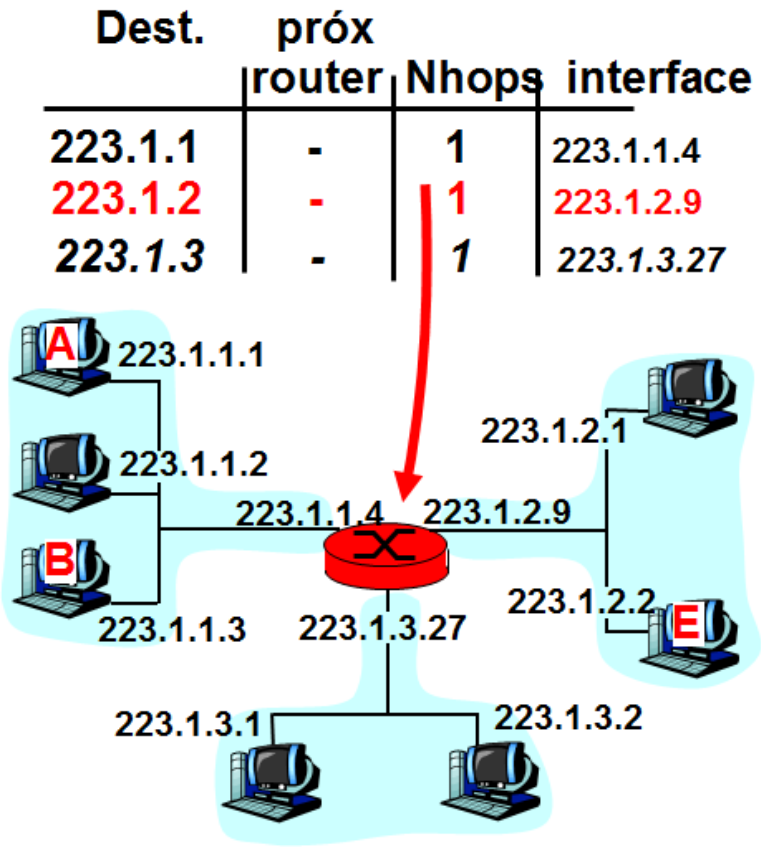


Datagrama enviado por A:

camp head	223.1.1.1	223.1.2.2	data

Direccionamiento Indirecto - 2

- El router detecta que E está directamente conectado a una de sus interfaces.
- El datagrama es despachado a través de 223.1.2.9 .
- El datagrama llega a 223.1.2.2



Estamos en:

¿Por Qué?

- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

¿Por Qué?

- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

¿Por Qué?

- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

¿Por Qué?

- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

¿Por Qué?

- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

¿Por Qué?

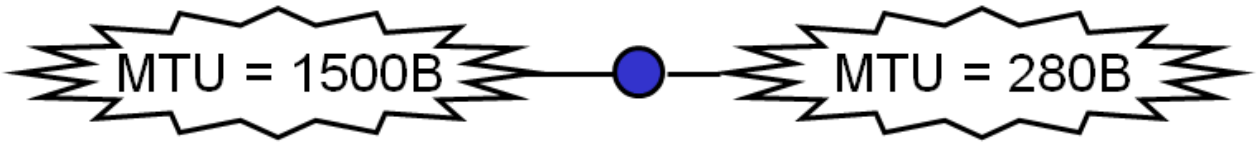
- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

¿Por Qué?

- ✓ MTU: maximum transfer unit.
  - Ethernet= 1500 bytes
  - FDDI= 4500 bytes
  - Se corresponde con la longitud completa del datagrama (header + payload)
- ✓ Los datagramas mayores al MTU deben fragmentarse
- ✓ El header original se copia en cada fragmento y luego se modifica según corresponda
- ✓ Algunas opciones se copian. RFC 791.

Fragmentación - Ejemplo

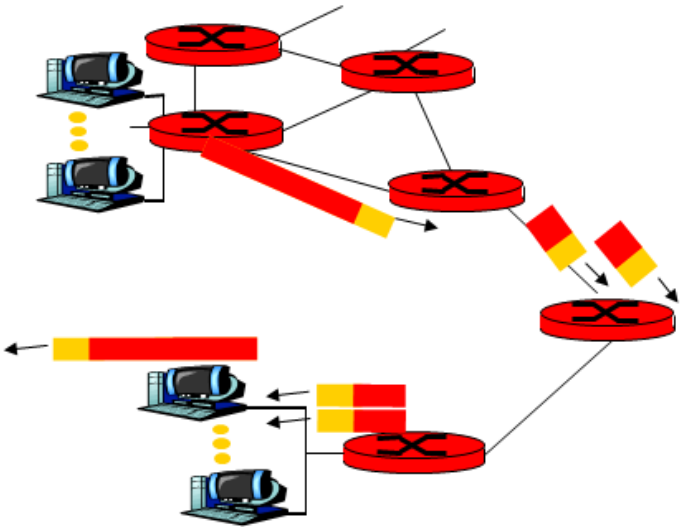
Un payload de 452 bytes debe transmitirse entre una red Ethernet (MTU=1500B) y una línea PPP(MTU=280B).



IHL = 5, ID = 342, More = 0
Offset = 0, Len = 472B

IHL=5, ID = 342, More = 1
Offset = 0, Len = 276B

IHL=5, ID = 342, More = 0
Offset = 32, Len = 216B



Fragmentación - Ejemplo

- ✓ Longitud= 472B, Header = 20B $\Longrightarrow$ Payload = 452B
- ✓ Fragmentos resultantes:

Deben ser múltiplos de 8 bytes
El múltiplo más cercano a 260 (280 - 20B) es 256B
Longitud del primer fragmento = 256B + 20B = 276B
Longitud del segundo fragmento = (452B - 256B) + 20B = 216B

Fragmentación - Ejemplo

- ✓ Longitud= 472B, Header = 20B $\Longrightarrow$ Payload = 452B

- ✓ Fragmentos resultantes:

Deben ser múltiplos de 8 bytes
El múltiplo más cercano a 260 (280 - 20B) es 256B
Longitud del primer fragmento = 256B + 20B = 276B
Longitud del segundo fragmento = (452B - 256B) + 20B = 216B

Fragmentación : Rearmado

- ✓ El datagrama se reconstruye sólo en el destino final
- ✓ Los fragmentos se descartan después de un timeout
- ✓ Los fragmentos pueden a su vez fragmentarse en el resto del camino
- ✓ El MTU mínimo a lo largo del camino $\Longrightarrow$ Path MTU.

Fragmentación : Rearmado

- ✓ El datagrama se reconstruye sólo en el destino final
- ✓ Los fragmentos se descartan después de un timeout
- ✓ Los fragmentos pueden a su vez fragmentarse en el resto del camino
- ✓ El MTU mínimo a lo largo del camino $\Longrightarrow$ Path MTU.

Fragmentación : Rearmado

- ✓ El datagrama se reconstruye sólo en el destino final
- ✓ Los fragmentos se descartan después de un timeout
- ✓ Los fragmentos pueden a su vez fragmentarse en el resto del camino
- ✓ El MTU mínimo a lo largo del camino $\Longrightarrow$ Path MTU.

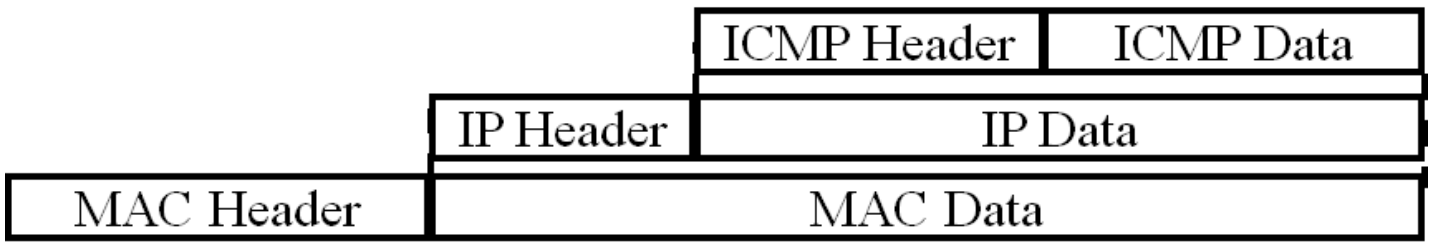
Fragmentación : Rearmado

- ✓ El datagrama se reconstruye sólo en el destino final
- ✓ Los fragmentos se descartan después de un timeout
- ✓ Los fragmentos pueden a su vez fragmentarse en el resto del camino
- ✓ El MTU mínimo a lo largo del camino $\Longrightarrow$ Path MTU.

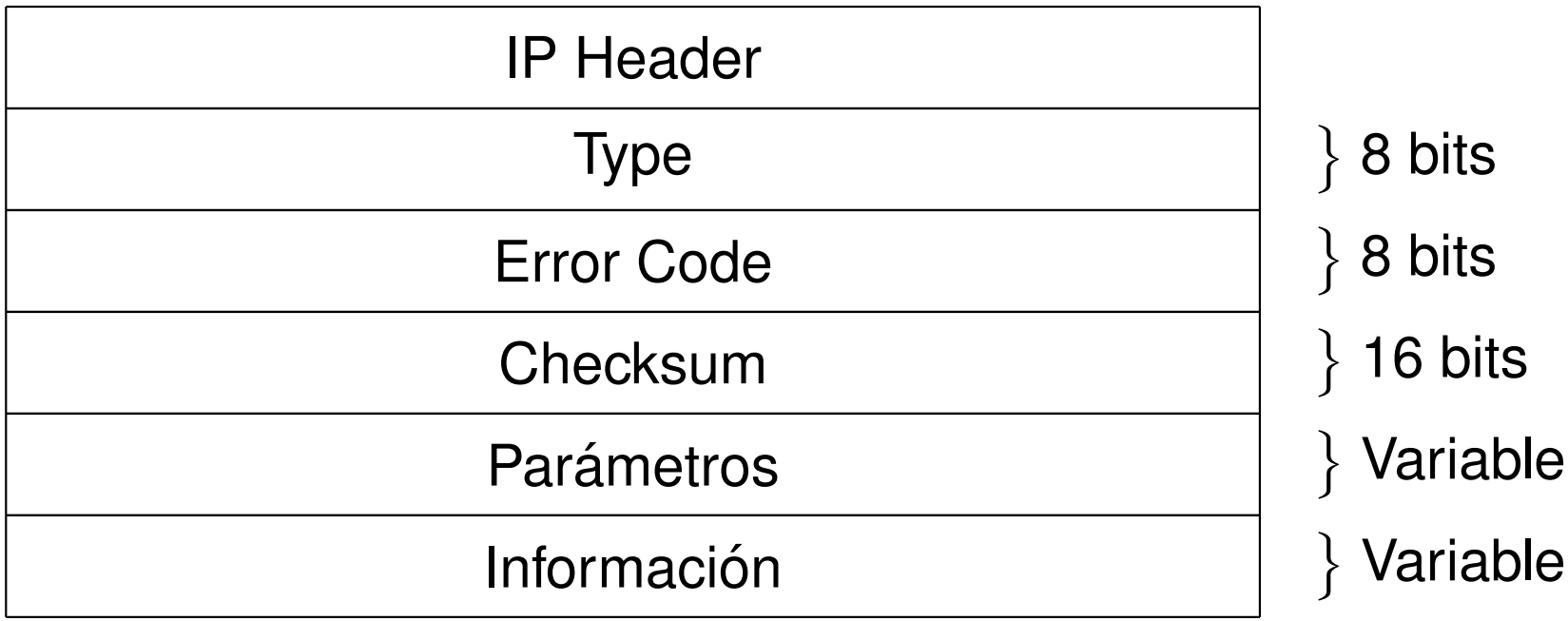
Estamos en:

Datos

- ✓ RFC 792 parte de STD 5
- ✓ Internet Control Message Protocol - J. Postel - Septiembre 1981
- ✓ Actualizada por RFC 950, RFC 4884, RFC 6633, RFC 6918
- ✓ Reporte de errores
- ✓ Envío de mensajes
- ✓ Es informativo. No toma decisiones
- ✓ Se encapsula en IP.
  - Protocol type : 1



ICMP - Formato



Al descartarse un datagrama ICMP incluye el header del datagrama que produjo el mensaje y por lo menos 8 bytes del campo de datos del datagrama.

ICMP - Formato

Type	Message
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded
12	Parameter unintelligible
13	Time-stamp request
14	Time-stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

ICMP - Mensajes

- ✓ Echo Request/Reply: Utilizado en Ping
- ✓ Source Quench: Control de flujo
- ✓ Time Exceeded: Time to live del datagrama llegó a 0 o expiró el timer de fragmentación

Herramientas basadas en ICMP

Ping

- ✓ Utilizado para verificar:
  - Destino alcanzable
  - Calcular round trip time
  - Contar el número de saltos (hops) al destino
  - Record route
- ✓ La falla de Ping no garantiza problemas
- ✓ Los Firewalls pueden filtrarlos

Herramientas basadas en ICMP

Traceroute

- ✓ Hace uso de TTL e ICMP
  - Envía el mensaje con TTL = 1 (hop)
  - EL primer router descarta el mensaje y envía un mensaje ICMP al origen
  - Envía el mensaje con TTL = 2 (hops) etc

Path MTU Discovery

- ✓ Hace uso de Flags del datagrama e ICMP
  - Envía un datagrama con el bit Don't fragment activo
  - Se genera un mensaje ICMP por el descarte, indicando además el MTU
  - Reenvía el datagrama según el MTU recibido