

REDES DE INFORMACIÓN



PROTOCOLOS TCP/IP

DEFINICIONES

INTERNET

ES UN CONJUNTO DE REDES HETEROGENEAS, DISPERSAS E INTERCONECTADAS VIA **TCP/IP**

TCP/IP

CONJUNTO DE **PROTOCOLOS** QUE PERMITEN LA INTERCONEXIÓN ENTRE REDES **HETEROGÉNEAS**.

NO ESTÁN ASOCIADOS A UN SISTEMA OPERATIVO NI PROVEEDOR.

PROTOCOLOS

PROPORCIONAN REGLAS PARA LA COMUNICACIÓN SIN DEPENDER DEL HARDWARE DE RED.

COMPARACIÓN ENTRE MODELO OSI Y TCP/IP

MODELO OSI

APLICACION
PRESENTACION
SESION
TRANSPORTE
RED
ENLACE DE DATOS
FISICO

MODELO TCP/IP

APLICACIÓN
TRANSPORTE
INTERNET
ACCESO A LA RED
FISICA

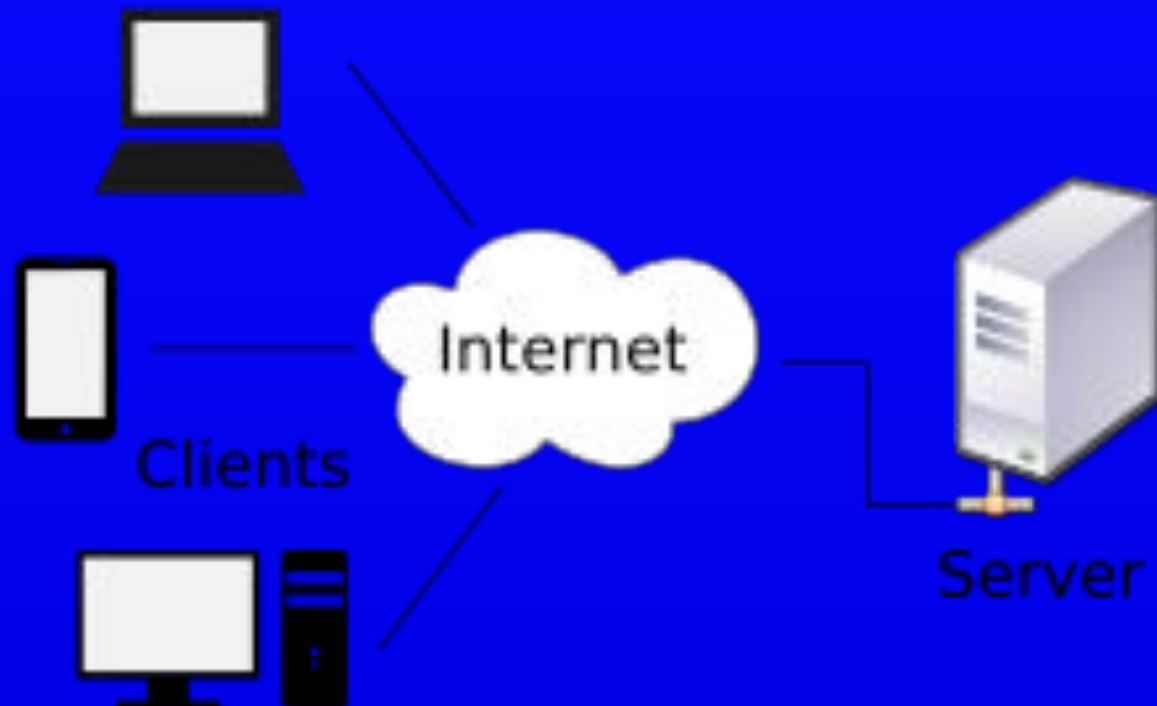
PROTOCOLOS TCP/IP

FTP TELNET SMTP NSP SNMP
TCP UDP
IP ICMP IGMP
ARP RARP

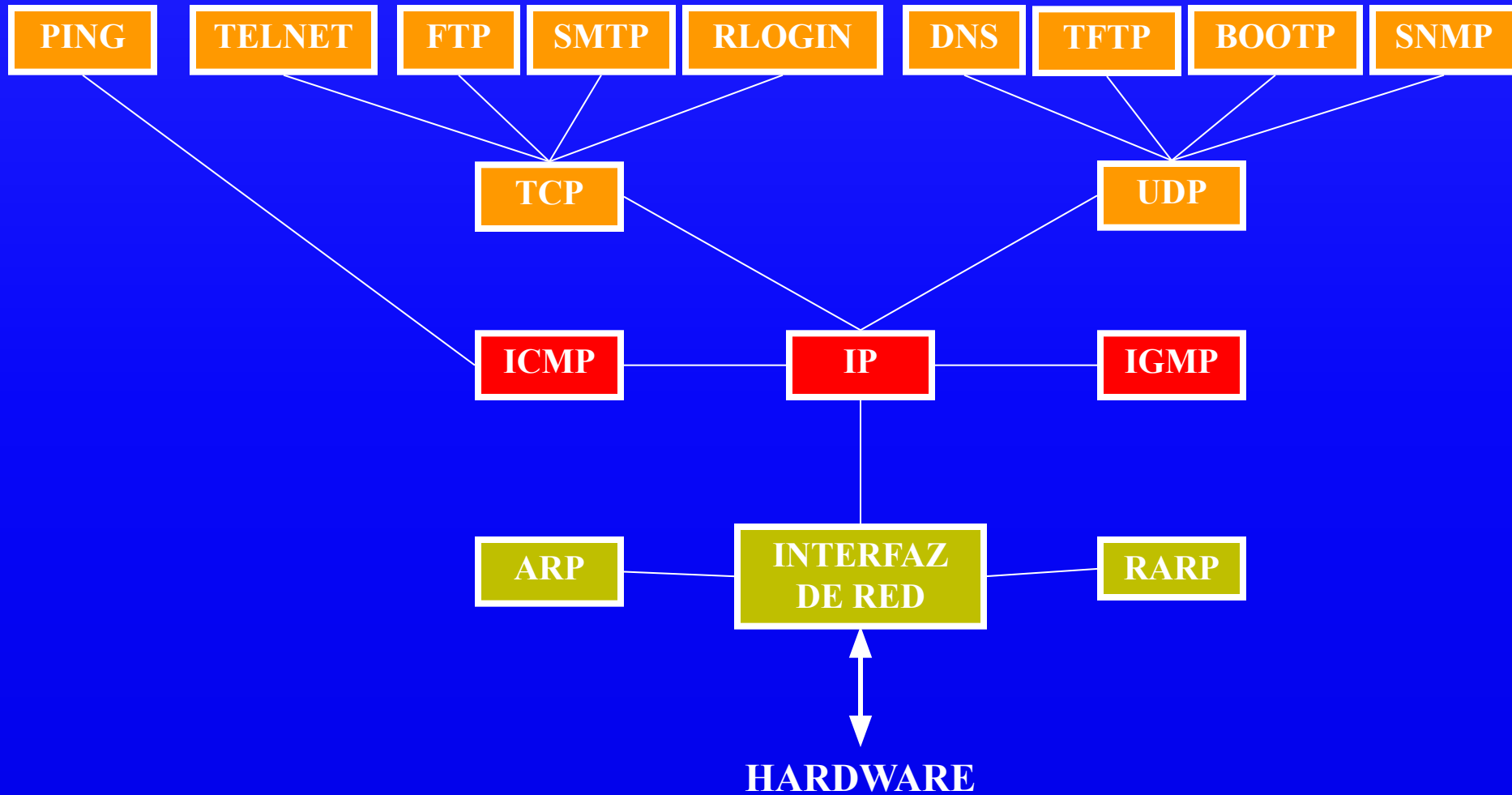
CLIENTE - SERVIDOR

Aplicación distribuida, las tareas se reparten entre los proveedores de servicios, llamados *Servidores*, y los demandantes, llamados *Clientes*.

Un *Cliente* realiza peticiones a otro programa, el *Servidor*, quien le da respuesta.



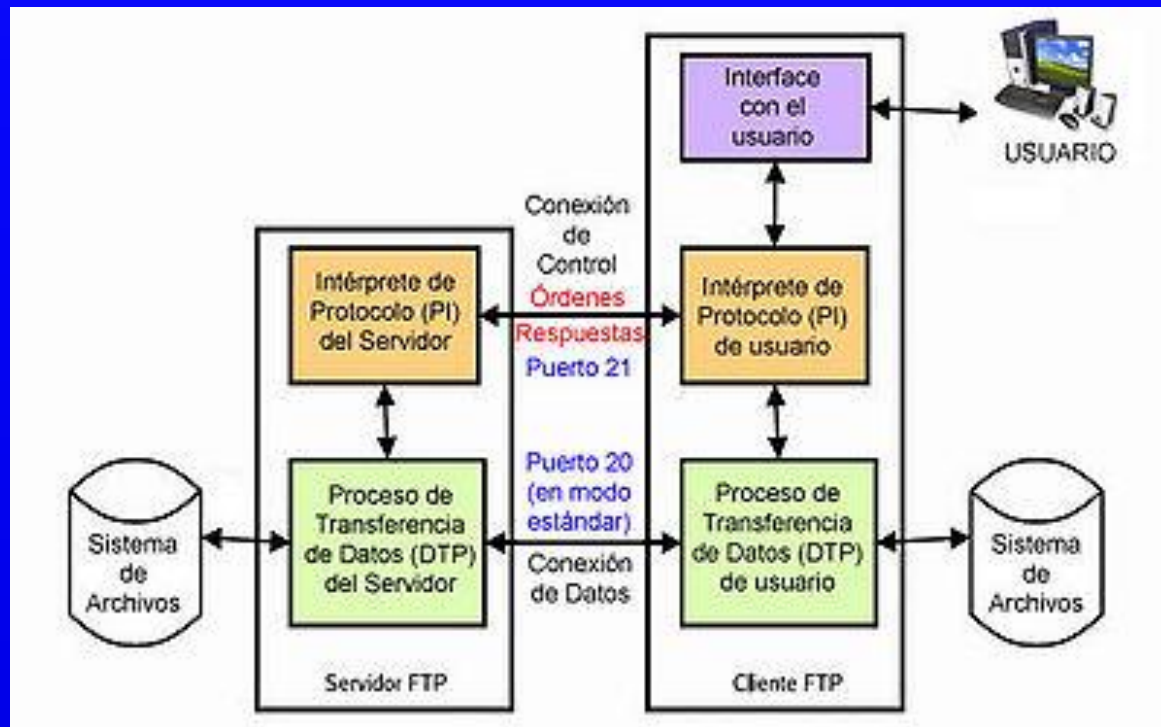
ESQUEMA EN BLOQUES DE LOS PROTOCOLOS



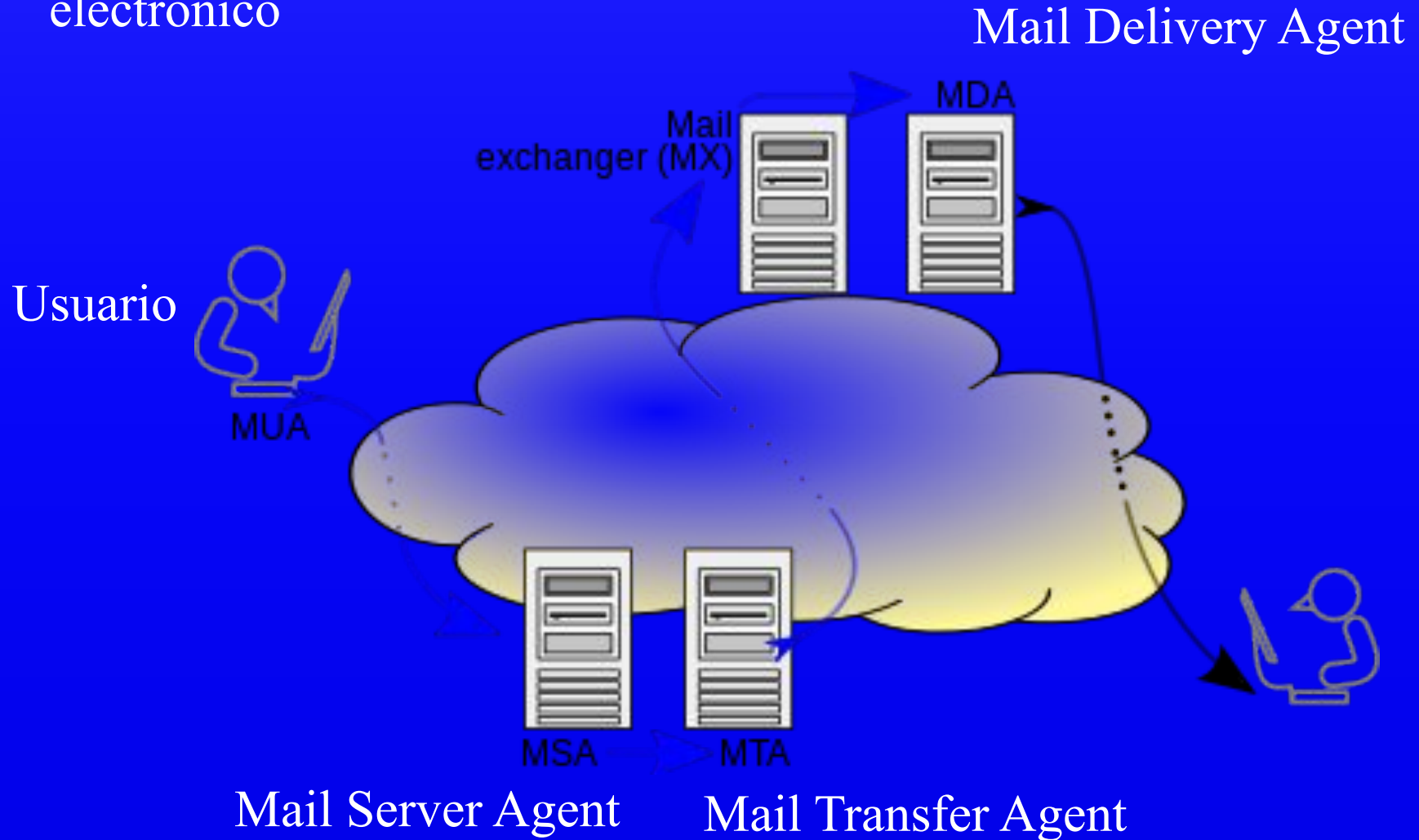
PING herramienta de diagnóstico del estado, velocidad y calidad de una red determinada.

TELNET (*Telecommunication Network*) protocolo de red que nos permite para manejar una PC remotamente

FTP (File Transfer Protocol) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol)

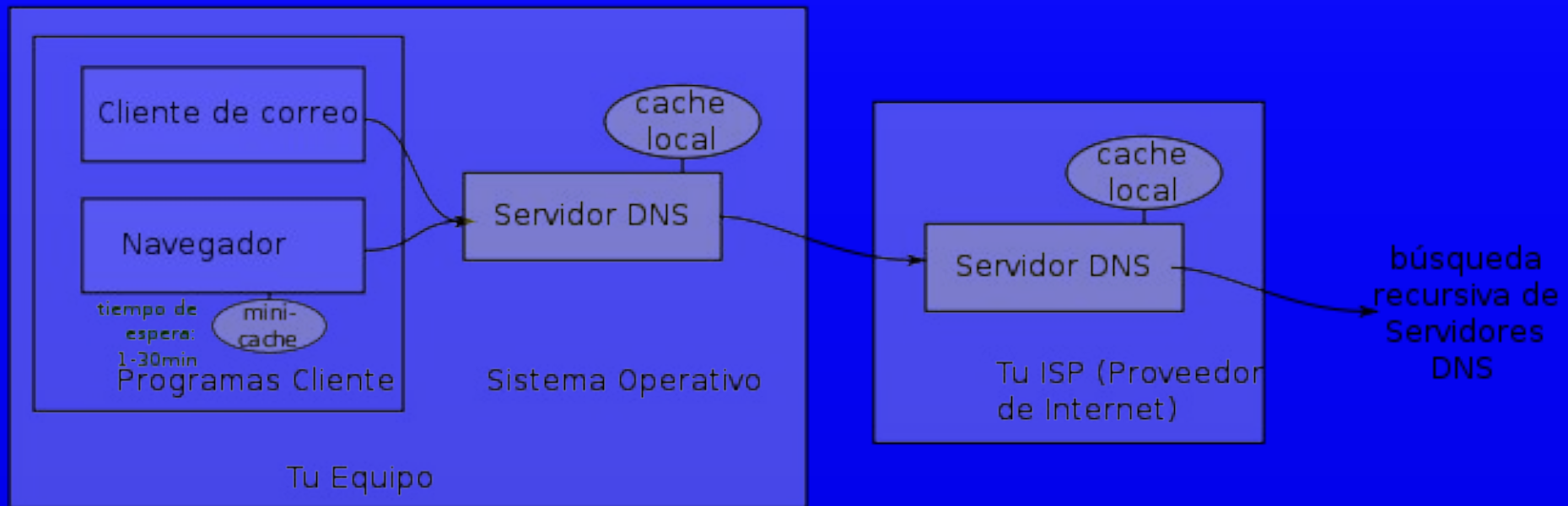


SMTP (*Simple Mail Transfer Protocol*), es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico



RLOGIN (Remote Login) es una aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como host

DNS (Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

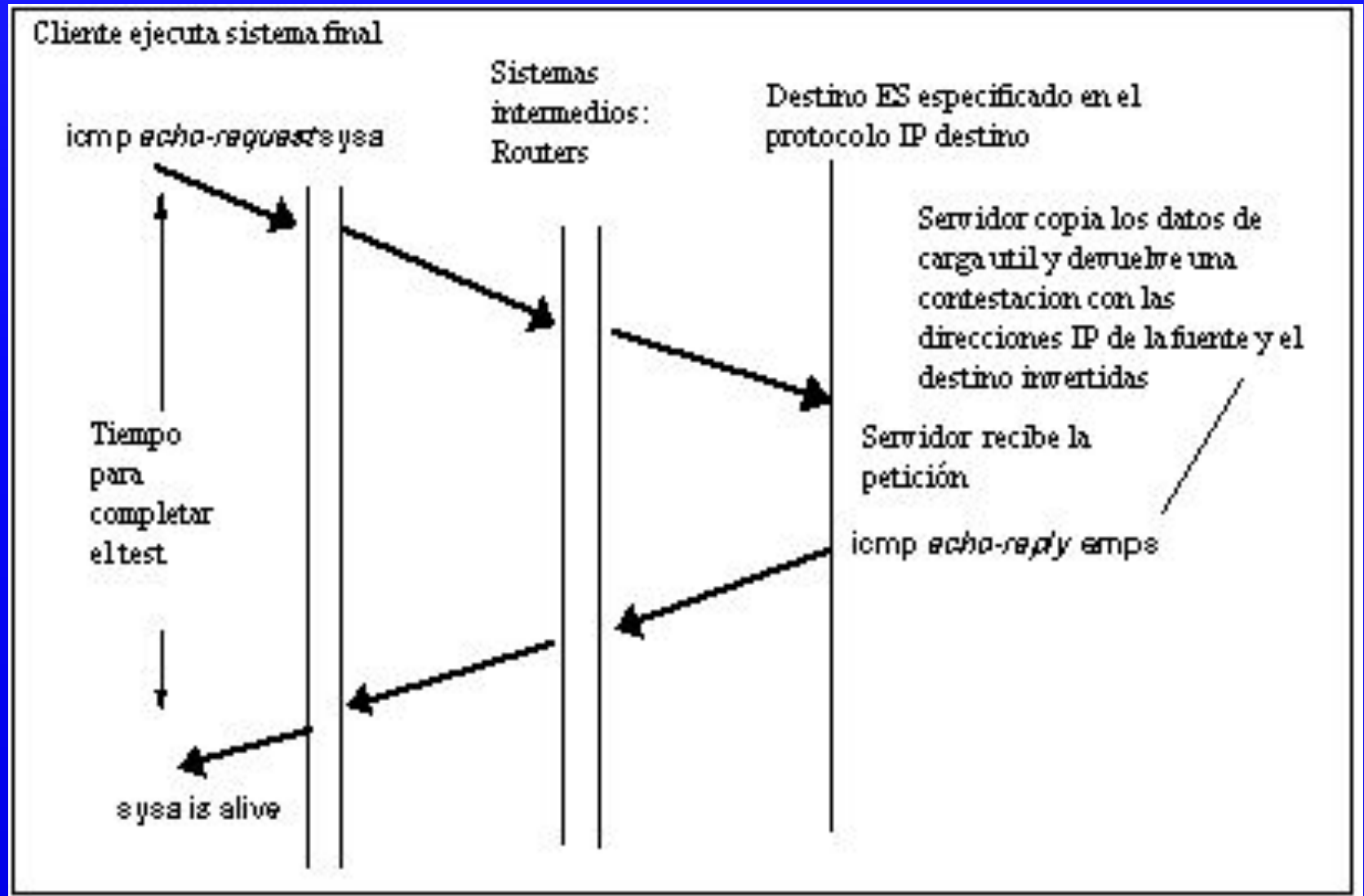


TFTP (Trivial file transfer Protocol) protocolo de transferencia muy simple semejante a una versión básica de FTP

BOOTP (Bootstrap Protocol, es un protocolo de UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de las computadoras o del sistema operativo.

SNMP (Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

ICMP (Internet Control Message Protocol) subprotocolo de control y notificación de errores del Protocolo de Internet (IP).



IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre routers que admiten la multidifusión

ARP, (Address Resolution Protocol) es un protocolo de la capa de red, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP

RARP) es un protocolo utilizado para resolver la dirección IP de una dirección de hardware dada (dirección Ethernet)

PROTOCOLO DE INTERNET (IP)

- **DEFINE: UNIDAD BÁSICA PARA LA TRANSFERENCIA DE DATOS, SELECCIÓN DE RUTAS (RUTEO) Y CONJUNTO DE REGLAS PARA LA ENTREGA DE PAQUETES NO CONFIABLE.**
- **TOMA LOS DATOS DEL NIVEL SUPERIOR (TCP O UDP) Y LOS INSERTA EN LA INTERNET COMO DATAGRAMAS O PAQUETES.**
- **USA ICMP PARA REPORTAR ERRORES.**
- **SE BASA EN SERVICIO NO ORIENTADO A LA CONEXIÓN Y NO CONFIABLE (SIN VALIDACIÓN). NO SE GARANTIZA QUE EL DATAGRAMA LLEGUE A DESTINO.**
- **ES UN SERVICIO DE ENTREGA CON EL MEJOR ESFUERZO (BEST EFFORT).**
- **LOS DATAGRAMAS SON INDEPENDIENTES. NO HAY RELACIÓN ENTRE ELLOS.**
- **DATAGRAMAS VIAJAN POR DISTINTAS REDES (ETHERNET, FDDI, FRAME RELAY, X.25, TOKEN RING, ETC).**

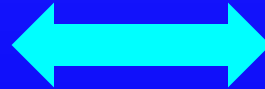
ALGO MÁS SOBRE DATAGRAMAS

PROTOCOLO IP

PROTOCOLO DE LAN

RELACIÓN

DATAGRAMA
DIR IP

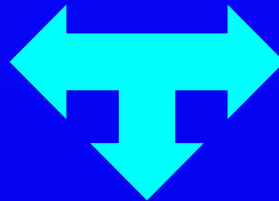


TRAMA
DIR MAC

MANEJADAS POR SW

RECONOCIDAS POR HW

TAMAÑO DE
DATAGRAMA



TAMAÑO DE TRAMA
SEGÚN LAN

ADAPTACIÓN MAS CONVENIENTE PARA LA
COMUNICACIÓN DEL USUARIO

FRAGMENTACIÓN

ENCAPSULAMIENTO

IDEAL

**DATAGRAMA O
PAQUETE**

ENCABEZADO

CAMPO DE DATOS



TRAMA

ENCABEZADO

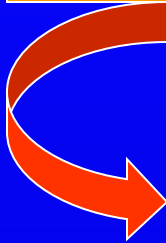
CAMPO DE DATOS

REAL

**DATAGRAMA O
PAQUETE**

ENCABEZADO

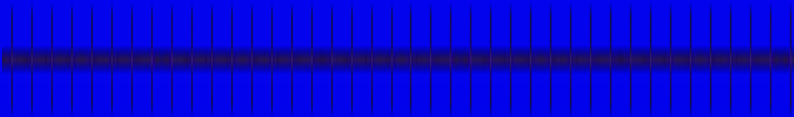
CAMPO DE DATOS



TRAMA

ENCABEZADO

CAMPO DE DATOS



FRAGMENTACIÓN

A CARGO DEL ROUTER

MTU

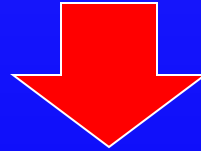
UNIDAD DE TRANSFERENCIA MÁXIMA DE UNA RED

**TAMAÑO MÁXIMO DEL CAMPO DE DATOS DE LA PDU DE LA RED
DONDE SE ENCAPSULA EL DATAGRAMA**

TECNOLOGÍA DE RED	MTU
ETHERNET	1500 B
FDDI	4470 B
TOKEN BUS	8182 B
TOKEN RING	65535 B
X.25	128 B (N3)
FRAME RELAY	4090 B
ATM	48 B
DATAGRAMA IP (+ común)	65515 B

FRAGMENTACIÓN

TAMAÑO DE DATAGRAMA



MTU DE DISTINTAS REDES

PROBL
EMA

FRAGMENTACIÓN

SOLUCI
ÓN

**DIVIDIR EL DATAGRAMA EN PARTES
(DATAGRAMAS MÁS PEQUEÑOS) QUE PUEDAN
ENCAPSULARSE EN MTU MÁS PEQUEÑAS**

FORMATO DATAGRAMA



DESCRIPCIÓN DE LOS CAMPOS

- **VERSION:** SE VERIFICA LA VERSIÓN DEL IP (4, 5 o 6).
- **LONG DE ENCABEZADO:** SE MIDEN PALABRAS DE 32 BITS (MAXIMO 16 PALABRAS = 64 BYTES).
- **TIPO DE SERV:** 6 BITS DE SERVICIOS DIFERENCIADOS Y 2 BITS RESERVADOS PARA NOTIFICACIÓN EXPLÍCITA DE CONGESTIÓN.
- **LONG TOTAL:** SE MIDEN OCTETOS. INCLUYE ENCABEZADO Y DATOS (MAXIMO 65535 BYTES).
- **IDENTIFICACIÓN:** IDENTIFICA AL DATAGRAMA (FRAGMENTACIÓN).
- **DESPLAZAMIENTO DE FRAGMENTO:** ESPECIFICA EL DESPLAZAMIENTO EN EL DATAGRAMA ORIGINAL DE LOS DATOS ACARREADOS EN EL FRAGMENTO (UNIDADES DE 8 BYTES).
- **BANDERA:** CONTROLAN LA FRAGMENTACIÓN DANDO INFORMACIÓN (NO FRAGMENTAR, MÁS FRAGMENTOS).

Fragmentación de IP y reensamblado

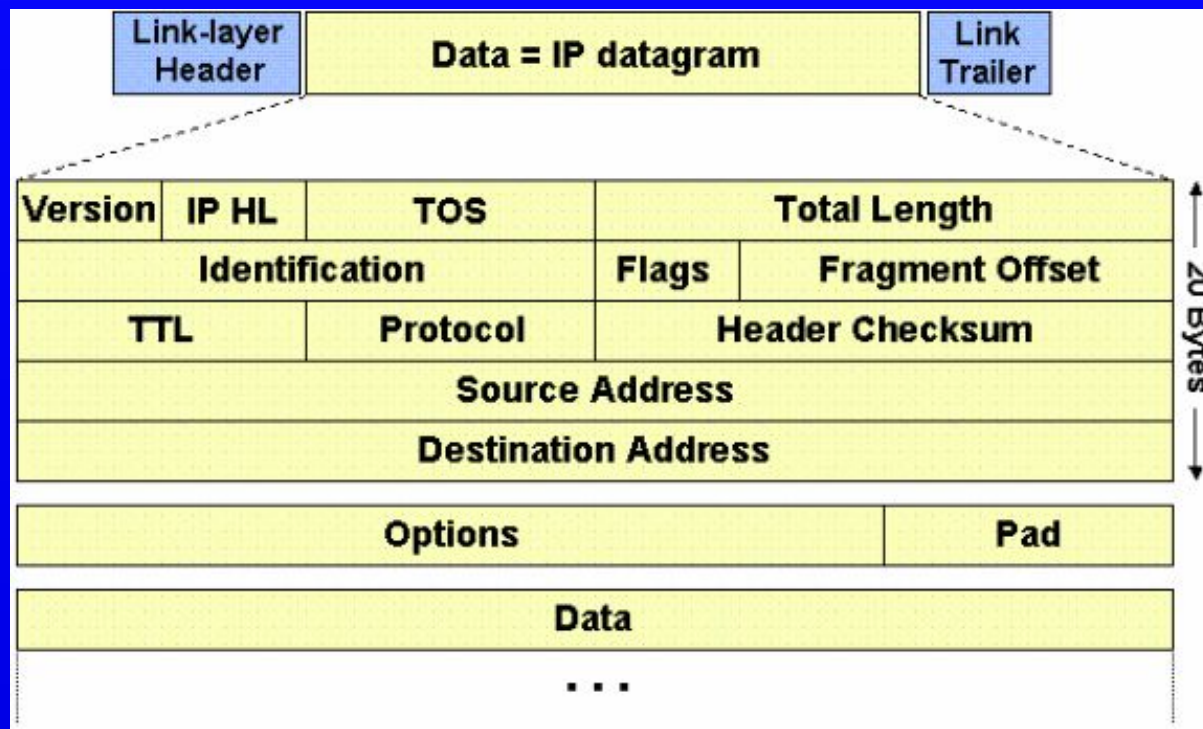
El protocolo IP se utiliza en una variedad de enlaces de transmisión. unidireccionales.

La longitud máxima de un datagrama IP es de 64K, pero la mayoría de enlaces de transmisión imponen un límite más pequeño en la longitud máxima del paquete, unidad de transmisión máxima (MTU).

El valor de la MTU depende del tipo de enlace de transmisión. El diseño de IP tiene en cuenta las diferencias de MTU al permitir que los routers fragmenten los datagramas IP como sea necesario. La estación receptora se encarga de reensamblar los fragmentos en el datagrama IP al tamaño completo original.

La fragmentación de IP implica la división de un datagrama en diferentes partes que pueden reensamblarse más adelante.

Los campos source IP (IP de origen), destination (destino) identificación (identificación), total length (longitud total) y fragment offset (desplazamiento de fragmentos) y los indicadores "more fragments" (más fragmentos) y "don't fragment" (no fragmentar) en el encabezado IP, se usan para fragmentar y reensamblar el IP. (RFC 791)



La identificación es de 16 bits y es un valor asignado por el emisor de un datagrama IP para ayudar en el reensamblado de los fragmentos de un datagrama.

El desplazamiento de fragmentos es de 13 bits e indica la ubicación del fragmento en el datagrama IP original. Este valor es un múltiplo de ocho bytes.

En el campo de indicadores del encabezado IP, hay tres bits para indicadores de control. Es importante el bit "don't fragment" (no fragmentar) (DF) tiene un papel central en la PMTUD (Path MTU Discovery), ya que determina si se permite la fragmentación de un paquete.

El bit 0 está reservado y siempre se define en 0. El bit 1 es el bit DF (0 = "may fragment" (puede fragmentar) 1 = "don't fragment" (no fragmentar)). El bit 2 es el bit MF (0 = "last "fragment" (último fragmento) 1 = "don't fragment" (no fragmentar)).

Original IP Datagram

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

IP Fragments (Ethernet)

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

Ejemplo de fragmentación.

La suma todas las longitudes de los fragmentos IP, el valor excede la longitud original del datagrama IP en 60.

La causa es porque se han creado tres encabezados IP adicionales, uno para cada fragmento después del primer fragmento.

El primer fragmento tiene un desplazamiento de 0, la longitud de este fragmento es 1500; esto incluye 20 bytes para el encabezado IP original que se ha modificado.

El segundo fragmento tiene un desplazamiento de 185 ($185 \times 8 = 1480$), lo que significa que la porción de datos de este fragmento empieza en los 1480 bytes en el datagrama IP original.

La longitud de este fragmento es 1500; esto incluye el encabezado IP adicional creado para este fragmento.

El tercer fragmento tiene un desplazamiento de 370 ($370 \times 8 = 2960$), lo que significa que la porción de datos de este fragmento empieza en los 2960 bytes en el datagrama IP original.

La longitud de este fragmento es 1500; esto incluye el encabezado IP adicional creado para este fragmento.

El cuarto fragmento tiene un desplazamiento de 555 ($555 \times 8 = 4440$), lo que significa que la porción de datos de este fragmento empieza en los 4440 bytes en el datagrama IP original. La longitud de este fragmento es 700 bytes; esto incluye el encabezado IP adicional creado para este fragmento.

El tamaño original del datagrama IP sólo se puede determinar cuando se recibe el último fragmento.

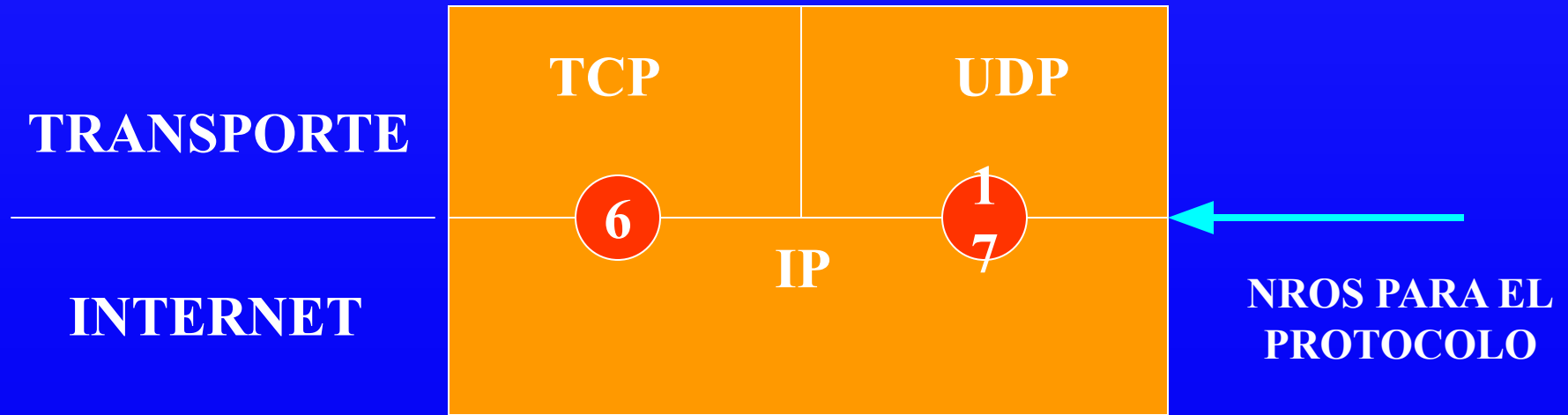
El desplazamiento en el último fragmento (555) proporciona un desplazamiento de datos de 4440 bytes en el datagrama IP original.

Si luego agrega bytes de datos desde el último fragmento ($680 = 700 - 20$), el resultado será 5120 bytes, que es la porción de datos del datagrama IP original.

A continuación, la adición de 20 bytes para un encabezado IP resultará en el tamaño del datagrama original IP ($4440 + 680 + 20 = 5140$).

DESCRIPCIÓN DE LOS CAMPOS

- **TIEMPO DE VIDA:** TIEMPO EN SEGUNDOS QUE EL DATAGRAMA TIENE PERMITIDO PERMANECER EN LA INTERNET. LUEGO SE ELIMINA.
- **PROTOCOLO:** IDENTIFICA AL PROTOCOLO DE LA CAPA SUPERIOR



- **SUMA DE VERIFICACIÓN DEL ENCABEZADO:** DETECTA ERRORES
- **OPCIONES:** NO SIEMPRE SE EMPLEA. USO PARA PRUEBAS DE RED O DEPURACIÓN. LONGITUD VARIABLE.
- **RELLENO:** ASEGURA QUE LA CABECERA TENGA UNA LONGITUD MÚLTIPLO DE 32 BITS.

http://www.cisco.com/cisco/web/support/LA/7/76/76108_pmtud_ipfrag.html

DIRECCIONES IP

- PARA **INTERNET** SON ADMINISTRADAS POR EL NETWORK INFORMATION CENTER (NIC)
- EMPLEA 32 BITS (4 BYTES). LA DIRECCIÓN IP SE REPRESENTA **EN BINARIO** O CON 4 NÚMEROS **EN DECIMAL**, SEPARADOS POR PUNTOS (MÁS COMÚN).
- SE COMPONEN DE:
 - IDENTIFICADOR DE CLASE**
 - NÚMERO DE RED**
 - NÚMERO DE HOST**
- DIR DE CADA RED DEBE SER ÚNICA
- DIR DE CADA HOST DEBE SER ÚNICA DENTRO DE CADA RED
- SI TODOS LOS BITS DEL CAMPO DE HOST SON “1” = **DIFUSIÓN DIRIGIDA A UNA RED** (SE DEBE COLOCAR LA DIRECCIÓN DE LA RED)
- SI TODOS LOS BITS SON “1” (32) = **DIFUSIÓN LIMITADA EN RED LOCAL**
- SI TODOS LOS BITS DEL CAMPO DE RED O DE HOST SON “0” = **LOOPBACK** (SE REFIERE A ESTA RED O A ESTE HOST). **USO EN EL ARRANQUE.**
- LAS DIR QUE COMIENZAN CON 127, CON 255 O QUE ESTÁN ENTRE 224 Y 247 SON RESERVADAS (TIPO D Y E).

REGLA PRACTICA PARA MANEJO DE DIRECCIONES IP

VALORES DECIMALES DEL BYTE

<div><div>PESO</div><div>EJEMPLOS</div></div>	Bit 8 +	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1 -
CALCULO DEL PESO	128 2^7	64 2^6	32 2^5	16 2^4	8 2^3	4 2^2	2 2^1	1 2^0
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0

TIPOS DE DIRECCIONES IP

1	2	3	4	5	8	16	24	32																							
0	NRO RED				NRO HOST																										
1	0	NRO RED										NRO HOST																			
1	1	0	NRO RED																NRO HOST												
1	1	1	0	DIRECCIÓN MULTIDIFUSIÓN																											
1	1	1	1	0	RESERVADO PARA USO POSTERIOR																										

REGLA DEL PRIMER OCTETO (EN DECIMAL)

1 A 126 CLASE A

192 A 223 CLASE C

240 A 247 CLASE E

128 A 191 CLASE B

224 A 239 CLASE D

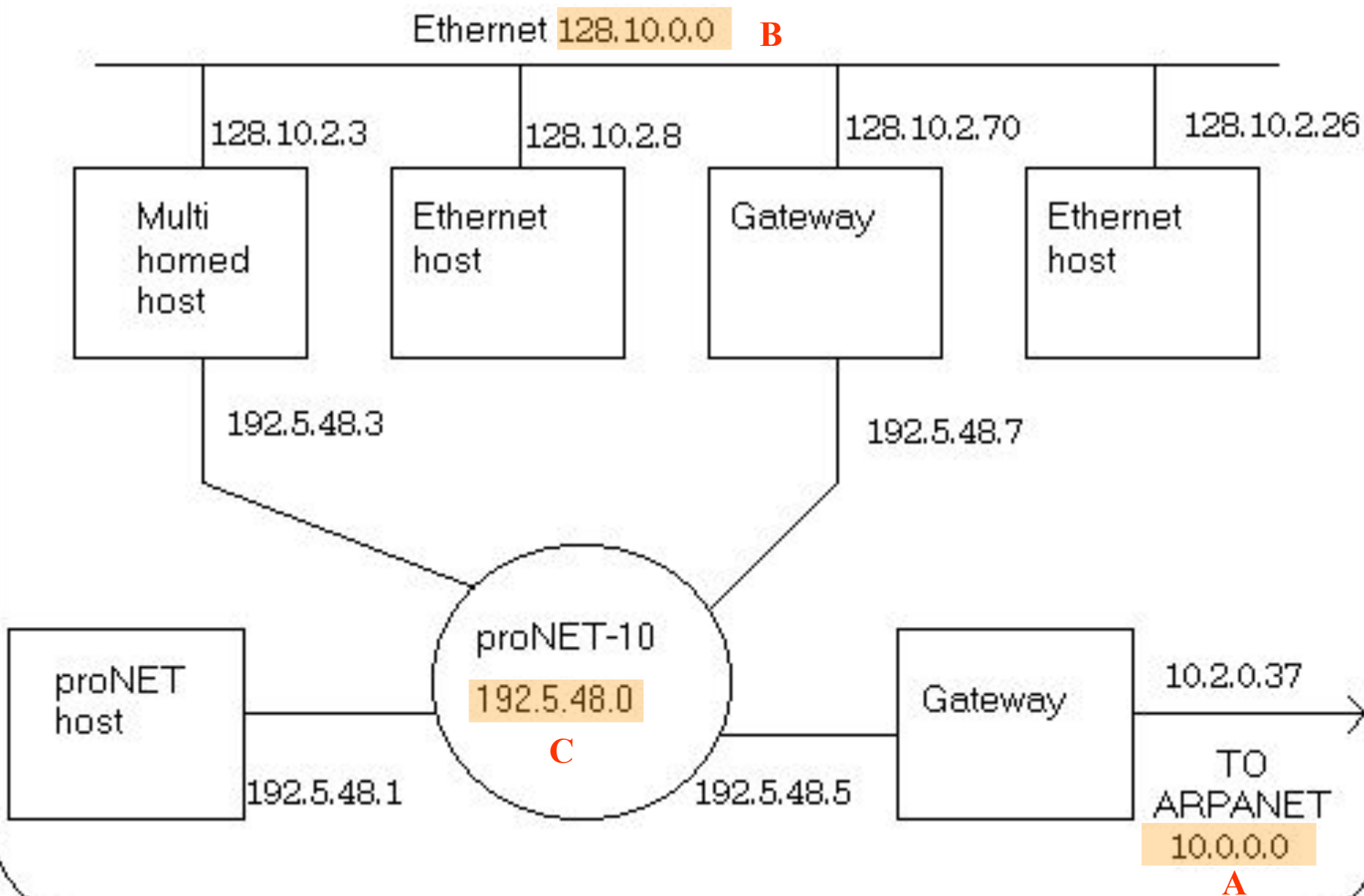
CUADRO COMPARATIVO

TIPO DE RED	CANT REDES	CANT HOSTS	DIR MENOR DE RED	DIR MAYOR DE RED
A	126 ($2^7 - 2$)	16.777.214 ($2^{24} - 2$)	1.0.0.0	126.0.0.0
B	16.382 ($2^{14} - 2$)	65.534 ($2^{16} - 2$)	128.1.0.0	191.254.0.0
C	2.097.150 ($2^{21} - 2$)	254 ($2^8 - 2$)	192.0.1.0	223.255.254.0
D	-----	-----	224.0.0.0	239.255.255.255
E	-----	-----	240.0.0.0	247.255.255.255

ALGO MÁS SOBRE DIRECCIONES IP

- **UNA DIRECCIÓN IDENTIFICA MÁS PRECISAMENTE A UNA CONEXIÓN DE RED**
- **SI UN HOST SE MUEVE DE UNA RED A OTRA, SU DIRECCIÓN IP DEBE CAMBIAR**
- **EMPLEO PARA RUTEAR DATAGRAMAS**
- **UN ROUTER MANEJA UNA TABLA DE DIRECCIONES PARA ENRUTAMIENTO. CADA PUERTO LAN Y WAN DEL ROUTER TIENE SU DIRECCIÓN IP**
- **UN HOST MULTI-HOMED ES AQUEL QUE TIENE MAS DE UNA CONEXIÓN FÍSICA (ESTO IMPLICA UNA DIR IP POR CADA UNA)**

IP ADDRESSES ASSIGNMENT EXAMPLE



SUBREDES

PARA EL MEJOR APROVECHAMIENTO DE LAS GRANDES REDES, SE PUEDEN DIVIDIR A LAS MISMAS EN REDES MÁS PEQUEÑAS (SUBREDES).



MÁSCARA

AL IGUAL QUE LA DIR IP TIENE 32 BITS



LOS “1” DE LA MÁSCARA SON DE RED Y SUBRED

LOS “0” DE LA MÁSCARA SON DE HOST






EJEMPLOS

SIN SUBRED

	RED		HOST	
				
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
NO HAY SUBRED	172	16	0	0
NRO DE RED				

CON SUBRED

	RED		SUBRED	HOST
				
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000
NRO DE SUBRED	172	16	2	0

IP Subnetting Example

Subnet mask = 255.255.255.0

Network 128.10.1.0

128.10.1.1

128.10.1.2

G

H1

H2

REST OF THE
INTERNET

Network 128.10.2.0

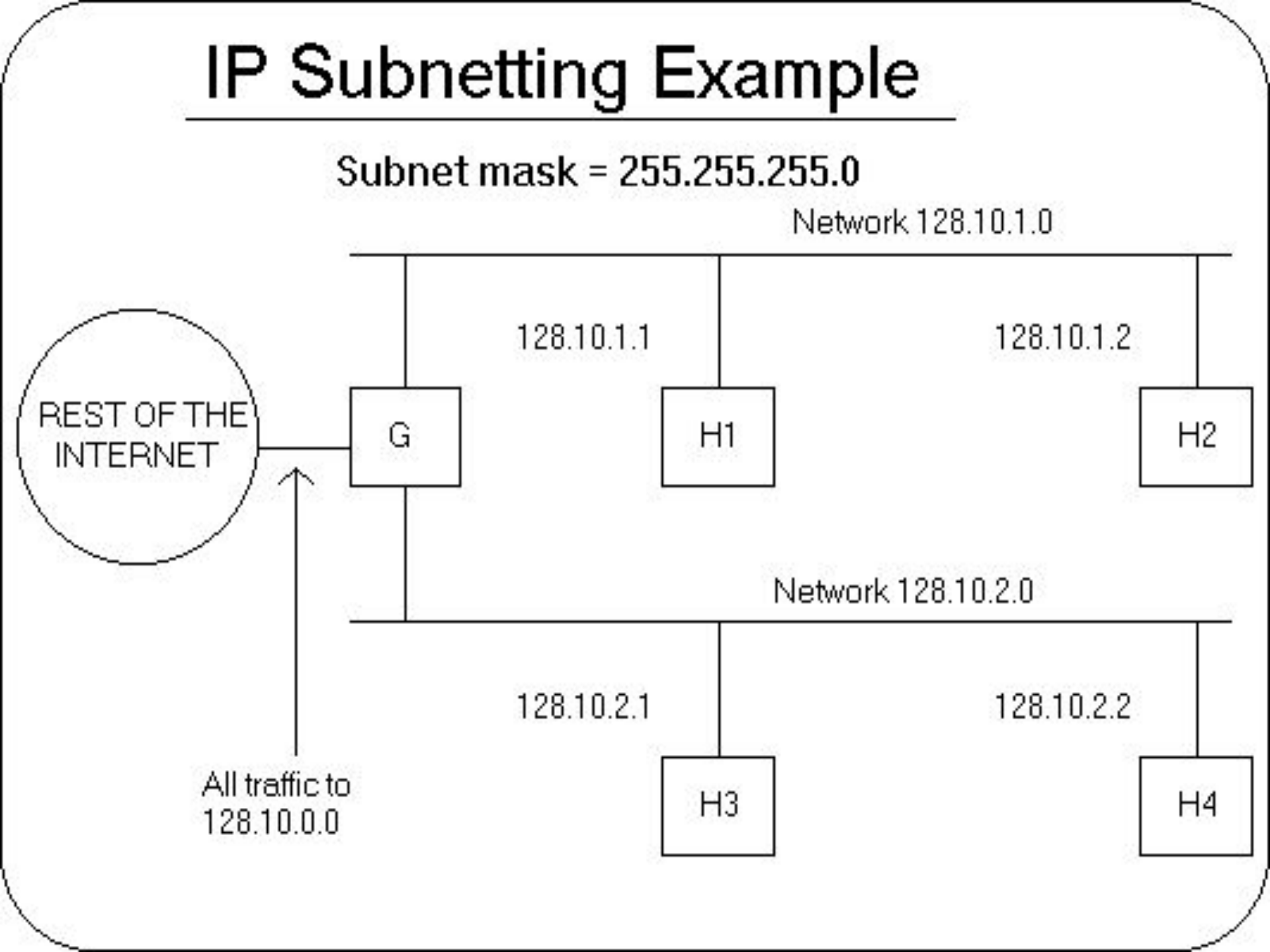
128.10.2.1

128.10.2.2

H3

H4

All traffic to
128.10.0.0



PASOS

DETERMINAR

CANT SUBREDES

CANT HOSTS POR
SUBRED

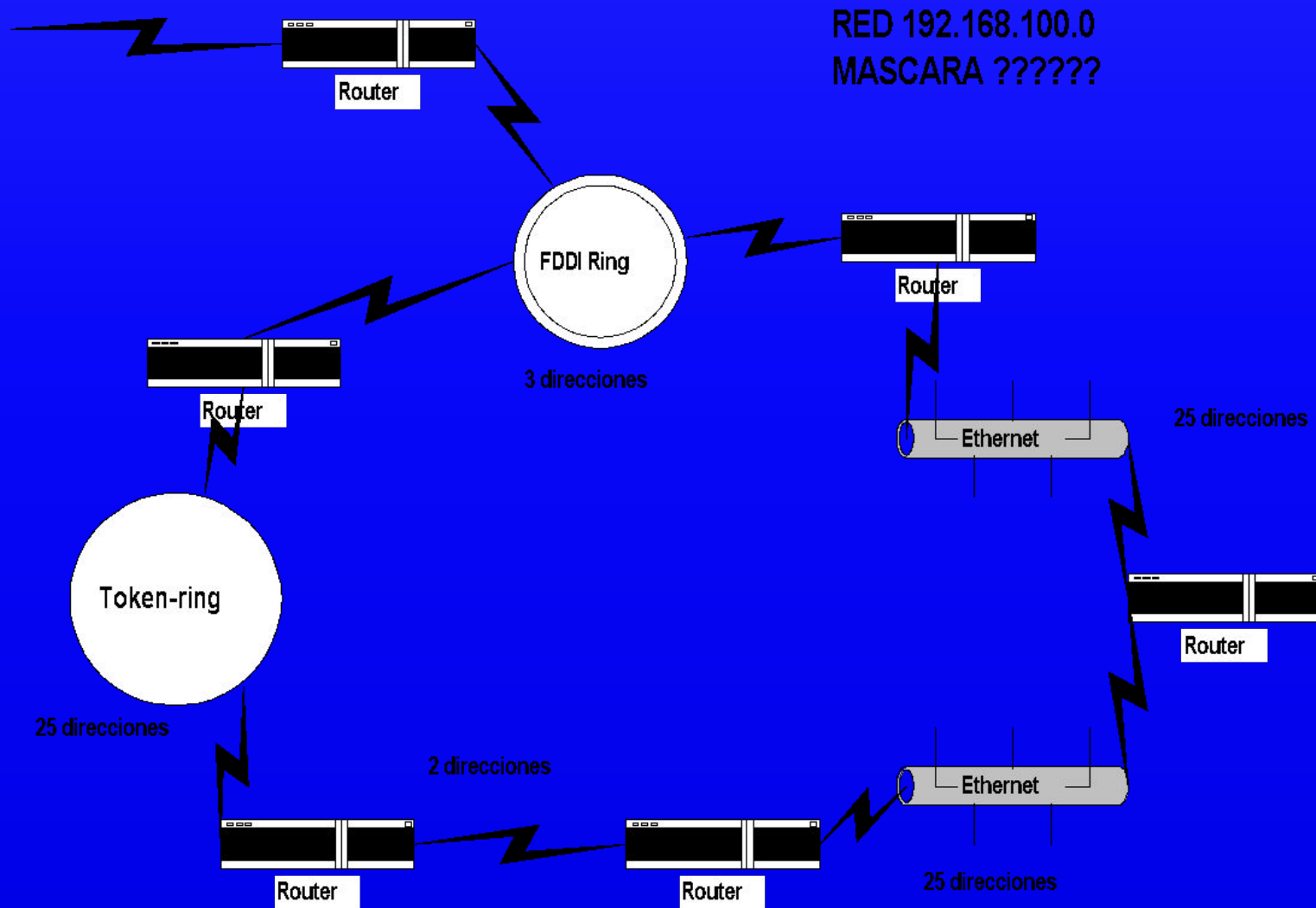
DEFINIR

MÁSCARA DE
SUBRED

DIR RED ÚNICA
PARA CADA SUBRED

RANGO DE DIR DE
HOST VÁLIDAS

EJERCICIO



VLSM (MÁSCARA VARIABLE)

- **PERMITE UN USO MÁS EFICIENTE ASIGNANDO DISTINTAS MÁSCARAS A LAS INTERFASES DE UN ROUTER.**

CIDR (DIRECCIONAMIENTO SIN CLASE)

- **SE ASIGNAN BLOQUES DE DIRECCIONES SIN PERTENECER A NINGUNA CLASE.**
- **USO DE MÁSCARA EN NOTACIÓN CIDR (x.x.x.x/n).**
- **SE DETERMINAN LA PRIMERA DIRECCIÓN, LA LONGITUD Y EL BROADCAST DEL BLOQUE.**

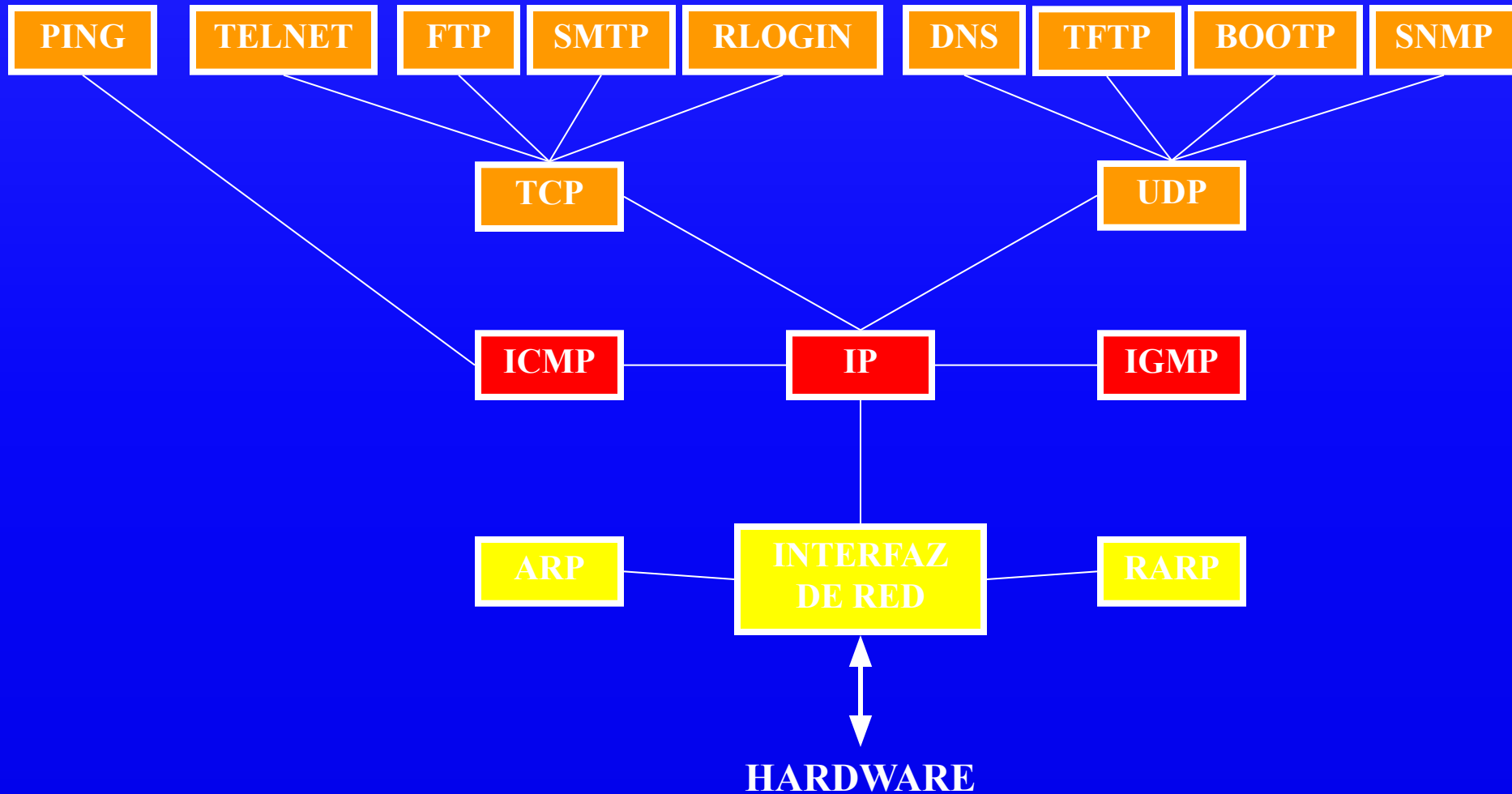
RESUMEN DE TÉCNICA DE SUBRED

- **PERMITE QUE UNA MISMA DIRECCIÓN DE RED IDENTIFIQUE A VARIAS REDES FÍSICAS.**
- **EXIGE ALGORITMOS MODIFICADOS DE RUTEO QUE CONTENGAN TABLAS CON MÁSCARA DE SUBRED.**
- **CAMBIA LA INTERPRETACIÓN DE LA DIRECCIÓN IP (RED, SUBRED Y HOST). MAYOR FLEXIBILIDAD YA QUE PUEDE SER INDEPENDIENTE EN CADA RED FÍSICA.**
- **CONCEPTO DE DIRECCIONAMIENTO JERÁRQUICO = RUTEO JERÁRQUICO. FACILITA EL PROCESO DE RUTEO.**

CONCEPTO DE SUPERRED

- **USO DE VARIAS DIRECCIONES DE RED PARA UNA MISMA ORGANIZACIÓN (VARIAS CLASE C).**
- **RUTEO: DIR IP Y NRO CONTEO (DIR CONTIGUAS).**

ESQUEMA EN BLOQUES DE LOS PROTOCOLOS



PROTOCOLOS PARA RESOLUCIÓN DE DIRECCIONES



ARP

PROTOCOLO DE RESOLUCIÓN
DE DIRECCIÓN

PERMITE CONOCER LA
DIRECCIÓN MAC A TRAVÉS DE
SU DIRECCIÓN IP.

TRANSMITE **BROADCAST MAC**
CON LA **DIR IP** DESTINO PARA
QUE EL DESTINO RESPONDA
CON SU **DIR MAC** Y SE
REGISTRE EN LA TABLA ARP
DEL HOST.

RARP

PROTOCOLO DE RESOLUCIÓN
DE DIRECCION INVERSA

PERMITE QUE UNA MÁQUINA
CONOZCA SU DIRECCIÓN IP
MEDIANTE SU DIR MAC.

TRANSMITE **BROADCAST MAC**
DE SOLICITUD PARA QUE EL
SERVIDOR RARP DE LA **DIR IP**
CORRESPONDIENTE A LA **DIR**
MAC DE LA MÁQUINA
SOLICITANTE.

PROTOSCOLOS PARA RESOLUCIÓN DE DIRECCIONES

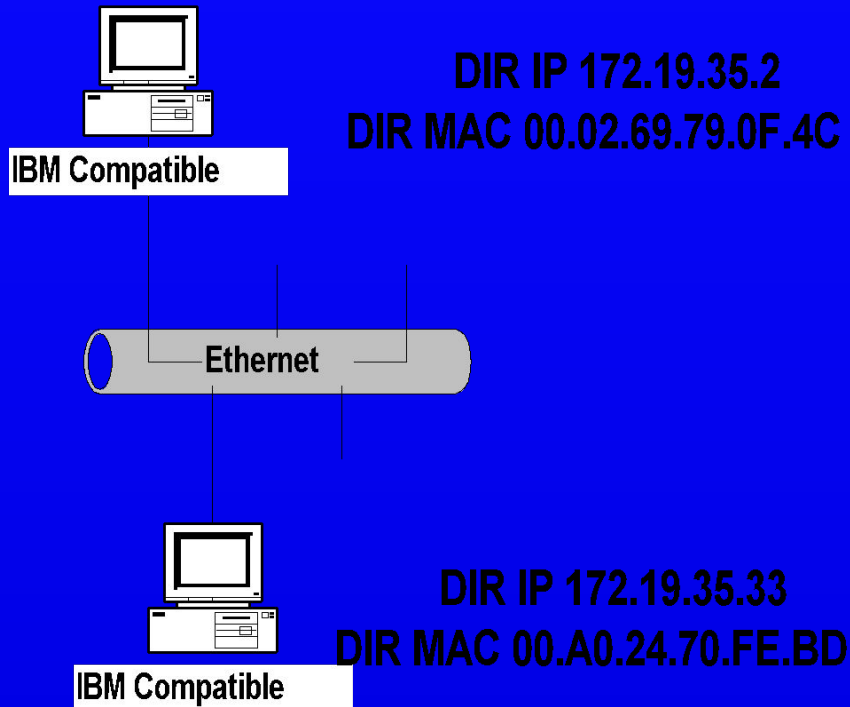
MENSAJE ARP / RARP



TRAMA

ENCABEZADO

CAMPO DE DATOS



MSJ ARP

SOLICITUD DE "1" A TODOS

MAC 1

IP 1

MAC DIF.

IP 2

RESPUESTA DE "2" A "1"

IP 1

MAC 1

IP 2

MAC 2

Tracer: Uso de los comandos show

11.3.4 Host y comandos de IOS

11.3.4.1 Opciones del comando ipconfig

11.3.4.2 Opciones del comando arp

11.3.4.3 Opciones del comando show cdp neighbors

11.3.4.4 Uso del comando show ip interface brief

11.3.4.5 Actividad: Comandos show

11.3.4.6 Práctica de laboratorio: Uso de la CLI para recopilar información sobre dispositivos de red.pdf

11.4 Administración de los archivos de configuración de IOS

11.4.1 Sistemas de archivos del router y del switch

11.4.1.1 Sistemas

Rendimiento básico de la red

Host y comandos de IOS

comando **arp** se ejecuta desde el símbolo del sistema de Windows.

Para ejecutar un comando **arp**, introduzca lo siguiente en el símbolo del sistema de un host:

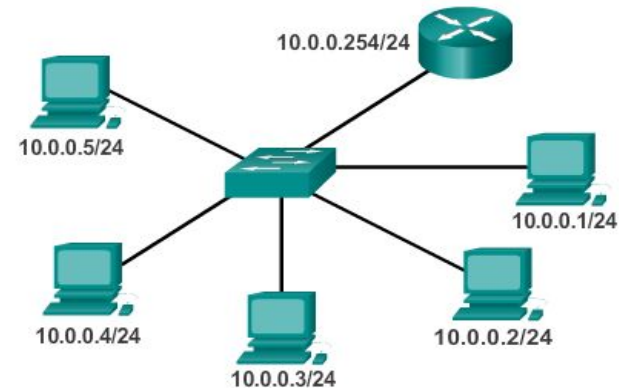
```
C:\host1> arp -a
```

Como se muestra en la ilustración, el comando **arp -a** enumera todos los dispositivos que se encuentran actualmente en la caché ARP del host, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo.

Se puede borrar la caché mediante el comando **arp -d** en caso de que el administrador de red desee volver a llenarla con información actualizada.

Nota: la caché ARP solo contiene información de los dispositivos a los que se accedió recientemente. Para asegurar que la caché ARP esté cargada, haga ping a un dispositivo de manera tal que tenga una entrada en la tabla ARP.

Nociones sobre los nodos de la red



```
c:\>arp -a
```

Internet Address	Physical Address	Type
10.0.0.2	00-08-a3-b6-ce-04	dynamic
10.0.0.3	00-0d-56-09-fb-d1	dynamic
10.0.0.4	00-12-3f-d4-6d-1b	dynamic
10.0.0.254	00-10-7b-e7-fa-ef	dynamic

Par de direcciones IP y MAC

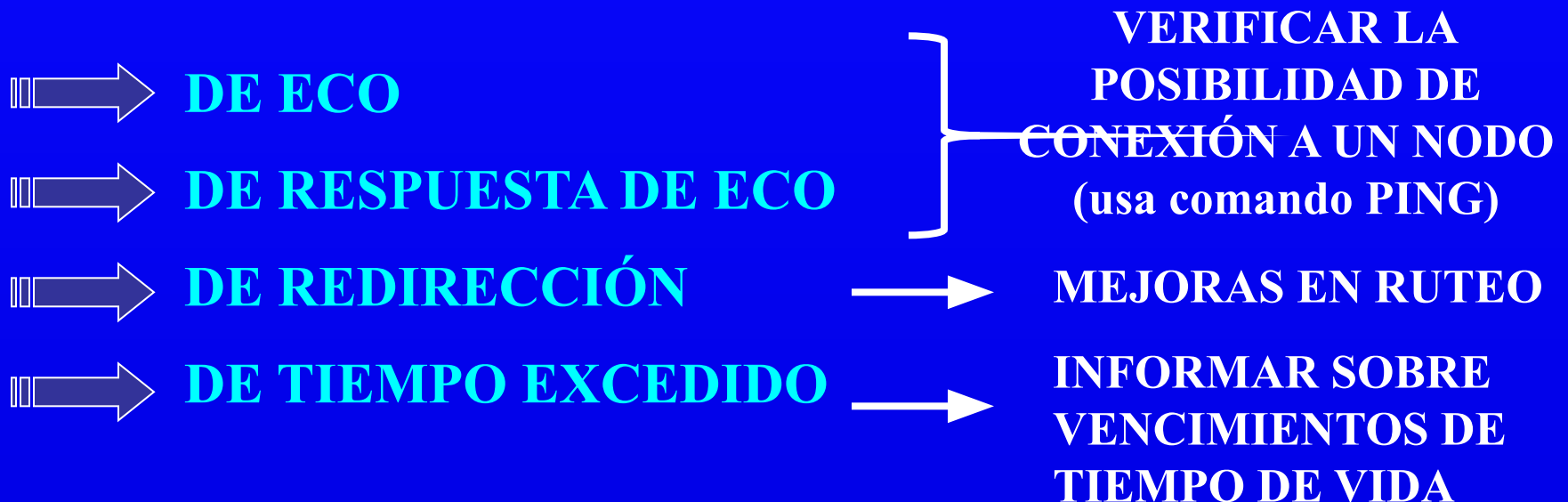
- C:\Documents and Settings\usuario>arp -a
- Interfaz: 192.168.1.103 --- 0x2
- Dirección IP Dirección física Tipo
- 192.168.1.1 00-23-69-ea-9c-a2 dinámico

**MOSTRAR LA
TABLA ARP QUE SE
ENCUENTRA EN
MEMORIA**

ICMP

PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET

- PARTE DE LA CAPA IP
- SE EMPAQUETA DENTRO DE UN DATAGRAMA PERO NO ES NIVEL DE TRANSPORTE
- VERIFICA E INFORMA SOBRE EVENTOS EN RED IP
- MENSAJES



C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Versión 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\usuario>ipconfig /all

Configuración IP de Windows

Nombre del host : FAMILIA
Sufijo DNS principal :
Tipo de nodo : desconocido
Enrutamiento habilitado : No
Proxy de WINS habilitado : Sí
Lista de búsqueda de sufijo DNS : fibertel.com.ar

Adaptador Ethernet Conexión de área local :

Sufijo de conexión específica DNS : fibertel.com.ar
Descripción : Realtek PCIe GBE Family Controller
Dirección física : 00-1C-C0-72-C1-3F
DHCP habilitado : No
Autoconfiguración habilitada : Sí
Dirección IP : 192.168.1.103
Máscara de subred : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP : 192.168.1.1
Servidores DNS : 192.168.1.1
200.49.130.41
200.42.4.203

Concesión obtenida : Martes, 25 de Noviembre de 2014 09:00:46 a.m.

Concesión expira : Miércoles, 26 de Noviembre de 2014 09:00:46 a.m.

C:\Documents and Settings\usuario>ping 192.168.1.103

Haciendo ping a 192.168.1.103 con 32 bytes de datos:

Respuesta desde 192.168.1.103: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.103: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.103: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.103: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.103:

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

Tiempos aproximados de ida y vuelta en milisegundos:

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

C:\Documents and Settings\usuario>ping 200.42.4.203

Haciendo ping a 200.42.4.203 con 32 bytes de datos:

Respuesta desde 200.42.4.203: bytes=32 tiempo=8ms TTL=55
Respuesta desde 200.42.4.203: bytes=32 tiempo=9ms TTL=55
Respuesta desde 200.42.4.203: bytes=32 tiempo=11ms TTL=55
Respuesta desde 200.42.4.203: bytes=32 tiempo=9ms TTL=55

Estadísticas de ping para 200.42.4.203:

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

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 8ms, Máximo = 11ms, Media = 9ms

C:\Documents and Settings\usuario>

Escriba una pregunta

Estilo Nueva diapositiva...

12:11

IGMP

PROTOCOLO DE ADMINISTRACIÓN DE GRUPO EN INTERNET

- **ES UN PROTOCOLO DE MULTIDIFUSIÓN QUE UTILIZA DATAGRAMAS PARA LLEVAR A CABO LA COMUNICACIÓN. INTERCAMBIA INFORMACIÓN ENTRE ROUTERS.**
- **PARTE DE LA CAPA IP.**
- **TRANSMITE DATAGRAMAS IP A UN CONJUNTO DE MÁQUINAS (GRUPO DE MULTIDIFUSIÓN).**
- **GRUPO CON PROCESO DINÁMICO.**
- **DIRECCIÓN MULTIDIFUSIÓN ÚNICA (CLASE D). SE USAN SOLO COMO DIRECCIONES DE DESTINO.**
- **SE PROPAGA EN UNA SOLA RED FÍSICA O A TRAVÉS DE VARIAS REDES.**

UDP

PROTOCOLO DE DATAGRAMA DE USUARIO

- USA IP COMO NIVEL 3. RESIDE EN LA CAPA DE TRANSPORTE.
- ESTRECHA RELACIÓN ENTRE UDP ↔ IP.
- LA PDU SE DENOMINA **DATAGRAMA UDP**.
- TRANSMISIONES NO CONFIABLES, SIN VALIDACIONES. NO IMPLEMENTA CONTROL DE FLUJO. PUEDEN EXISTIR PÉRDIDAS, DUPLICACIONES, RETRASOS Y ENTREGA SIN ORDEN.
- LAS APLICACIONES DEBEN RESOLVER ESTOS PROBLEMAS.
- **MÁS VELOZ QUE EL TCP.**
- REALIZA MULTIPLEXADO Y DEMULTIPLEXADO DE PUERTOS. CONCEPTO DE MULTIPROCESOS.
- **ORIENTADO A LA NO CONEXIÓN.**

FORMATO DEL DATAGRAMA UDP

0	15	16	31
PUERTO ORIGEN		PUERTO DESTINO	
LONGITUD DEL MENSAJE UDP		SUMA DE VERIFICACIÓN	
DATOS			

- **PUERTO ORIGEN:** ES OPCIONAL. PUEDE VALER 0 SI NO SE UTILIZA.
- **LONGITUD:** CUENTA LA CANTIDAD DE OCTETOS (ENCABEZADO Y DATOS). VALOR MÍNIMO ES 8 Y EL MÁXIMO 65515.
- **SUMA DE VERIFICACIÓN:** ES OPCIONAL. SI VALE 0 NO SE ESTÁ USANDO. NORMALMENTE SE USA. INCLUYE LA DIR IP ORIGEN, DIR IP DESTINO (SACADAS DEL DATAGRAMA IP), EL ENCABEZADO Y LOS DATOS DEL DATAGRAMA UDP.

TCP

PROTOCOLO DE CONTROL DE TRANSMISIÓN

- TRANSFERENCIA CONFIABLE Y DE **EXTREMO A EXTREMO**.
- USA IP COMO NIVEL 3. RESIDE EN LA CAPA DE TRANSPORTE.
- LA PDU SE DENOMINA **SEGMENTO TCP**.
- REALIZA MULTIPLEXADO Y DEMULTIPLEXADO DE PUERTOS.
- MANEJA CONEXIONES FULL DUPLEX.
- USA SUMA DE VERIFICACIÓN Y NRO DE SECUENCIA (SEGURIDAD Y ORDENAMIENTO). LA SUMA INCLUYE LAS DIRECCIONES IP DEL DATAGRAMA, EL ENCABEZAMIENTO Y LOS DATOS DEL SEGMENTO.
- **ORIENTADO A LA CONEXIÓN**.
- CONTROL DE FLUJO MEDIANTE MÉTODO DE VENTANA DESLIZANTE. PARÁMETRO DE TAMAÑO DE VENTANA **VARIABLE**.
- MANEJO DE TIME OUT PARA RETRANSMISIÓN. RETRASOS VARIABLES.

FORMATO DEL SEGMENTO TCP

0	4	10	16	24	31
PUERTO ORIGEN			PUERTO DESTINO		
NRO DE SECUENCIA					
NRO DE ACUSE DE RECIBO					
LONG ENCAB &	RES	COD BITS +	VENTANA		
SUMA DE VERIFICACIÓN #			PUNTERO DE URGENCIA		
OPCIONES *				RELLENO	
DATOS					
.....					

(*) VARIABLE (#) INCLUYE CONTROL DIR IP ORIGEN Y DESTINO

(+) DETERMINA PROPÓSITO Y CONTENIDO DEL SEGMENTO (&) MÚLTIPLO DE 32

PUERTOS UDP Y TCP

- **UTILIZAN NÚMEROS DE PUERTO DE PROTOCOLO PARA IDENTIFICAR EL DESTINO FINAL.**
- **DEFINE PAR (DIR IP, N° PUERTO) = PUNTO EXTREMO**
- **CONEXIÓN TCP SE IDENTIFICA POR UN PAR DE PUNTOS EXTREMOS.**
- **EL N° DE PUERTO EN UNA MISMA MÁQUINA PUEDE SER COMPARTIDO POR VARIAS CONEXIONES.**

APLICACIÓN		TRANSPORTE		NRO PUERTOS	
FTP	21	TCP	21	1	
TELNET	23	TCP	23	1	
SMTP	25	TCP	25	1	
DNS	53	UDP	53	1	
TFTP	69	UDP	69	1	
SNMP	161	UDP	161	1	

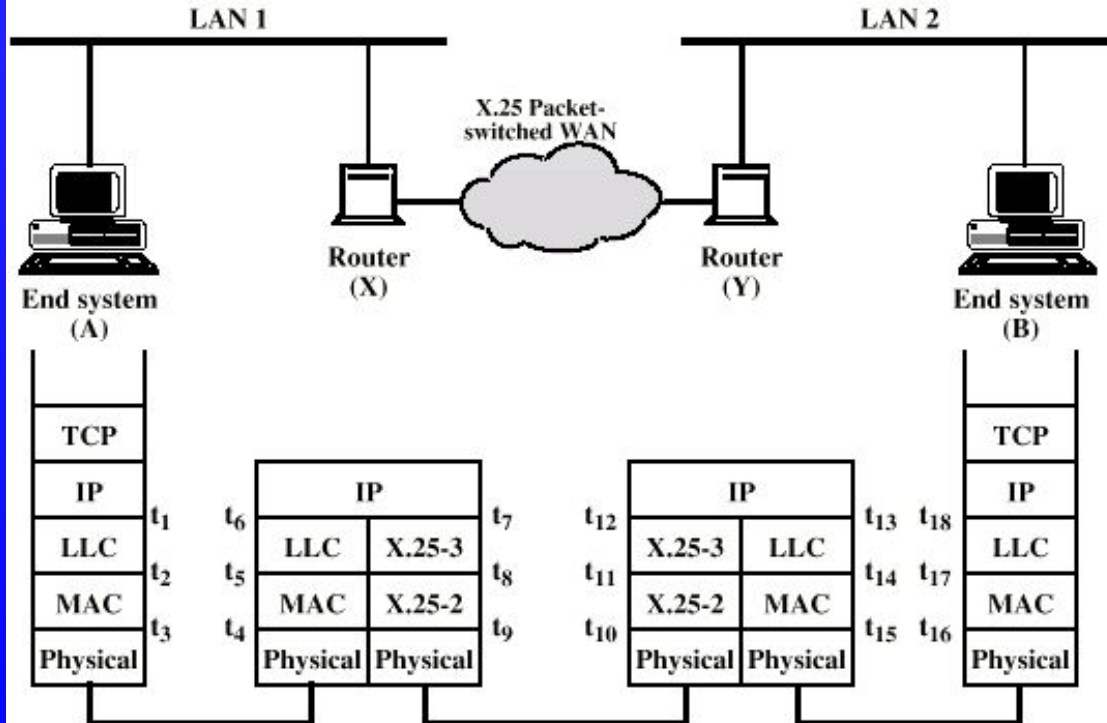
PUERTOS UDP Y TCP

- 20 (TCP), utilizado por FTP (File Transfer Protocol) para datos
- 21 (TCP), utilizado por FTP (File Transfer Protocol) para control
- 25 (TCP), utilizado por SMTP (Simple Mail Transfer Protocol)
- 53 (TCP), utilizado por DNS (Domain Name System)
- 53 (UDP), utilizado por DNS (Domain Name System)
- 67 (UDP), utilizado por BOOTP BootStrap Protocol (Server) y por DHCP
- 68 (UDP), utilizado por BOOTP BootStrap Protocol (Client) y por DHCP
- 69 (UDP), utilizado por TFTP (Trivial File Transfer Protocol)
- 80 (TCP), utilizado por HTTP (HyperText Transfer Protocol)
- 88 (TCP), utilizado por Kerberos (agente de autenticación)
- 110 (TCP), utilizado por POP3 (Post Office Protocol)
- 137 (TCP), utilizado por NetBIOS (servicio de nombres)
- 137 (UDP), utilizado por NetBIOS (servicio de nombres)
- 138 (TCP), utilizado por NetBIOS (servicio de envío de datagramas)
- 138 (UDP), utilizado por NetBIOS (servicio de envío de datagramas)
- 139 (TCP), utilizado por NetBIOS (servicio de sesiones)
- 139 (UDP), utilizado por NetBIOS (servicio de sesiones)
- 143 (TCP), utilizado por IMAP4 (Internet Message Access Protocol)
- 443 (TCP), utilizado por HTTPS/SSL (transferencia segura de páginas web)
- 631 (TCP), utilizado por CUPS (sistema de impresión de Unix)
- 993 (TCP), utilizado por IMAP4 sobre SSL
- 995 (TCP), utilizado por POP3 sobre SSL
- 1080 (TCP), utilizado por SOCKS Proxy
- 1433 (TCP), utilizado por Microsoft-SQL-Server
- 1434 (TCP), utilizado por Microsoft-SQL-Monitor
- 1434 (UDP), utilizado por Microsoft-SQL-Monitor
- 1701 (UDP), utilizado para Enrutamiento y Acceso Remoto para VPN con L2TP.
- 1723 (TCP), utilizado para Enrutamiento y Acceso Remoto para VPN con PPTP.
- 1761 (TCP), utilizado por Novell Zenworks Remote Control utility
- 1863 (TCP), utilizado por MSN Messenger

CONTROL DE ERRORES

IP - UDP - TCP

	PROTOCOLO		
Tipo de control de error	IP	UDP	TCP
Detección	Del Header	Del datagrama UDP + Dir IP	Del segmento TCP + Dir IP
Corrección / Recuperación	No	No (a cargo de aplicaciones)	Del segmento TCP + Dir IP



$t_1, t_6, t_7, t_{12}, t_{13}, t_{18}$

IP-H	TCP-H	Data
------	-------	------

t_2, t_5

LLC1-H	IP-H	TCP-H	Data
--------	------	-------	------

t_3, t_4

MAC1-H	LLC1-H	IP-H	TCP-H	Data	MAC1-T
--------	--------	------	-------	------	--------

t_8, t_{11}

XP-H	IP-H	TCP-H	Data
------	------	-------	------

t_9, t_{10}

XL-H	XP-H	IP-H	TCP-H	Data	XL-T
------	------	------	-------	------	------

t_{14}, t_{17}

LLC2-H	IP-H	TCP-H	Data
--------	------	-------	------

t_{15}, t_{16}

MAC2-H	LLC2-H	IP-H	TCP-H	Data	MAC2-T
--------	--------	------	-------	------	--------

TCP-H = TCP header

IP-H = IP header

LLCi-H = LLC header

MACi-H = MAC header

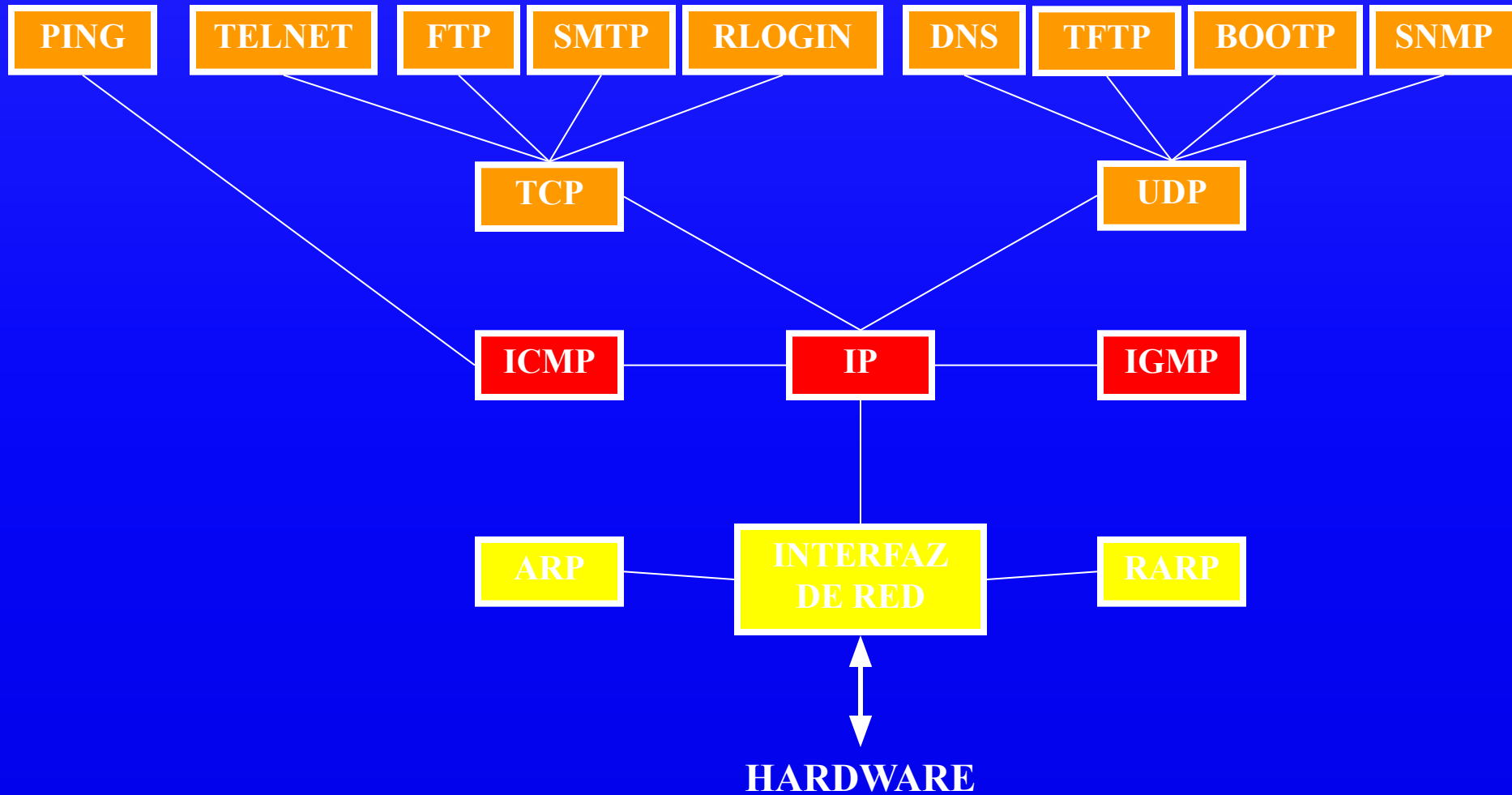
MACi-T = MAC trailer

XP-H = X.25 packet header

XL-H = X.25 link header

XL-T = X.25 link trailer

ESQUEMA EN BLOQUES DE LOS PROTOCOLOS



APLICACIONES

TELNET

TCP

CONEXIÓN REMOTA A TRAVÉS DE INTERNET
CON AUTENTICACION

FTP

TCP

PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS
COPIADO DE ARCHIVOS
CON AUTENTICACIÓN

TFTP

UDP

ECONÓMICO Y MENOS SOFISTICADO QUE EL FTP
SIN AUTENTICACIÓN
T (TRIVIAL)

DNS

UDP

SISTEMA DE NOMBRE DE DOMINIO
TRADUCE LA DIRECCIÓN IP A UN NOMBRE
SIGNIFICATIVO DE ALTO NIVEL

APLICACIONES

PING

ICMP

ENVIA SOLICITUD DE ECO, CAPTURA LA RESPUESTA Y REALIZA ESTADÍSTICA.

BOOTP

UDP

PROTOCOLO PARA MEJORAR EL RARP.

ESPECIFICA ASPECTOS DE ARRANQUE COMO DIR IP MÁQUINA, RUTEADOR Y SERVIDOR.

DHCP

UDP

PROTOCOLO PARA CONFIGURACIÓN DE HOST DINÁMICA. ASIGNACIÓN DE DIR IP POR SERVIDOR A CLIENTES.

SMTP

TCP

PROTOCOLO DE TRANSFERENCIA DE CORREO SIMPLE. ESPECIFICA FORMATO DE MENSAJES. USA EL ASCII.

SNMP

UDP

PROTOCOLO DE ADMINISTRACIÓN DE RED SIMPLE. DEFINEN RELACIONES ADMINISTRATIVAS ENTRE ROUTERS, FORMA Y SIGNIFICADO DE MENSAJES ENTRE OTROS ASPECTOS.

ROUTERS Y RUTEO

- **ROUTER** ES UN DISPOSITIVO DE NIVEL 3 DEL OSI
- POSEE PUERTAS PARA ENLACES LAN, WAN Y PARA CONSOLA.
- SU CONFIGURACIÓN INCLUYE TABLAS DE RUTEO. APRENDE DIRECCIONES IP.
- PERMITE LA SEGMENTACIÓN DE UNA LAN (IGUAL QUE EL BRIDGE Y EL SWITCH).
- PROVEE SEGURIDAD A LA RED.
- **RUTEO** ES EL ENCAMINAMIENTO DE LOS DATAGRAMAS DE UNA RED A LA OTRA, MEDIANTE RUTAS.
- LAS RUTAS PUEDEN SER **ESTÁTICAS** (INGRESADAS POR EL ADMINISTRADOR DE RED) O **DINÁMICAS** (AJUSTADAS AUTOMÁTICAMENTE MEDIANTE PROTOCOLOS DE RUTEO).
- PROTOCOLOS DE RUTEO PROVEEN INFORMACIÓN SOBRE ACCESIBILIDAD, RETARDOS Y TABLAS DE RUTEO.
- ALGUNOS PROTOCOLOS DE RUTEO: RIP, IGRP, OSPF, EGP

EJEMPLO DE RUTEO

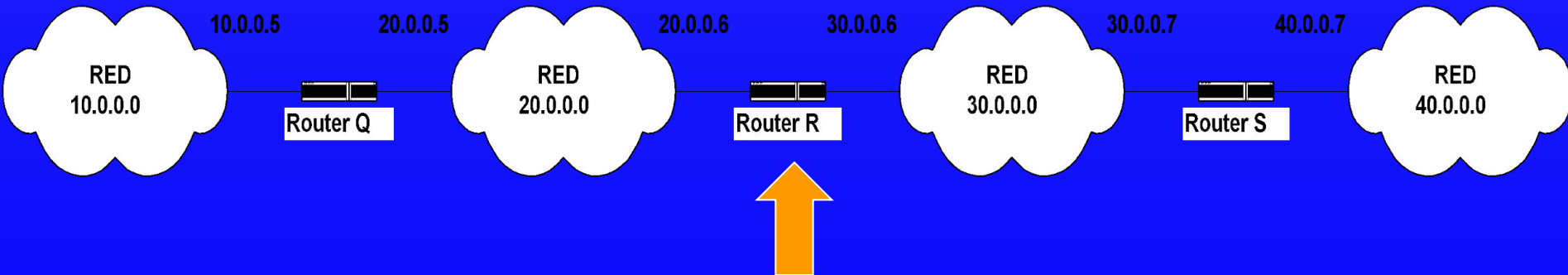


TABLA DE RUTEO EN R

PARA ALCANZAR LOS ANFITRIONES DE LA RED	RUTEAR A ESTA DIRECCIÓN
20.0.0.0	ENTREGA DIRECTA
30.0.0.0	ENTREGA DIRECTA
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

RUTEO

- **PROTOCOLO DE RUTEO INTERIOR (IRP):** distribuye información de ruteo dentro de un sistema autónomo (AS). Información más detallada.
- **PROTOCOLO DE RUTEO EXTERIOR (ERP):** distribuye información de ruteo entre diferentes sistemas autónomos. Más simple, información menos detallada. Ej: **BGP** (protocolo de pasarela de frontera)

ESTRATEGIAS DE RUTEO

- **POR VECTOR DISTANCIA:** intercambio de información con vecinos. Los nodos mantienen un vector de costo por enlace para cada red conectada directamente. Tx de considerable información por cada router pero menos complejo. Aplicable a los IRP. Ej: **RIP**
- **POR ESTADO DE ENLACE:** intercambio de info de costos de enlace con todos los routers. Tienen la configuración completa de la red. Aplicable a los IRP. Ej: **OSPF**
- **POR VECTOR CAMINO:** no incluye estimación de distancia ni de costo. Se puede limitar el paso por otros AS. Aplicable a los ERP.

BGP

- **Es un ERP. Usa mensajes (M) sobre TCP para intercambio de información entre routers (R). Versión actual es BGP 4.**
- **Procedimientos funcionales:**
 - **Adquisición de vecino. Entre R en diferentes AS. M de aceptación o rechazo.**
 - **Detección de vecino alcanzable. M de mantenimiento.**
 - **Detección de red alcanzable. Cada R mantiene una base de datos con redes alcanzables y rutas preferidas. R manda un M de actualización cuando cambios.**

OSPF

- **Es un IRP. Calcula una ruta a través de una interconexión de redes suponiendo el menor costo según configure el usuario (retardo, velocidad de tx, económico u otros).**
- **R mantiene una base de datos de la topología del AS.**

COMANDO TRACERT (WINDOWS)

- C:\Documents and Settings\usuario>tracert
- Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
- nombre_destino

- Opciones:
- -d No convierte direcciones en nombres de hosts.
- -h saltos_máximos Máxima cantidad de saltos en la búsqueda del objetivo.
- -j lista-de-host Enrutamiento relajado de origen a lo largo de la lista de hosts.
- -w tiempo_espera Cantidad de milisegundos entre intentos.

- C:\Documents and Settings\usuario>tracert http://www.comunicacionnueva.com.ar

- Traza a la dirección http://www.comunicacionnueva.com.ar [190.210.9.24]
- sobre un máximo de 30 saltos:

- 1 <1 ms <1 ms <1 ms 192.168.1.1
- 2 8 ms 7 ms 7 ms 1-1-167-181.fibertel.com.ar [181.167.1.1]
- 3 * * * Tiempo de espera agotado para esta solicitud.
- 4 * * * Tiempo de espera agotado para esta solicitud.
- 5 * * * Tiempo de espera agotado para esta solicitud.
- 6 10 ms 11 ms 12 ms 13-165-89-200.fibertel.com.ar [200.89.165.13]
- 7 9 ms 12 ms 28 ms 6-165-89-200.fibertel.com.ar [200.89.165.6]
- 8 31 ms 11 ms 11 ms 150-165-89-200.fibertel.com.ar [200.89.165.150]
- 9 11 ms 11 ms 16 ms 200-42-50-110.prima.net.ar [200.42.50.110]
- 10 12 ms 10 ms 11 ms customer-static-210-110-233.iplannetworks.net [1
- 90.210.110.233]
- 11 12 ms 11 ms 12 ms customer-static-210-110-54.iplannetworks.net [19
- 0.210.110.54]
- 12 9 ms 11 ms 11 ms customer-static-210-110-185.iplannetworks.net [1
- 90.210.110.185]
- 13 16 ms 19 ms 22 ms 190.210.124.225
- 14 8 ms 11 ms 12 ms hwy104.host4g.com [190.210.9.55]
- 15 10 ms 11 ms 11 ms ws56.host4g.com [190.210.9.24]

- Traza completa.

- C:\Documents and Settings\usuario>

IP v 6

CAUSAS IP NUEVA GENERACIÓN (IP NG)

- CAMPO DE DIRECCIÓN DE 32 BITS EN IP v 4.

MEJORAS DE IP v 6

- ESPACIO DE DIRECCIONES AMPLIADO. 128 BITS PARA DIRECCIÓN.
- FORMATO DE ENCABEZADO FLEXIBLE.
- MECANISMO DE OPCIONES MEJORADO.
- PERMITE CARACTERÍSTICAS ADICIONALES.
- FUNCIONALIDAD PARA LA ASIGNACIÓN DE RECURSOS.



ESTRUCTURA IPv6

Denominación de la PDU = PAQUETE (sigue siendo sin conexión)

Cabecera de longitud fija (40 octetos)

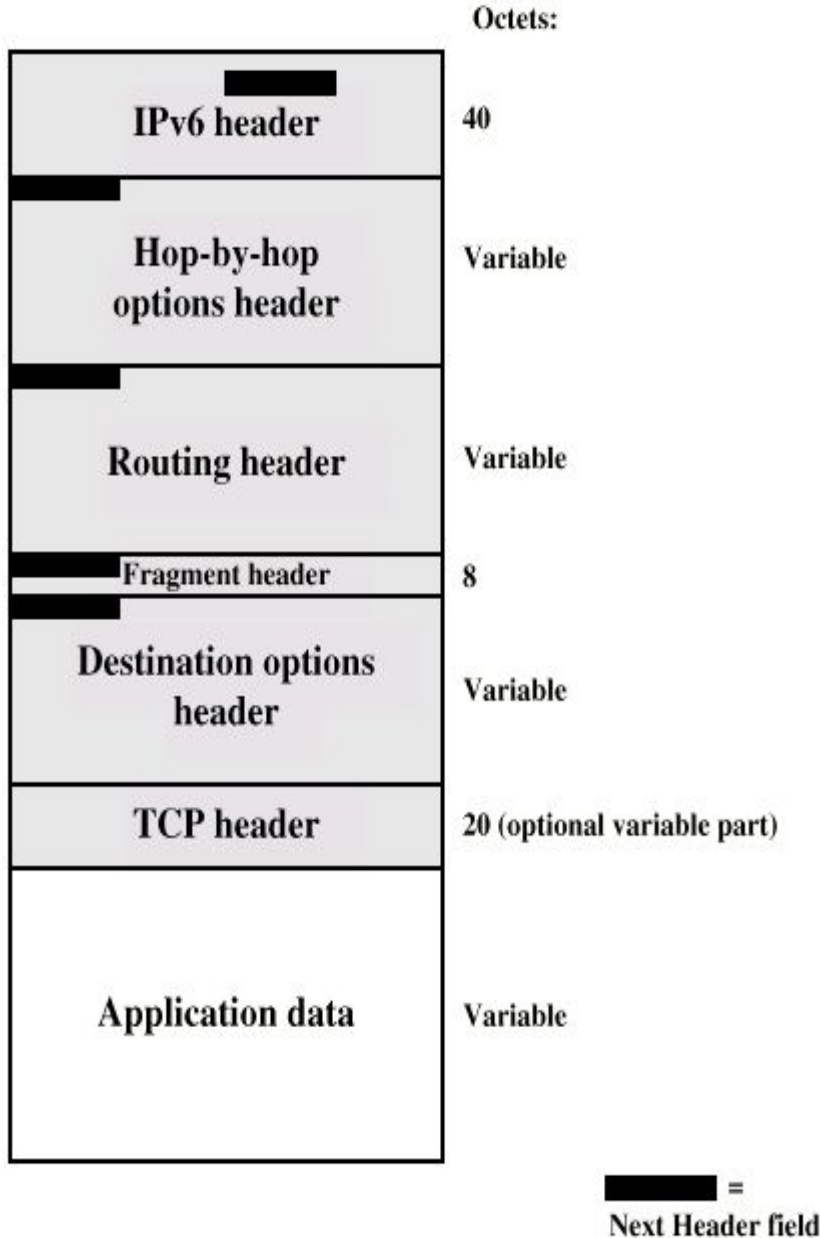
40 OCTETOS



Cabeceras de Extensión en orden según recomendación de estándar

- **Opciones salto a salto**
- **Opciones para el destino (primer destino y destinos subsecuentes)**
- **Encaminamiento**
- **Fragmentación**
- **Autenticación**
- **Encapsulado de la carga de seguridad**
- **Opciones para el destino (destino final)**

EJEMPLO DE PAQUETE IPv6



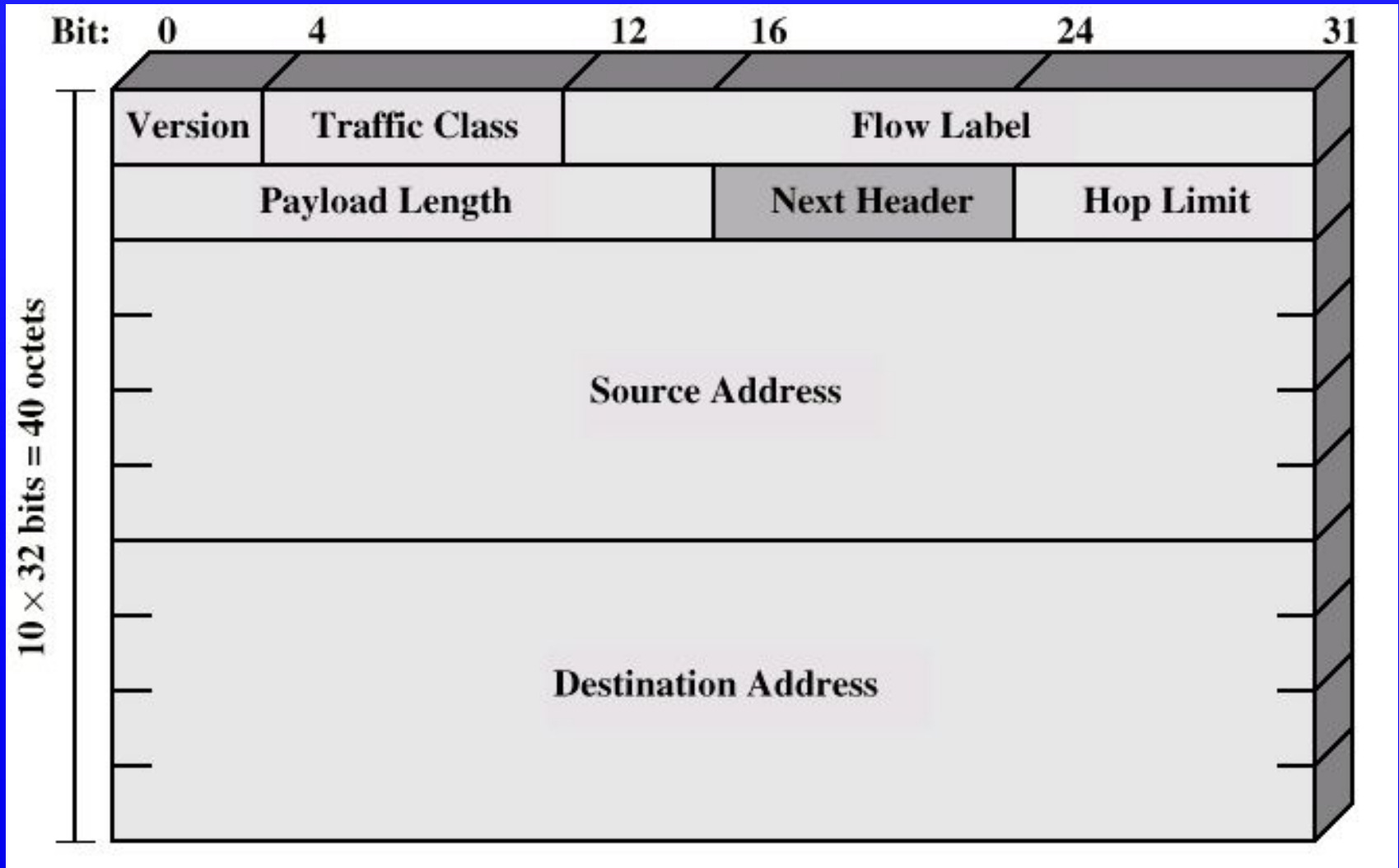
Cabecera obligatoria

Cabeceras de extensión opcionales

Cuerpo del paquete (TCP en este caso)

Campo cabecera siguiente: identifica el tipo de cabecera que sigue.

CABECERA PAQUETE IPv6



10 palabras de 4 Bytes (32 bits)

Menos campos que en IPv4 = menos procesamiento por paquete

CABECERA PAQUETE IPv6

- Versión (4 b): número
- Clase de tráfico (8 b): identificar y distinguir entre clases o prioridades de paquete. Servicios diferenciados (6) y Notificación de Congestión Explícita (2).
- Etiqueta de flujo (20 b): etiquetar paquetes con tratamiento especial de encaminamiento. Flujo es la secuencia de paquetes del origen, con iguales requisitos de tratamiento.
- Longitud de la carga útil (16 b): en octetos de todas las cabeceras de extensión y la PDU de transporte.
- Cabecera siguiente (8 b): puede ser de extensión o de TCP / UDP.
- Límite de saltos (8 b): saltos permitidos para el paquete que se descuenta en 1 en cada nodo que lo reenvía.
- Dirección origen y destino (128 b): en el caso de destino puede que no sea el último deseado si está la cabecera de encaminamiento.

DIRECCIONES IPv6

- Se asignan a interfaces individuales (II) de Nodos. Una interfaz puede tener múltiples direcciones asociadas y pueden identificar en forma única a un Nodo.
- Se combina dirección larga y múltiple por interfaz = eficiencia mejorada en el encaminamiento.
- Permite agrupar por jerarquía de red, proveedores de acceso, proximidad geográfica, institución, etc. Tablas de encaminamiento más pequeñas y consultas más rápidas.
- Tipos:
 - unidifusión (unicast): identificador para una II.
 - monodifusión (anycast): identificador para un conjunto de II. Se entrega a una II (la más cercana) según protocolo de enrutamiento.
 - multidifusión (multicast): identificador para un conjunto de II. Se entrega a todas las II.

DIRECCIONES IPv6

- Notación en hexadecimal con dos puntos, para facilitar el manejo.
- Son 16 Bytes, con dos números hexadecimales cada uno. Ejemplo de simplificación:

FF05:0000:0000:0000:0000:0000:0000:00B3

FF05:0:0:0:0:0:0:B3

FF05::B3

- Prefijos para determinar clases. Propuestas.

ALGO MAS SOBRE TCP/IP

RFC (REQUEST FOR COMMENT) = PUBLICACIONES QUE ESPECIFICAN ASPECTOS DE TCP/IP

PPP (POINT TO POINT PROTOCOL)

- PERMITE TRANFERIR INFORMACIÓN DESDE DISTINTOS PROTOCOLOS Y CONTROLA EL ESTADO DE LAS DISTINTAS OPCIONES DE ENLACES.
- REALIZA ENCAPSULACIÓN PPP.
- INCLUYE AUTENTICACIÓN, COMPRESIÓN, DETECCIÓN DE ERRORES Y MULTIENTLACE.

SOCKET

ES UNA ABSTRACCIÓN COMO MECANISMO DE ACCESO A ARCHIVOS DEL SISTEMA OPERATIVO. RELACIONA APLICACIÓN Y PROTOCOLOS TCP/IP SOBRE DETALLES DEL SISTEMA OPERATIVO.

DHCP

PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST

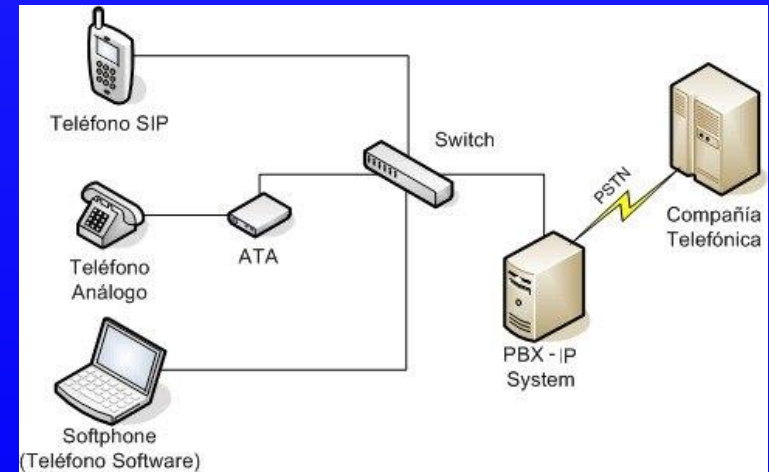
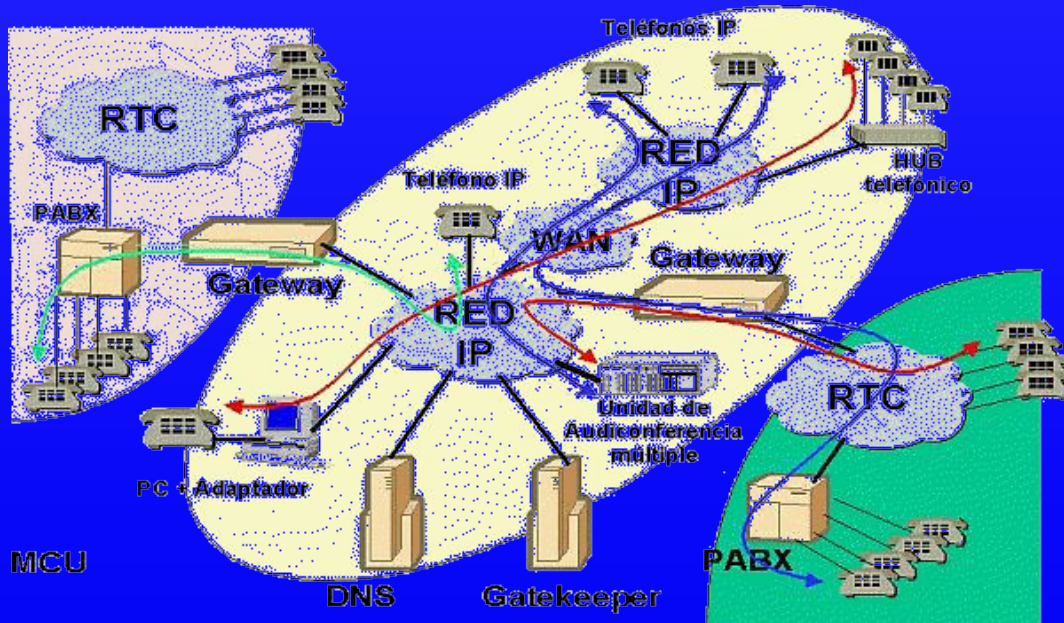
Dynamic Host Configuration Protocol (DHCP)	
Función	Configuración automática de parámetros de red
Puertos	67/UDP (servidor) 68/UDP (cliente)
Ubicación en la pila de protocolos	
Aplicación	DHCP
Transporte	UDP
Red	IP
Estándares	
RFC 2131 (1997)	

Protocolo tipo **CLIENTE SERVIDOR**

Extensión del protocolo **BOOTP**

Permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el dispositivo es conectado en un lugar diferente de la red.

VOZ SOBRE IP



Diferenciar VoIP de telefonía IP.

Cliente: usuario skype o tef IP con equipos ATA, teléfonos IP o softphones.

Servidor: conmutador IP - IP PBX (ASTERISK) o switches.

Gateway: puente de comunicación. Proveer interfases con la telefonía tradicional.

VOZ SOBRE IP

Estándares VoIP:

H.323 (UIT-1996)

SIP (IETF) – Protocolo de Inicio de Sesión

PARÁMETROS VoIP

- **CODECS.** Garantizan codificación y compresión del audio y del video. Entre los codecs más utilizados en VoIP están G.711, G.723.1 y el G.729 (especificados por la ITU-T).
- **Retardo o latencia**
- **Calidad de servicio**



Telefonía IP

