



# Redes de computadoras

Grupo: 7006 Semestre: 2024-1

---

Paulo  
Contreras Flores

Omar  
Martínez Olivares

Zinedine  
Patiño Maza

# Conceptos generales

---



# Pila de protocolos de Internet (5 capas) [1]



datos  
(data, payload)

segmento  
(segment)

paquete  
(packet)

trama  
(frame)

bit





## Capa Física

---

- Medios físicos necesarios para poder realizar el intercambio de información entre los componentes de hardware en los cuales se basa la comunicación. [3]
- Esta comunicación es simplemente una interpretación de bits (1 o 0), representados por la emanación de impulsos eléctricos o luz, entre los componentes. [3]



## Capa Física

---

- En esta capa se definen todos los métodos mecánicos, eléctricos y funcionales necesarios para establecer y mantener la comunicación física entre sistemas de red. [3]
- Se definen tipos de transmisión (*half-dúplex, full-duplex*), niveles de voltaje, tasas de transferencia y distancias máximas de transmisión. [3]



## Capa Física

---

- No existe ningún tipo de “inteligencia” en su operación.[3]
- No se realiza ningún tipo de interpretación por parte del dispositivo.[3]



## Capa Física

- Componentes
  - NIC (Network Interface Card)
  - Hubs
  - Repetidores
  - Antenas



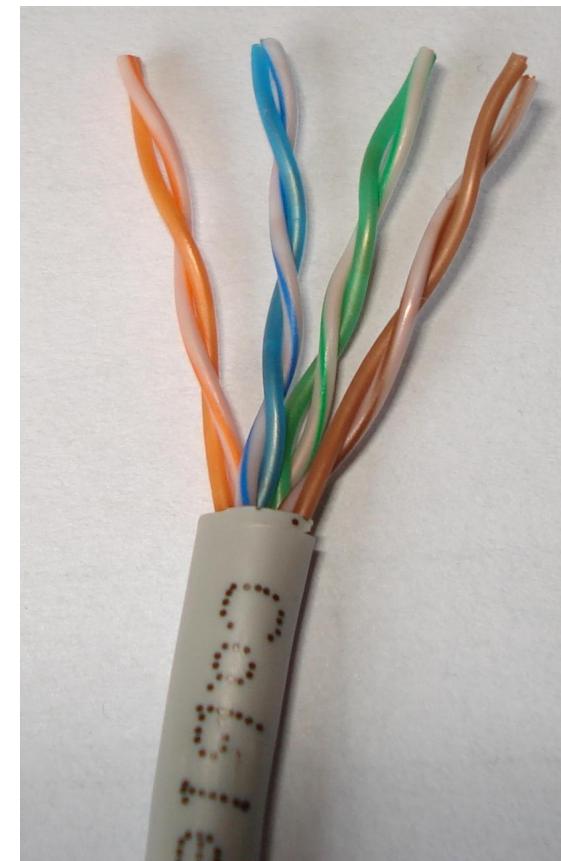
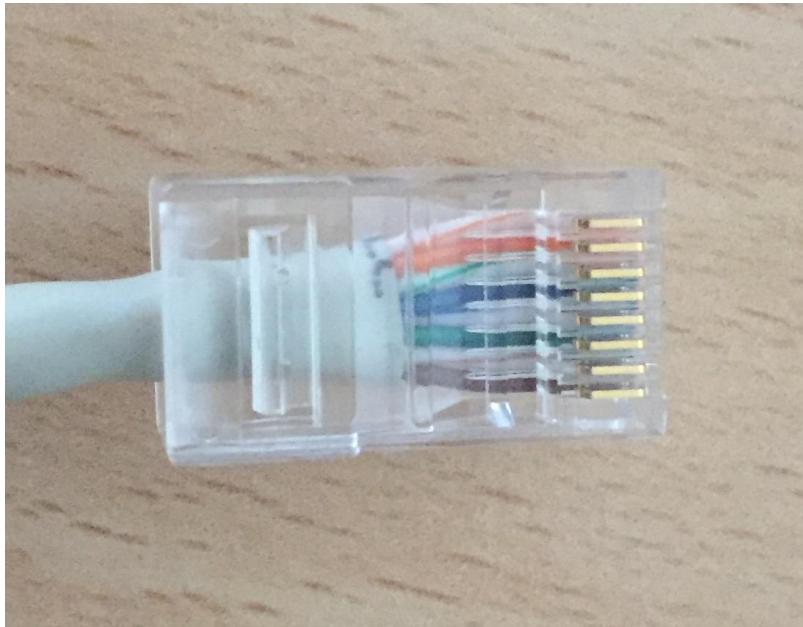
coaxial cable | [www.visualdictionaryonline.com/coaxial-cable/](http://www.visualdictionaryonline.com/coaxial-cable/) | fiber optic cable



twisted-pair cable

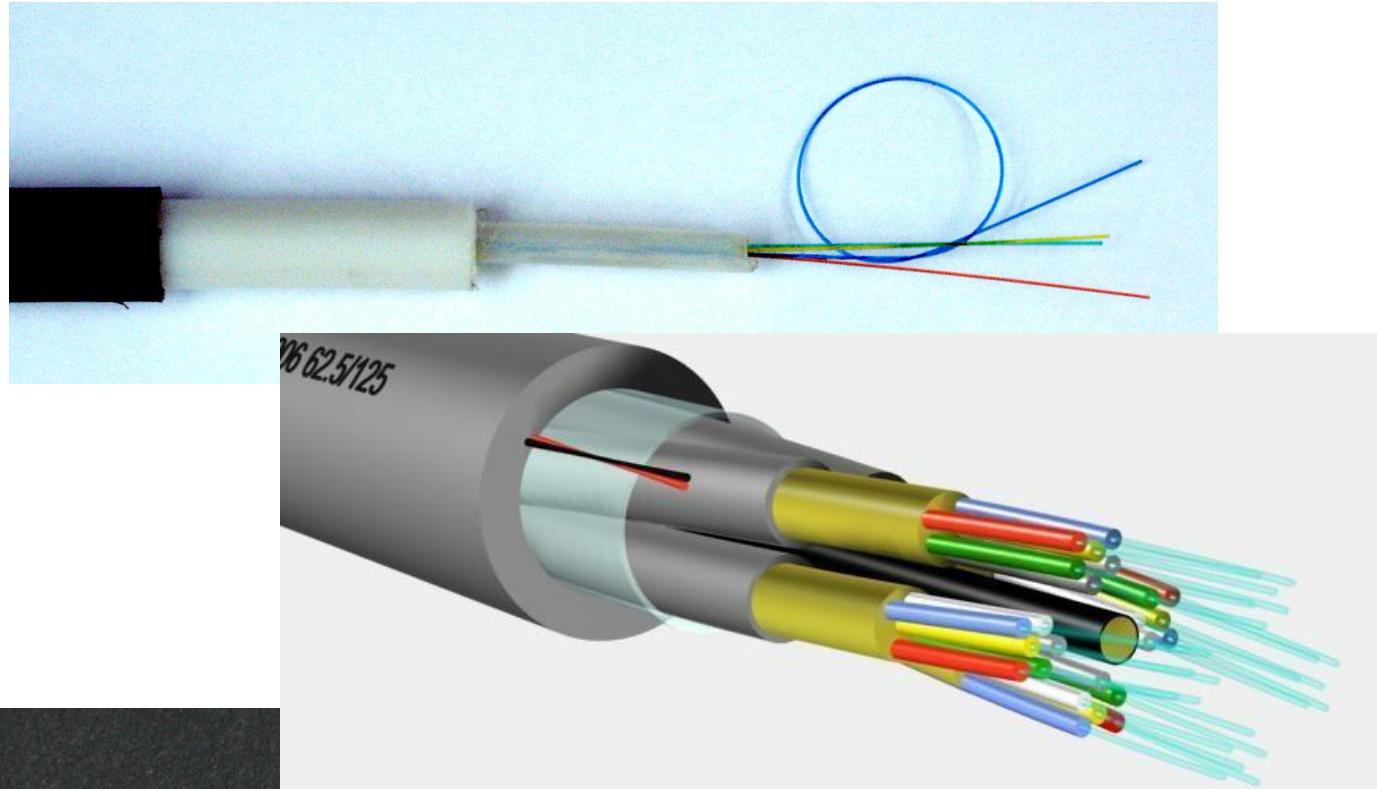
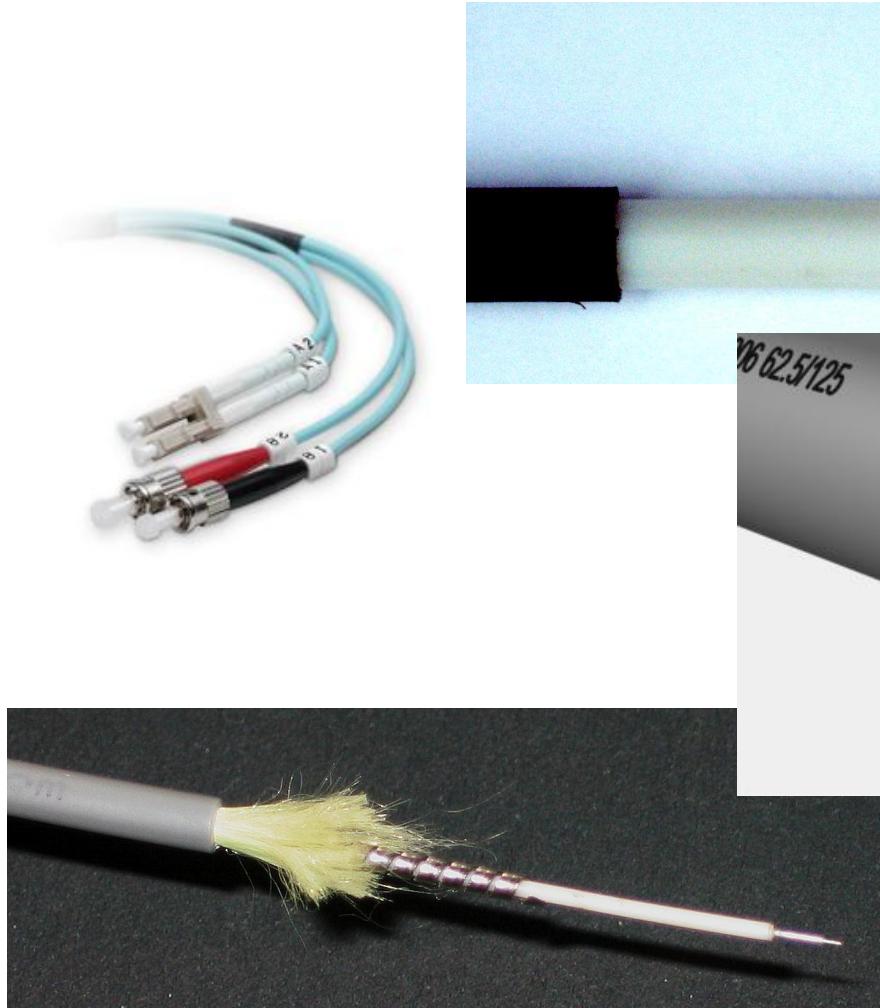


# Cable UTP



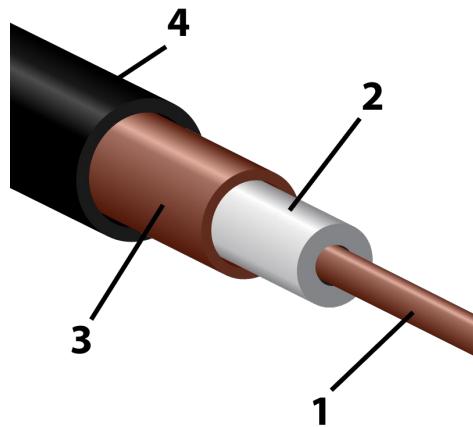


# Cable Fibra Óptica



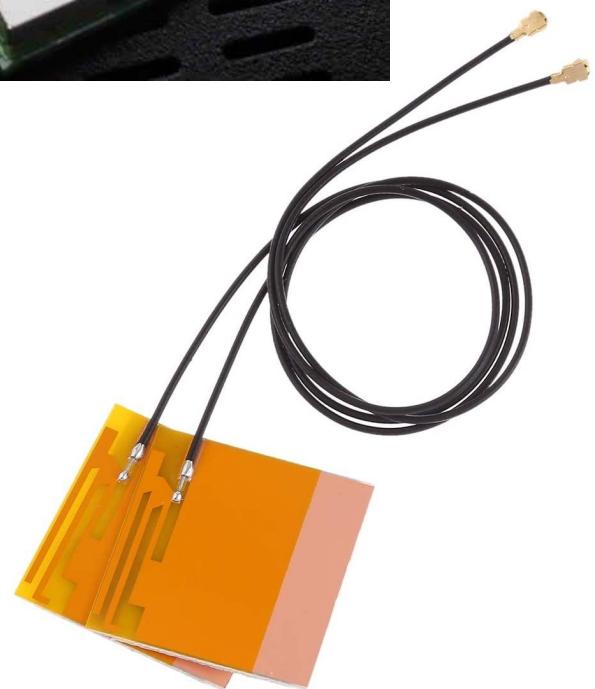


# Cable coaxial





## Antenas WiFi



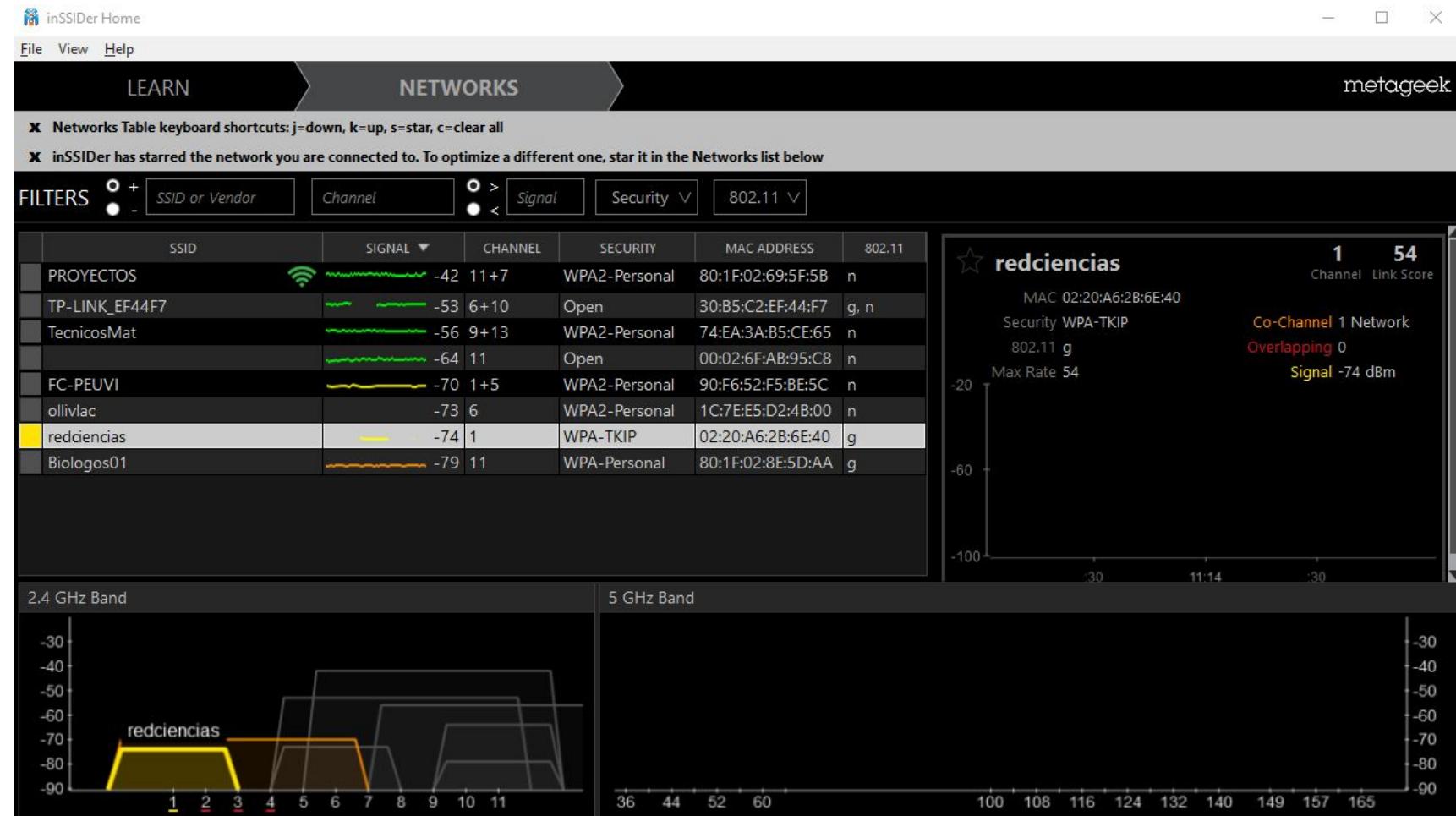


# Velocidades ethernet (IEEE 802.3) para cable UTP

Aplicación	Velocidad de transmisión	Frecuencia de operación	Pares de cable	Medio
10BASE-T	10 Mbps	10 MHz	2	cat 3, cat 5e, cat 6
100BASE-T	100 Mbps	31.25 MHz	2	cat 5e, cat 6
1000BASE-T	1 Gbps	62.5 MHz	4	cat 5e, cat 6
2.5GBASE-T	2.5 Gbps	100 MHz	4	cat 5e, cat 6
5GBASE-T	5 Gbps	200 MHz	4	cat 5e, cat 6
10GBASE-T	10 Gbps	500 MHz	4	cat 6 <sub>a</sub> , cat 7, cat 7 <sub>a</sub>
25GBASE-T	25 Gb/s	1250 MHz	4	cat 8
40GBASE-T	40 Gb/s	2000 MHz	4	cat 8



# Redes inalámbricas





# Velocidades para WiFi (IEEE 802.11) - Resumen

Velocidad de transmisión	IEEE 802.11	Frecuencia
2 Mbps		2.4 GHz
54 Mbps	a	5 GHz
11 Mbps	b	2.4 GHz
54 Mbps	g	2.4 GHz
450 Mbps	n	2.4 ó 5 GHz
1.73 Gbps	ac (WiFi 5)	5 GHz
2.4 Gbps	ax (WiFi 6)	2.4 ó 5 GHz



# Pila de protocolos de Internet (5 capas) [1]



datos  
(data, payload)

segmento  
(segment)

paquete  
(packet)

trama  
(frame)

bit





## Capa de Enlace

---

- A los datos que viajan sobre la capa de enlace se les identifica con el nombre de frame.
- La capa de enlace se encarga de recibir los bits de datos que provienen de la capa física, para poder enviarlos a las capas superiores de forma ordenada y sistemática.
- La capa física enviará siempre bits “sueltos”, pero la capa de enlace se encargará de entregar a sus capas superiores un conglomerado ordenado y segmentado de dichos bits, para que dichas capas puedan manejar la información de una manera más eficiente.



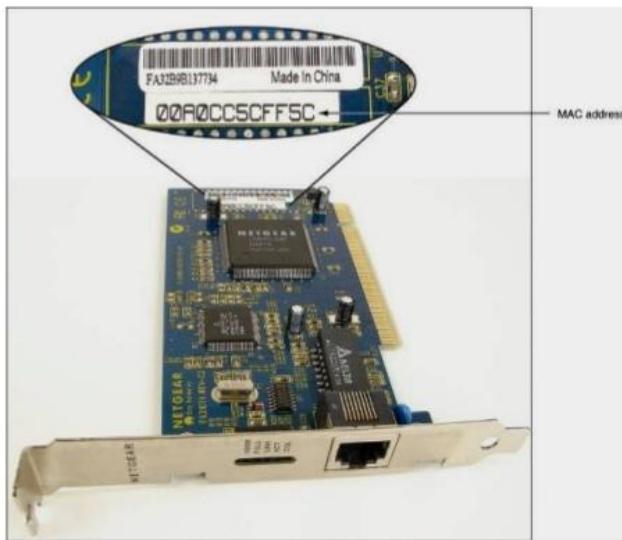
## Direcciones MAC

---

- En las redes bajo los estándares IEEE802.3 y IEEE802.11, la forma de identificar físicamente a los dispositivos de red es a través de la llamada dirección MAC (Media Access Control address).
- También se le conoce como dirección física (physical address), dirección de hardware (hardware address), dirección LAN (Local Área Network address).
- Es un identificador asignado a las NIC (Network Interface Card) por el fabricante. Esta identificación es única por dispositivo, no pudiendo repetirse en ningún lugar del mundo.



# Direcciones MAC en NIC



Ethernet (?) network card showing its MAC address

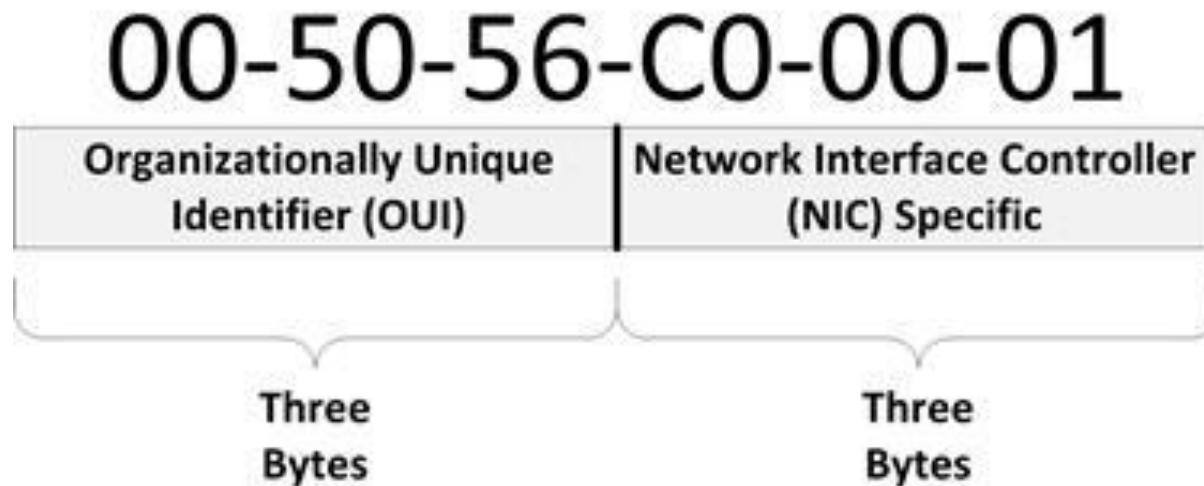


MAC Addresses  
are physically  
attached to a  
hardware device.



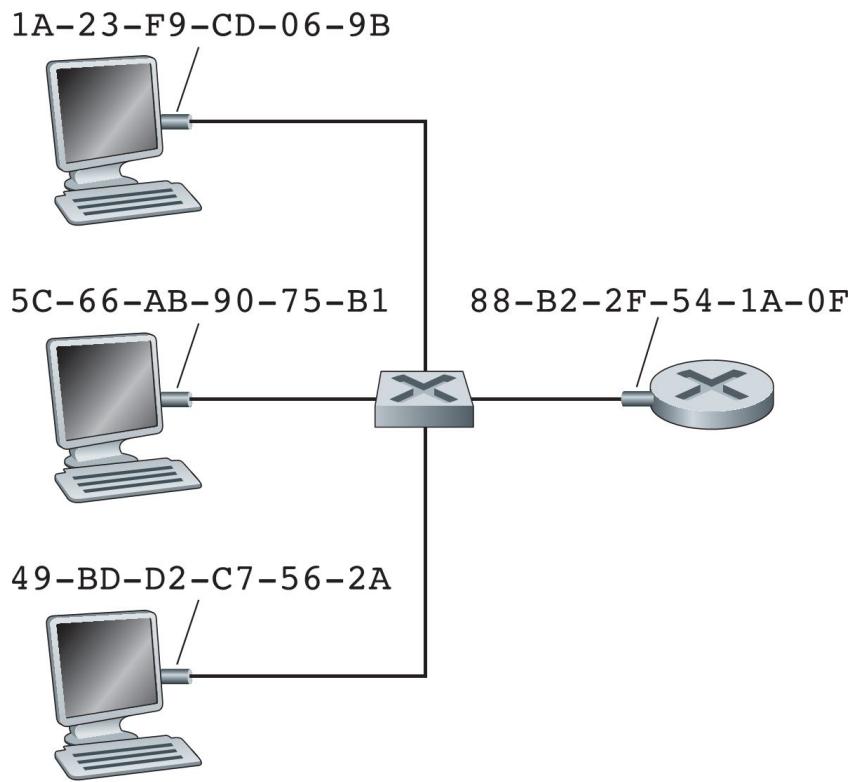
## Dirección MAC

- Está compuesta por 48 bits.
- Se representa en seis grupos de dos dígitos hexadecimales.





## Direcciones MAC



- Cada interfaz conectada a una LAN tiene una única dirección MAC o dirección física. [1]



# Comando Windows



# Comando Linux (Debian)

```
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:84:a3:87 brd ff:ff:ff:ff:ff:ff
        inet 192.168.95.91/23 brd 192.168.95.255 scope global dynamic ens33
            valid_lft 85590sec preferred_lft 85590sec
        inet 192.168.95.139/23 brd 192.168.95.255 scope global secondary ens33
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:fe84:a387/64 scope link
            valid_lft forever preferred_lft forever
```

```
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:~# ifconfig -a
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.95.91  netmask 255.255.254.0 broadcast 192.168.95.255
        inet6 fe80::20c:29ff:fe84:a387  prefixlen 64  scopeid 0x20<link>
            ether 00:0c:29:84:a3:87  txqueuelen 1000  (Ethernet)
            RX packets 93325  bytes 133601637 (127.4 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 23044  bytes 1415991 (1.3 MiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
            loop  txqueuelen 1  (Local Loopback)
            RX packets 278  bytes 23756 (23.1 KiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 278  bytes 23756 (23.1 KiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```



# Lista de MAC por fabricante

The screenshot shows a web browser window titled "Conectando..." with the URL "standards-oui.ieee.org/oui.txt". The page displays a table of MAC address entries. The columns are labeled "OUI/MA-L company\_id" and "Organization Organization Address". The data includes:

OUI/MA-L company_id	Organization Organization Address
E0-43-DB (hex) E043DB (base 16)	Shenzhen ViewAt Technology Co.,Ltd. Shenzhen ViewAt Technology Co.,Ltd. 9A,Micropofit,6th Gaoxin South Road, High-Tech Industrial Park, Nanshan, Shenzhen, CHINA.
	shenzhen guangdong 518057 CN
24-05-F5 (hex) 2405F5 (base 16)	Integrated Device Technology (Malaysia) Sdn. Bhd. Integrated Device Technology (Malaysia) Sdn. Bhd. Phase 3, Bayan Lepas FIZ Bayan Lepas Penang 11900 MY
2C-30-33 (hex) 2C3033 (base 16)	NETGEAR NETGEAR 350 East Plumeria Drive San Jose null 95134 US
3C-D9-2B (hex) 3CD92B (base 16)	Hewlett Packard Hewlett Packard 11445 Compaq Center Drive Houston 77070

<http://standards-oui.ieee.org/oui.txt>



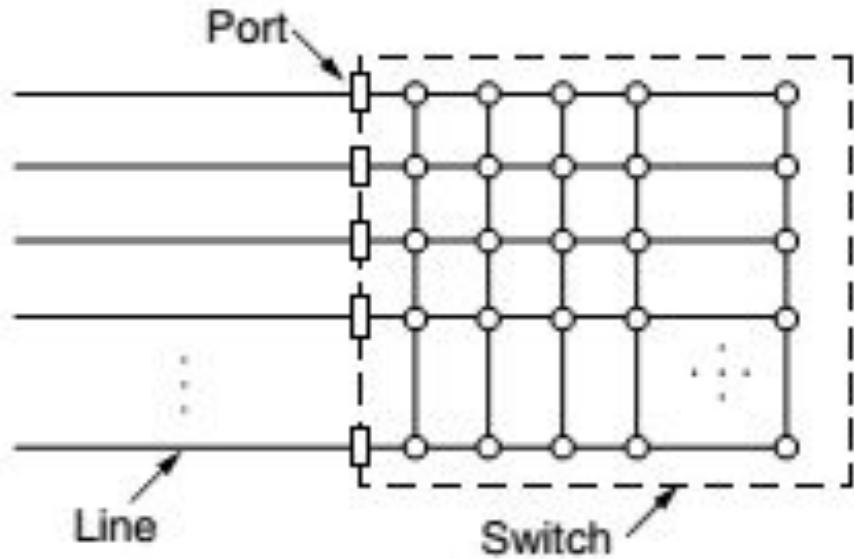
## Capa de Enlace

---

- Ejemplos de componentes de hardware de la capa de Enlace
  - Switch (comutadores)
  - Bridges (puentes)
  - Tarjeta de red (NIC)
- Ejemplos de protocolos en la capa de Enlace
  - ARP (Address Resolution Protocol)
  - PPP (Point-to-point protocol) ( $\neq$  a P2P)



## Switch



Conexión de tipo *crossbar*  
para un switch



Switch Cisco



# Switch

---

- El switch o commutador es la base de la ethernet conmutada.
- Contiene conexiones internas, el cual conecta a todos los puertos, para el tipo *crossbar*.
- Sólo envían frames (tramas) a los puertos para los cuales están destinadas.
- Cuando recibe un frame de un dispositivo, el switch verifica las direcciones MAC para ver cuál es el puerto de destino del frame.



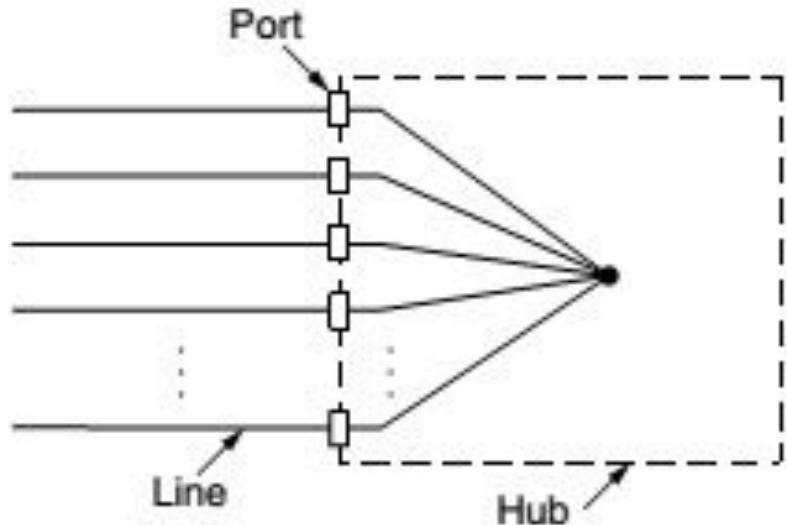
# Switch

---

- Re envía el frame a través de sus conexiones internas de alta velocidad hacia el puerto destino.
- Las conexiones internas operan a varios Gbps mediante el uso de un protocolo propietario que no necesita estandarización.
- El puerto de destino transmite el frame sobre el cable hacia el dispositivo destino.



## Hub





# Hub

---

- Conecta de manera eléctrica todos los cables que llegan a él.
- No incrementan la capacidad de la red debido a que son lógicamente equivalentes al cable extenso individual de la Ethernet clásica.
- Cuando se agregan dispositivos, cada uno recibe una parte cada vez menor de la capacidad fija de la red.
- Es un dispositivo de la capa física.



# Pila de protocolos de Internet (5 capas) [1]



datos  
(data, payload)

segmento  
(segment)

paquete  
(packet)

trama  
(frame)

bit



## Capa de Red

---

- Se encarga de la identificación lógica de los dispositivos o host conectados a una red. [3]
- Maneja los enlaces establecidos entre dichos equipos. [3]
- Establece las rutas necesarias para lograr el intercambio de paquetes entre diferentes redes. [3]



## Capa de Red

---

- A diferencia del funcionamiento de la capa 2, la identificación de los dispositivos o *host*, y el direccionamiento de enlaces de esta capa se hacen manera lógica. [3]
- Es decir, son configurados mediante software y pueden modificarse según sean necesarios. [3]
- El protocolo más utilizado para esta identificación es el IP (*Internet Protocol*), a través de las direcciones IP. [3]



## Direcciones IP

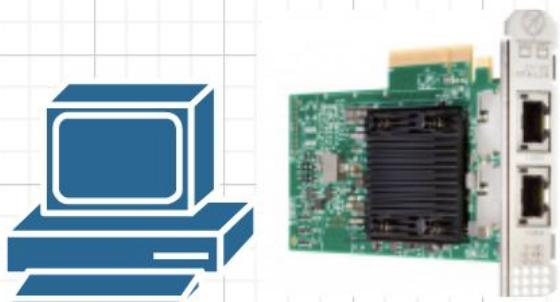
---

- Las direcciones IP permiten identificar a cada uno de los *host* dentro de una red de forma única. [3]
- No pueden existir dos *host* en una misma red con la misma dirección IP. [3]
- Técnicamente una dirección IP está asociada a una interfaz de red en un *host*. [1].
-



# Interfaces de Red

TarjetaRed con 2 interfaces/puertos



PC

enlace

Switch



Dispositivo de red



Router





## Direcciones IPv4

---

- En su versión 4 del protocolo IP, se define la dirección IP de tamaño de 32 bits. [4]
- Dando un total de  $2^{32}$  posibles direcciones IP, aproximadamente 4 mil millones de dir. IP. [1]
- Se puede definir el conjunto de direcciones IP como:  
$$IP = \{ip \mid 0 \leq ip < 2^{32}, ip \in \mathbb{Z}\}$$
- el conjunto de direcciones  $IP$  en donde cada dirección  $ip$  tiene valor entre 0 y  $2^{32}$ , siendo  $ip$  un número entero.



# Encabezado IP

Formato de la cabecera IP (versión 4)							
4 bytes							
	0-3	4-7	8-15	16-18	19-31		
20 bytes	Versión	Tamaño Cabecera	Tipo de Servicio		Longitud Total		
	Identificador			Flags	Posición de Fragmento		
	Tiempo de Vida		Protocolo	Checksum del Encabezado			
	Dirección IP de Origen						
	Dirección IP de Destino						
...	Opciones				Relleno		





# Direcciones IPv4

- Existen varias formas de representar una dirección IP, por ejemplo:

Representación	Valor
binario	11000000 10101000 00000001 00001010
octetos ( <i>dotted</i> )	192.168.1.10
decimal	3232235786
hexadecimal	C0 A8 01 0A



# Conversión de dirección IPv4

- Convertir la dirección IP:

**10000100 11111000 10110101 11111000**

a su formato por octetos

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	Total
1	0	0	0	0	1	0	0	
1	1	1	1	1	0	0	0	
1	0	1	1	0	1	0	1	
1	1	1	1	1	0	0	0	



# Conversión de dirección IPv4 (solución)

- Convertir la dirección IP:

**10000100 11111000 10110101 11111000**

a su formato por octetos

**132.248.181.248**

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	Total
1	0	0	0	0	1	0	0	132
1	1	1	1	1	0	0	0	248
1	0	1	1	0	1	0	1	181
1	1	1	1	1	0	0	0	248



# Conversión de dirección IPv4

- Convertir la dirección IP:

**10000100 11111000 10110101 11111000**

a su formato decimal

$2^{31}$	$2^{30}$	$2^{29}$	$2^{28}$	$2^{27}$	$2^{26}$	$2^{25}$	$2^{24}$	
1	0	0	0	0	1	0	0	
$2^{23}$	$2^{22}$	$2^{21}$	$2^{20}$	$2^{19}$	$2^{18}$	$2^{17}$	$2^{16}$	
1	1	1	1	1	0	0	0	
$2^{15}$	$2^{14}$	$2^{13}$	$2^{12}$	$2^{11}$	$2^{10}$	$2^9$	$2^8$	
1	0	1	1	0	1	0	1	
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	Total
1	1	1	1	1	0	0	0	



# Conversión de dirección IPv4 (solución)

- Convertir la dirección IP:

**10000100 11111000 10110101 11111000**

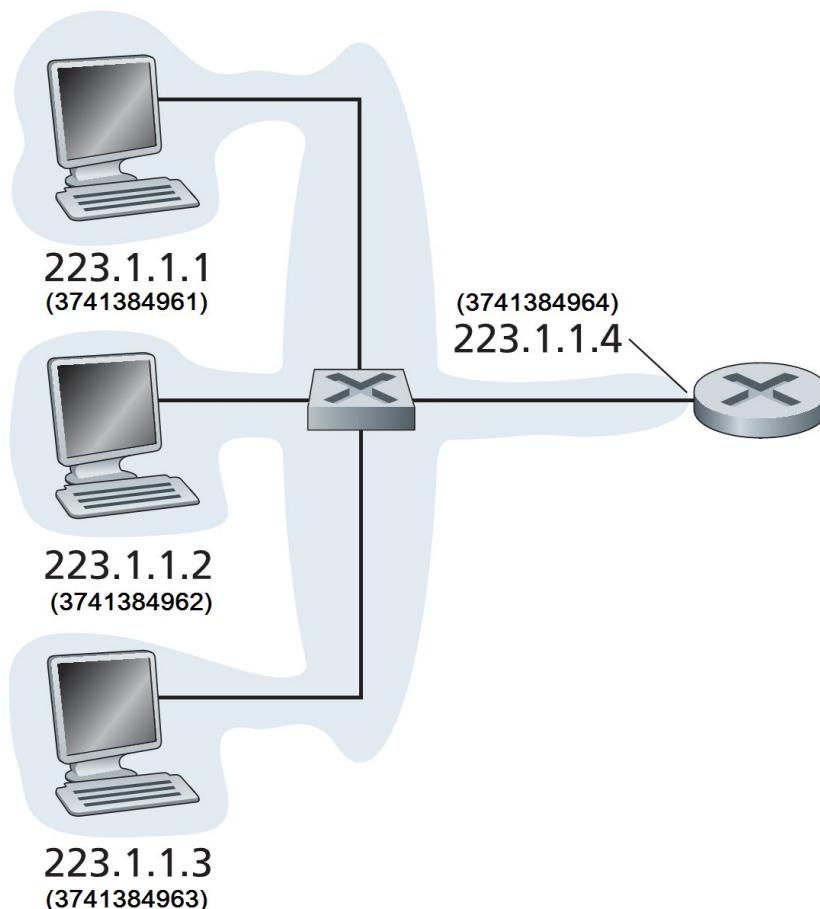
a su formato decimal

**2230892024**

$2^{31}$	$2^{30}$	$2^{29}$	$2^{28}$	$2^{27}$	$2^{26}$	$2^{25}$	$2^{24}$	
1	0	0	0	0	1	0	0	
$2^{23}$	$2^{22}$	$2^{21}$	$2^{20}$	$2^{19}$	$2^{18}$	$2^{17}$	$2^{16}$	
1	1	1	1	1	0	0	0	
$2^{15}$	$2^{14}$	$2^{13}$	$2^{12}$	$2^{11}$	$2^{10}$	$2^9$	$2^8$	
1	0	1	1	0	1	0	1	
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	Total
1	1	1	1	1	0	0	0	2230892024



## Direcciones IP



Dirección IP por interfaz de red

- Las direcciones IP permiten identificar a cada uno de los *host* dentro de una red de forma única.
- Las direcciones IP se encuentran entre:  
0.0.0.0 -> 255.255.255.255



# IANA

---



The global coordination of the DNS Root, IP addressing, and other Internet protocol resources is performed as the Internet Assigned Numbers Authority (IANA) functions. [Learn more.](#)

<https://www.iana.org/>  
<https://www.iana.org/numbers>



# Clases de direcciones IP

- Las clases de direcciones IP se establecieron para ofrecer un orden y una categorización. [3]

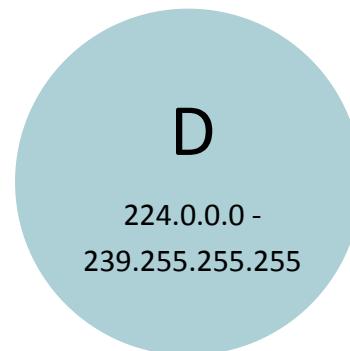
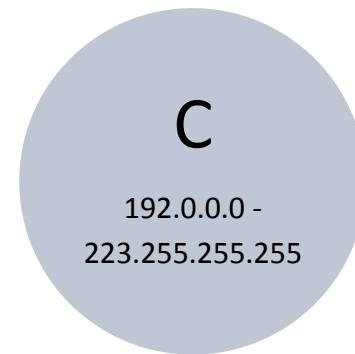
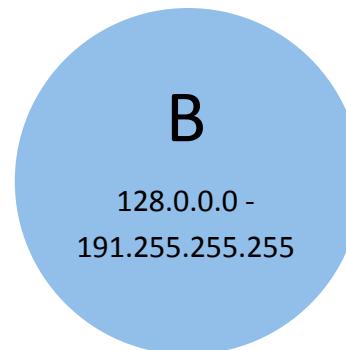
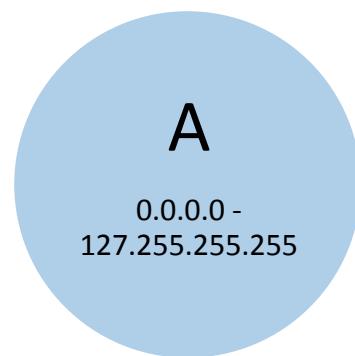
Clase	Rango	
A	0.0.0.0 - 127.255.255.255	255.0.0.0 Máscara de red
B	128.0.0.0 - 191.255.255.255	255.255.0.0 Máscara de red
C	192.0.0.0 - 223.255.255.255	255.255.255.0 Máscara de red
D	224.0.0.0 - 239.255.255.255	Para Multicast
E	240.0.0.0 - 255.255.255.255	Para uso futuro

<https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>



# Clases de direcciones IP

IPv4





# Pregunta

---

¿Que clase de direcciones IPv4 le fue asignada a la UNAM?



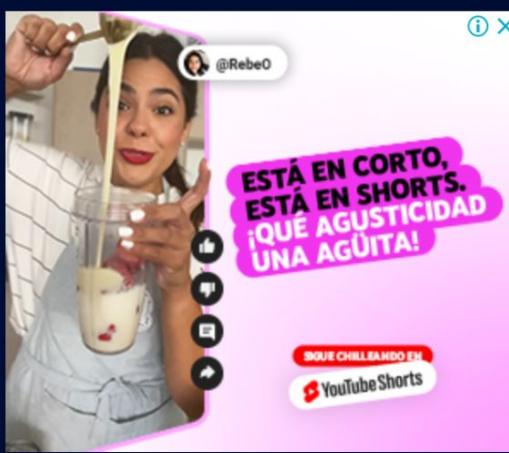
## Respuesta

Screenshot of the WhatIsMyIP.com website showing the user's public IP address and location.

https://www.whatismyip.com/es/

WhatIsMyIP.com Search.. Pricing API Sign Up Login Help

It Is My IP? IP Address Lookup IP WHOIS Lookup DNS Lookup Internet Speed Test Tools

ESTÁ EN CORTO,  
ESTÁ EN SHORTS.  
¡QUE AGUSTICIDAD  
UNA AGÜITA!

¿Cuál Es Mi IP?

Su IPv4 público es: 132.248.181.26

Su IPv6 público es: Not Detected

Ubicación: Mexico City, CMX MX

ISP: Universidad Nacional Autonoma de Mexico



## Máscara de Red predeterminada

- Conjunto de bits que permite distinguir en una dirección IP v4, la parte que corresponde al identificador de red de la parte que corresponde al asignado al host dentro de esa red

Clase A 255.0.0.0	NETID	HostID	HostID	HostID
Clase B 255.255.0.0	NETID	NETID	HostID	HostID
Clase C 255.255.255.0	NETID	NETID	NETID	HostID

NOTA: Se utiliza el operador **AND bit a bit** entre la IP del equipo y la máscara de red para obtener la dirección de la red a la que pertenece el equipo.



## Direcciones reservadas

---

**Loopback:** (Interfaces de red virtual hacia el mismo equipo)  
127.0.0.0/8, la más común 127.0.0.1.

**ID Red:** Todos los bits de la porción de host en cero

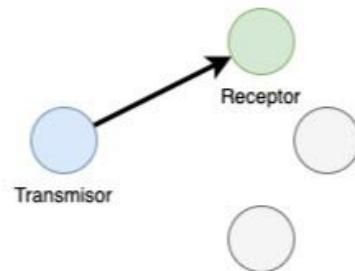
**BroadCast:** Todos los bits de la porción de host en uno

\* Ips asignables a host: ( $2^n$  bits de host) -2

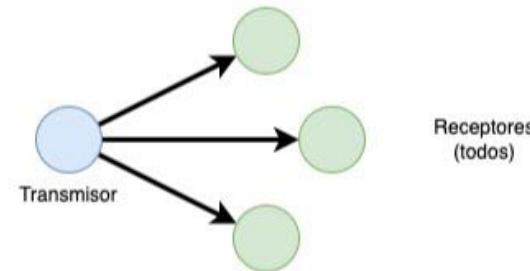


# Tipos de transmisión

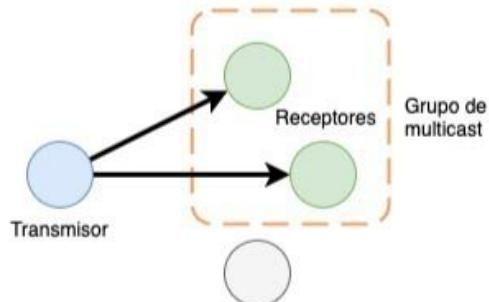
## Unicast



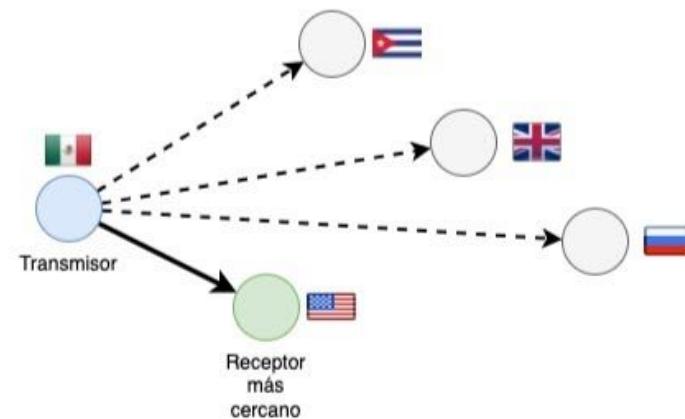
## Broadcast



## Multicast



## Anycast





## ID de red

IPv4 132.247.10.10

Máscara de red: 255.255.0.0

IP: 10000100.11110111.00001010.00001010

AND

NetMask: 11111111.11111111.00000000.00000000

=====

NetID: 10000100.11110111.00000000.00000000

AND		
A	B	R
0	0	0
0	1	0
1	0	0
1	1	1

NetID: **132.247.0.0**

Rango de direcciones asignables a host: **132.247.0.1-132.247.255.254**

$2^n$ (bits de host) -2 =  $2^{16} - 2 = 65536 - 2 = 65534$  direcciones asignables a hosts



## IP privadas por clase

- Direcciones IP **no direccionables** en Internet
- Exclusivas para uso Interno

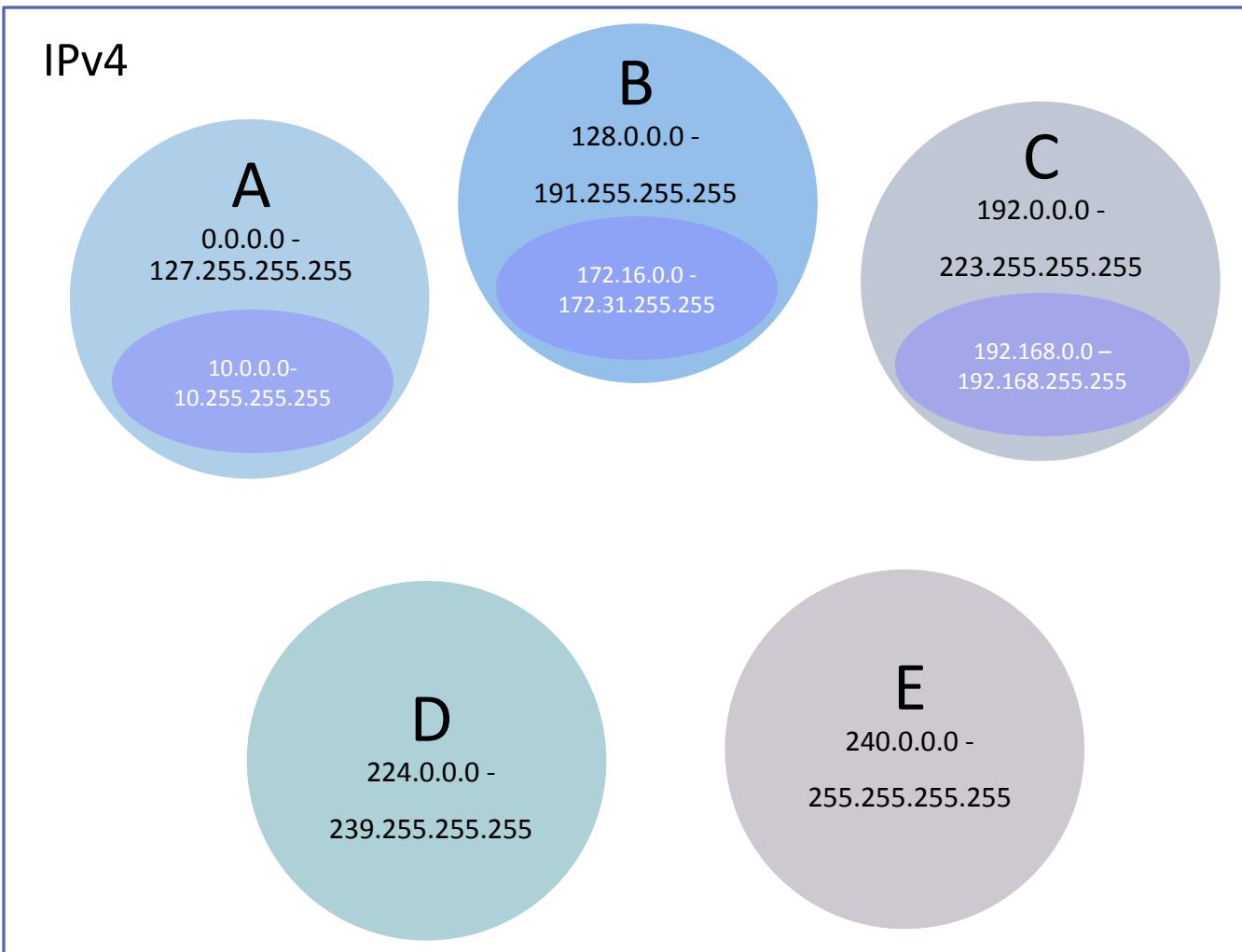
Rangos de direcciones IP privadas por clase.

Clase	Rango	
A	10.0.0.0 - 10.255.255.255	255.0.0.0 Máscara de red
B	172.16.0.0 - 172.31.255.255	255.240.0.0 Máscara de red
C	192.168.0.0 - 192.168.255.255	255.255.0.0 Máscara de red

<https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml>



# IP privadas por clase





# NAT (Network Address Translation)

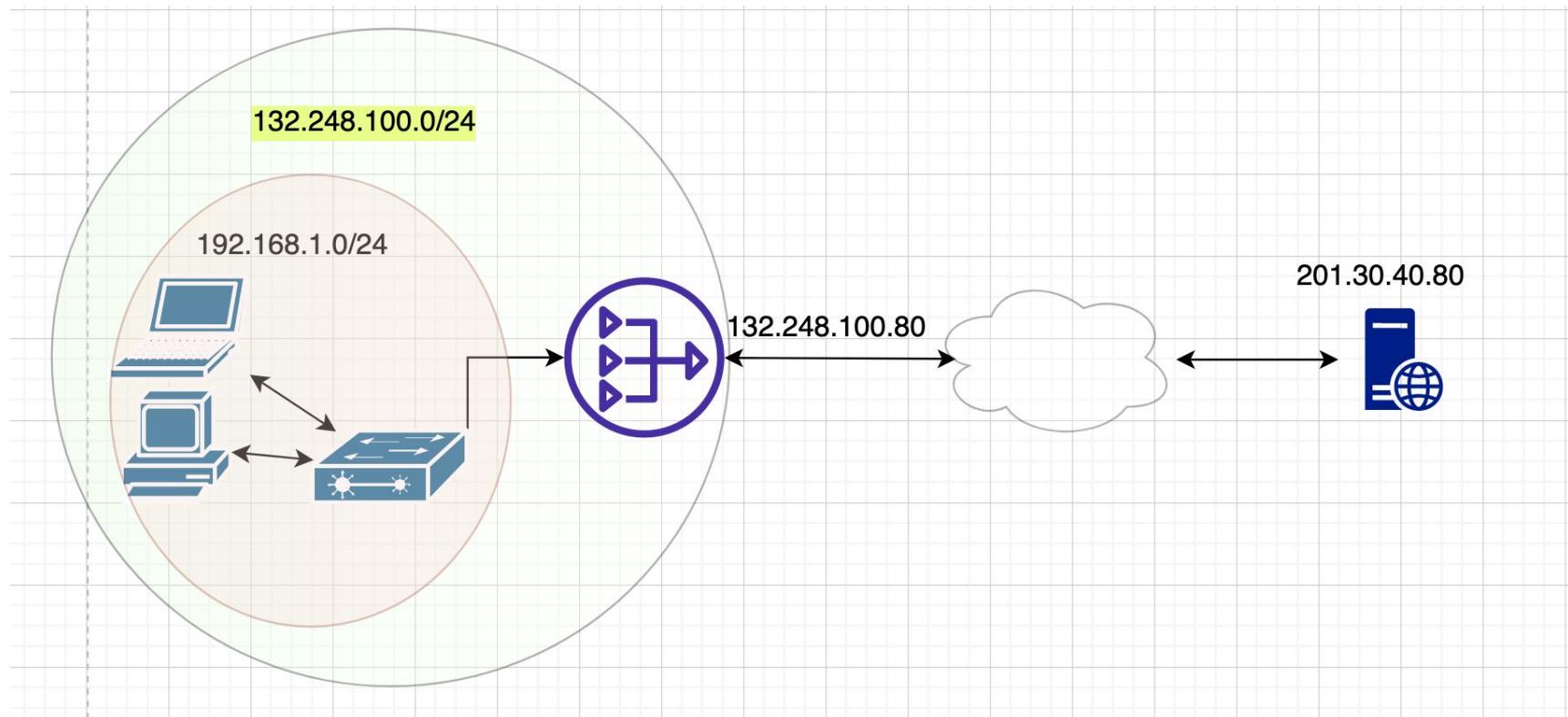
---

Protocolo de traducciones de direcciones de red.

Permite llevar a cabo la conversión de paquetes desde una red interna (por ejemplo IPs privadas) hacia una red externa (por ejemplo IPs públicas) en la capa de red.



## NAT





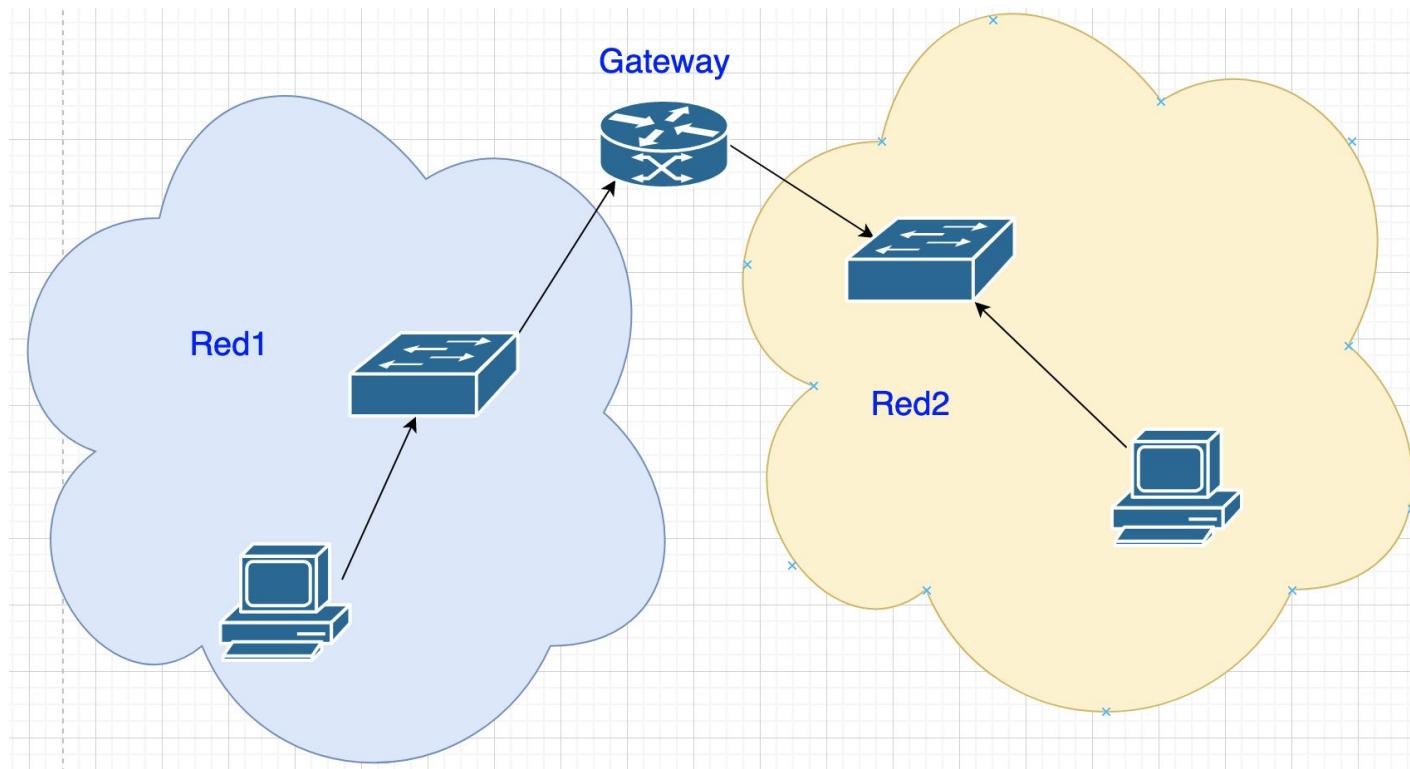
## Tabla NAT

Tabla NAT 			
IP Local	Puerto Local	IP Externa	PuertoNat
192.168.1.20	5323	132.248.10.20	4567



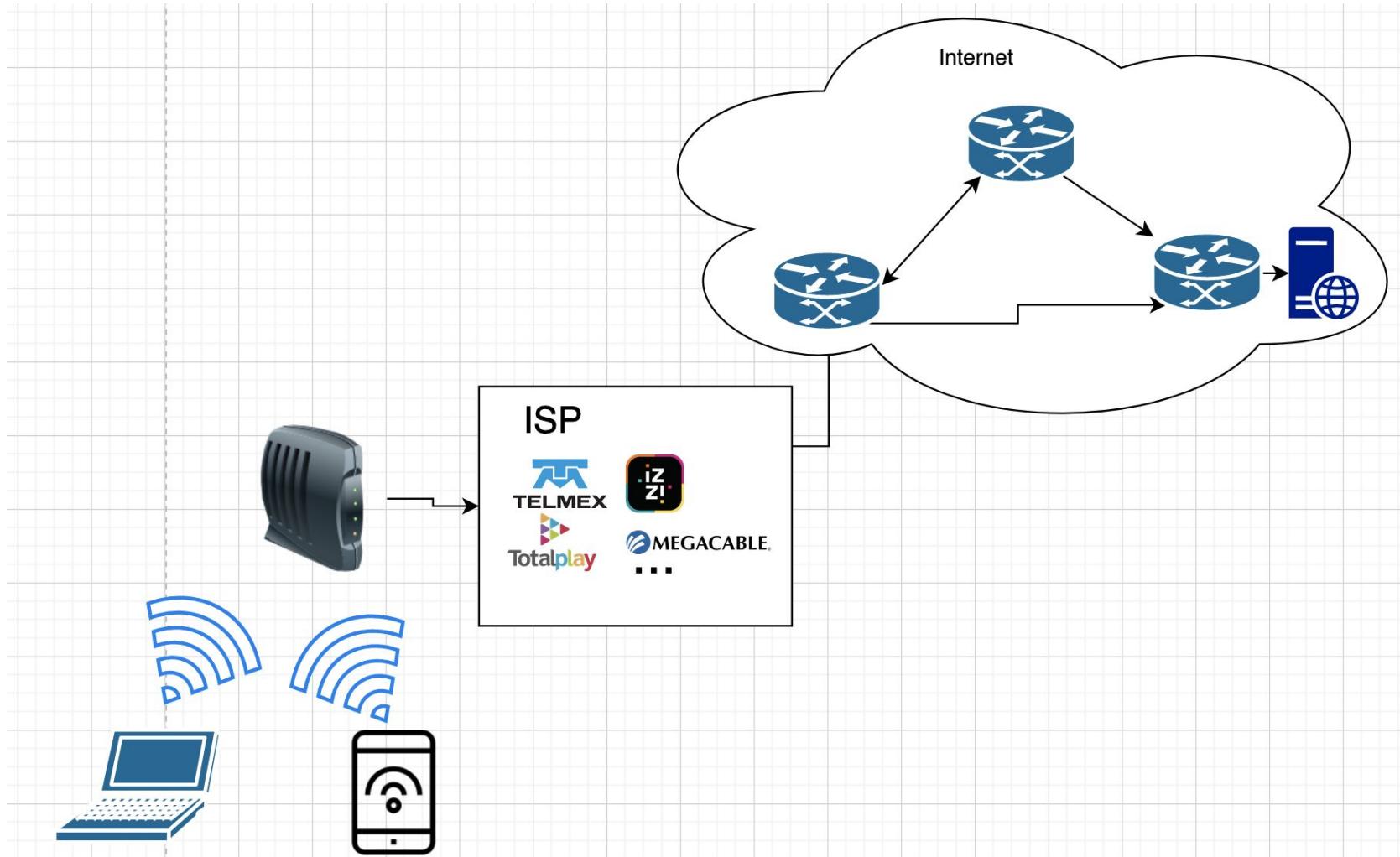
# Puerta de enlace(gateway)

Dispositivo que permite la comunicación entre dos redes distintas (red interna y red externa)





## ISP





## Capa de Red

- Ejemplos de componentes de hardware de la capa de Red
  - Router (enrutadores)
  - Layer 3 switches (switch de capa 3)
- Ejemplos de protocolos en la capa de Red
  - IP (*Internet Protocol*)
  - ICMP (*Internet Control Message Protocol*)





## Routing (ruteo)

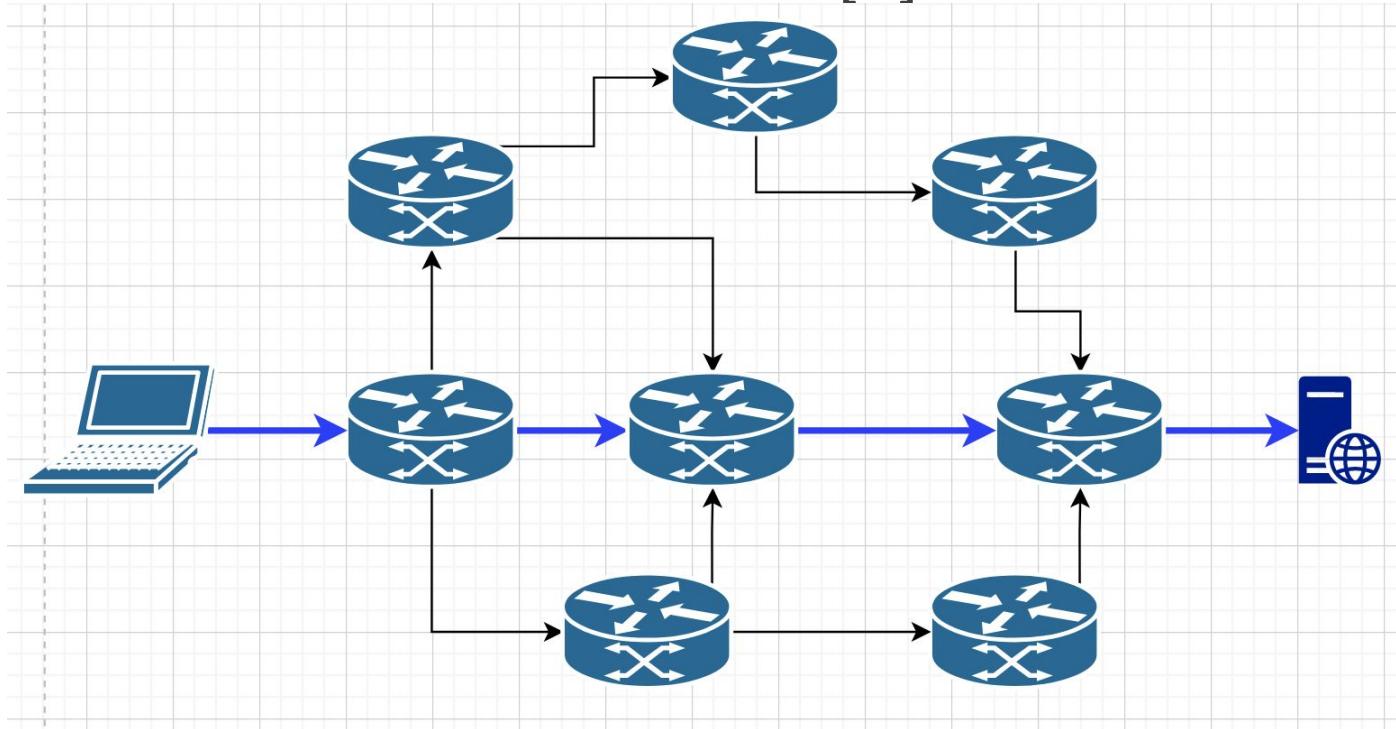
---

- Para comunicar a los *host* que se encuentren en diferentes redes es necesario establecer rutas entre dichas redes.
- Esta ruta es un camino lógico que puede estar preestablecido de manera estática, o puede ser generado de manera dinámica en el momento de la comunicación.



## Routing (ruteo)

- Gracias al *routing* es posible establecer fácilmente rutas entre diferentes redes, desde redes pequeñas hasta redes de gran tamaño como Internet. [3]





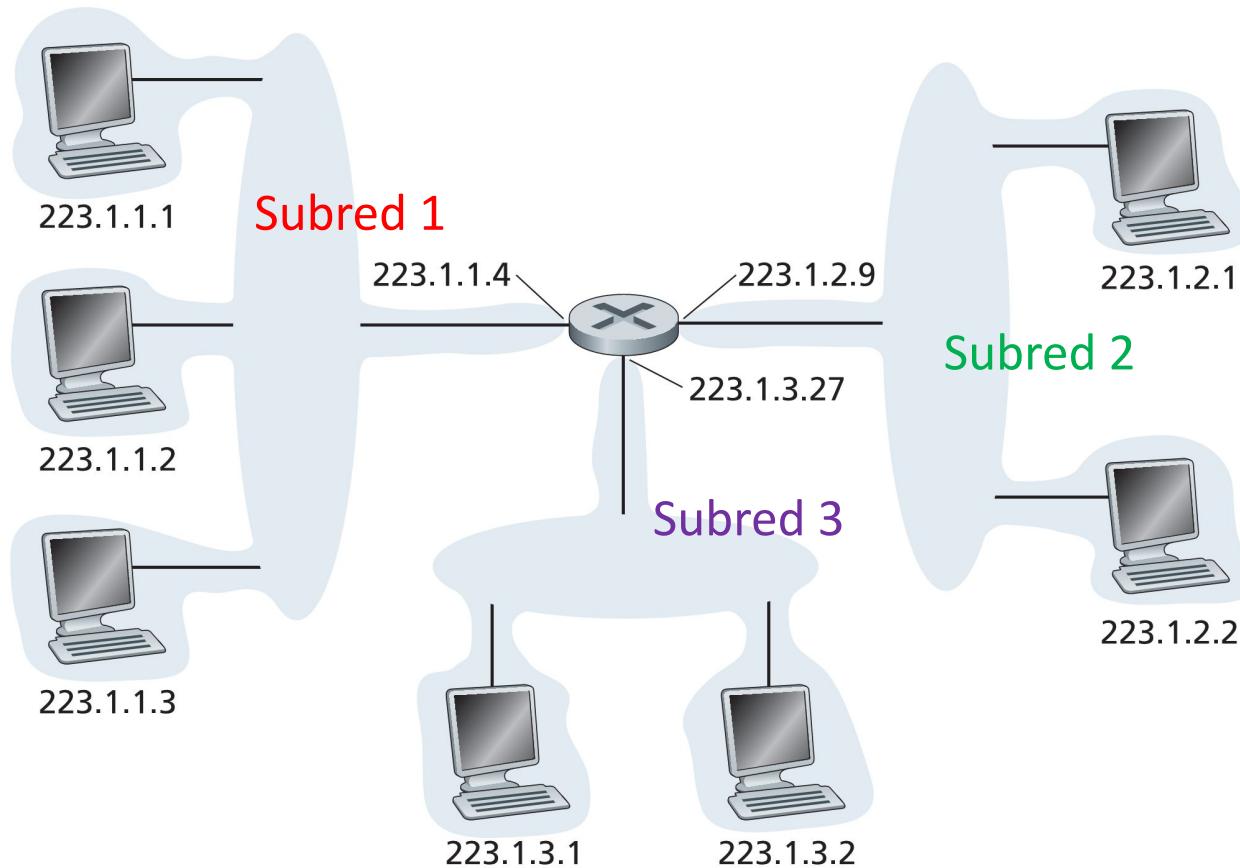
## Tarea

---

Elaborar un diagrama de red casera, las especificaciones se encuentran en moodle



## Subredes



Tres subredes diferentes conectadas entre sí con un Router [1]



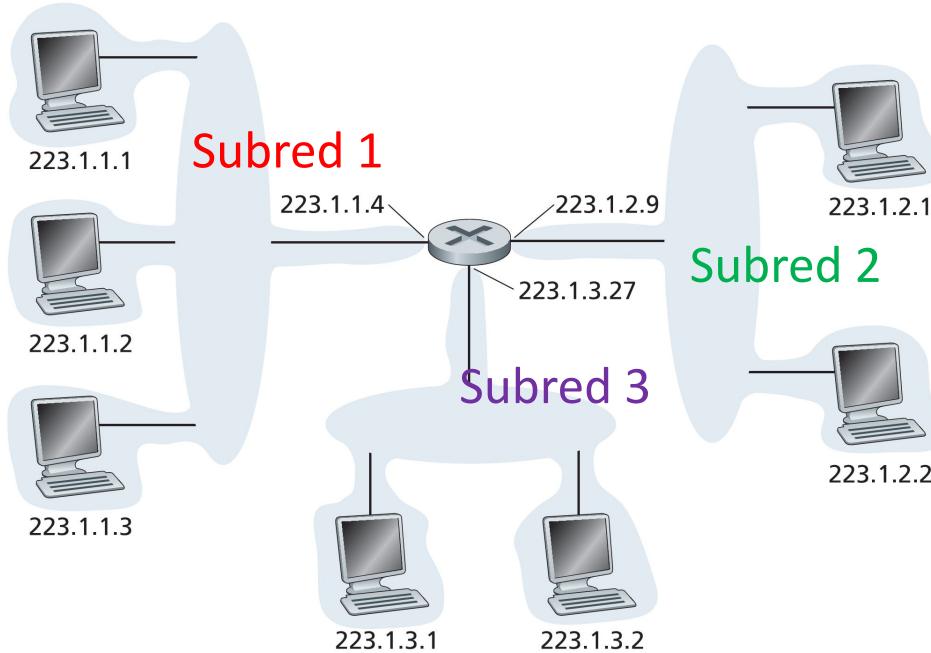
## Subredes

---

- En la imagen anterior se observan tres diferentes subredes conectadas entre sí por un *router*.
- Como se tienen tres subredes, entonces se tienen tres diferentes conjuntos de direcciones IP.
- Las direcciones IP de las tres subredes se encuentran en el rango de direcciones IP de la Clase C.
- A cada *host* de cada subred se le asigna una dirección IP perteneciente al conjunto de direcciones IP para esa subred.



## Subredes



### Clase C

192.0.0.0 - 223.255.255.255

#### Subred 1

223.1.1.0 –  
223.1.1.255

#### Subred 2

223.1.2.0 –  
223.1.2.255

#### Subred 3

223.1.3.0 –  
223.1.3.255



## Subredes

- Siguiendo con el ejemplo de las tres subredes, cada subred pertenece a la Clase C, por lo tanto se asigna la Máscara de red o *Netmask* 255.255.255.0
- Para determinar la pertenencia de la dirección IP de un *host* a una subred es a través de la operación AND ( $\otimes$ ) bit a bit entre la dirección IP del *host* y la Máscara de red.

$$\begin{array}{r} \text{IP del } host \\ \otimes \\ \text{Máscara de red} \\ \hline \text{IP de la subred} \end{array}$$



## Subredes

- Determinar la dirección IP de subred para el *host* con dirección IP 223.1.2.2 y máscara de red 255.255.255.0

$$\begin{array}{r} \text{IP del host } 223.1.2.2 \\ \otimes \\ \text{Máscara de red } 255.255.255.0 \\ \hline \text{IP de la subred } 223.1.2.0 \end{array}$$

$$\begin{array}{r} \text{11011111 00000001 00000010 00000010} \\ \otimes \\ \text{11111111 11111111 11111111 00000000} \\ \hline \text{11011111 00000001 00000010 00000000} \end{array}$$



## Subredes

- Parte de la dirección IP de un *host* corresponde a la identificación de red [3], y está determinada por la máscara de red.

⊗	IP del host	223.1.2.2	Porción para la subred
	Máscara de red	255.255.255.0	Porción para los <i>host</i>
<hr/>			
	IP de la subred	223.1.2.0	

⊗	11011111 00000001 00000010 00000010
	11111111 11111111 11111111 00000000
<hr/>	
	11011111 00000001 00000010 00000000



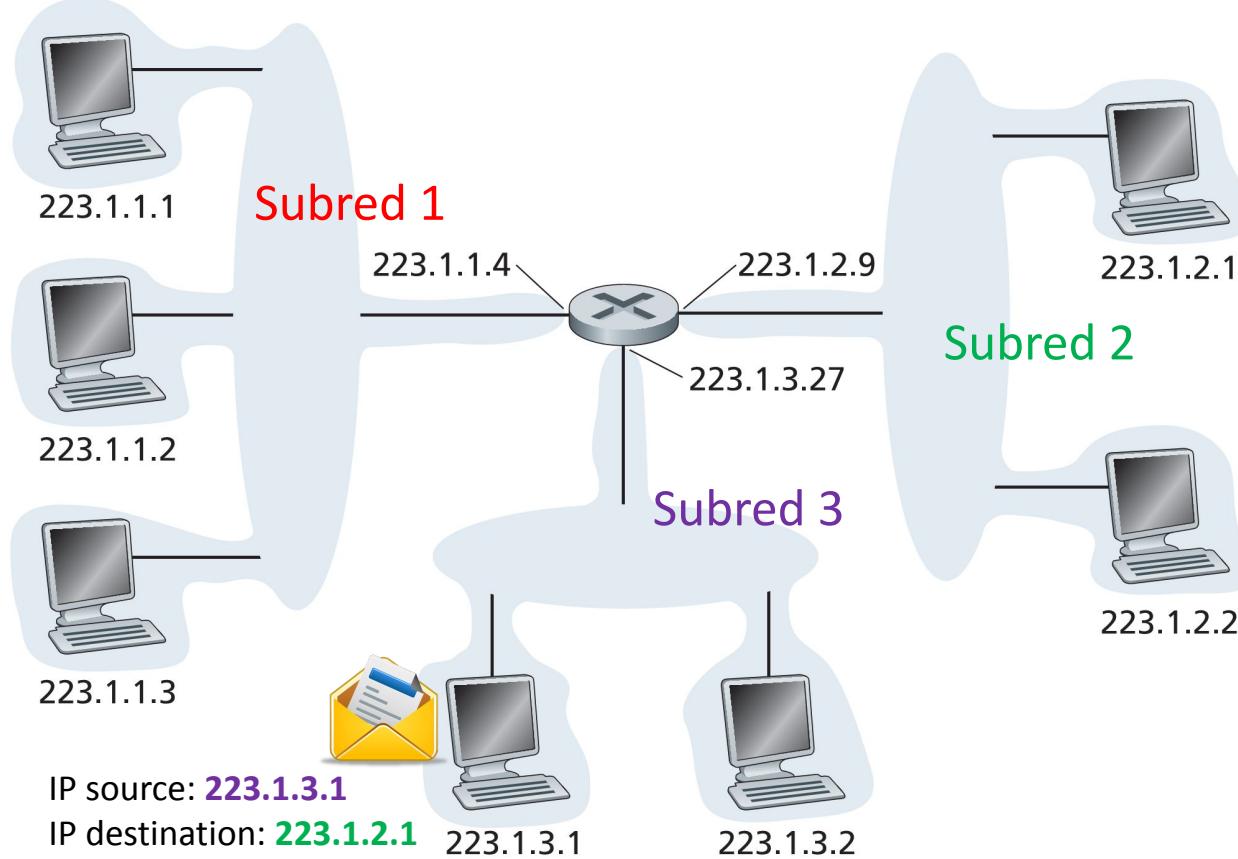
## Envío de mensajes entre subredes

---

- Para enviar un mensaje de un *host* a otro *host*, se usa la dirección IP del origen destino, similar a una dirección postal o número de teléfono.
- Si el *host* destino tiene una dirección IP que no pertenece a la misma subred del *host* origen, será necesario dirigir este paquete hacia el Router para que éste pueda dirigirlo o encaminarlo a su destino.



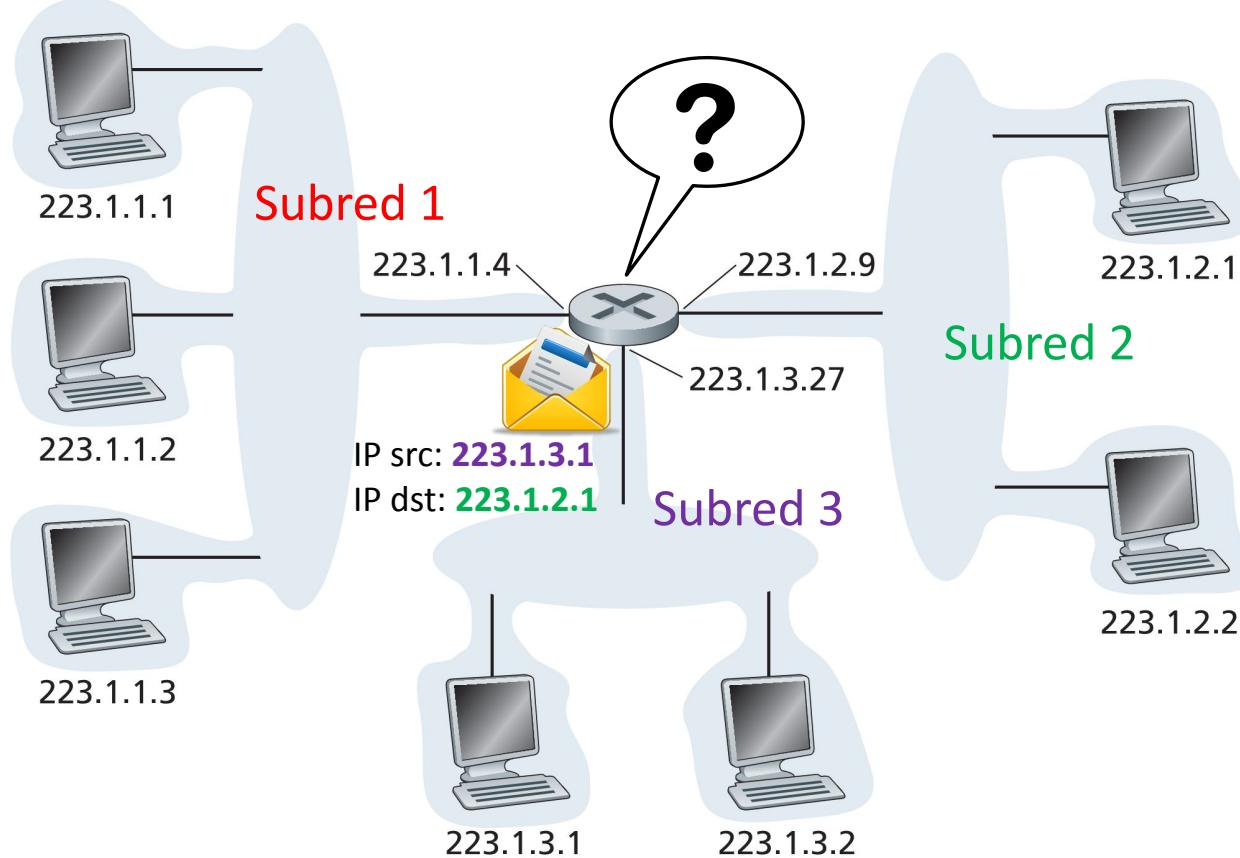
# Envío de mensajes entre subredes



Tres subredes diferentes conectadas entre sí con un Router [1]



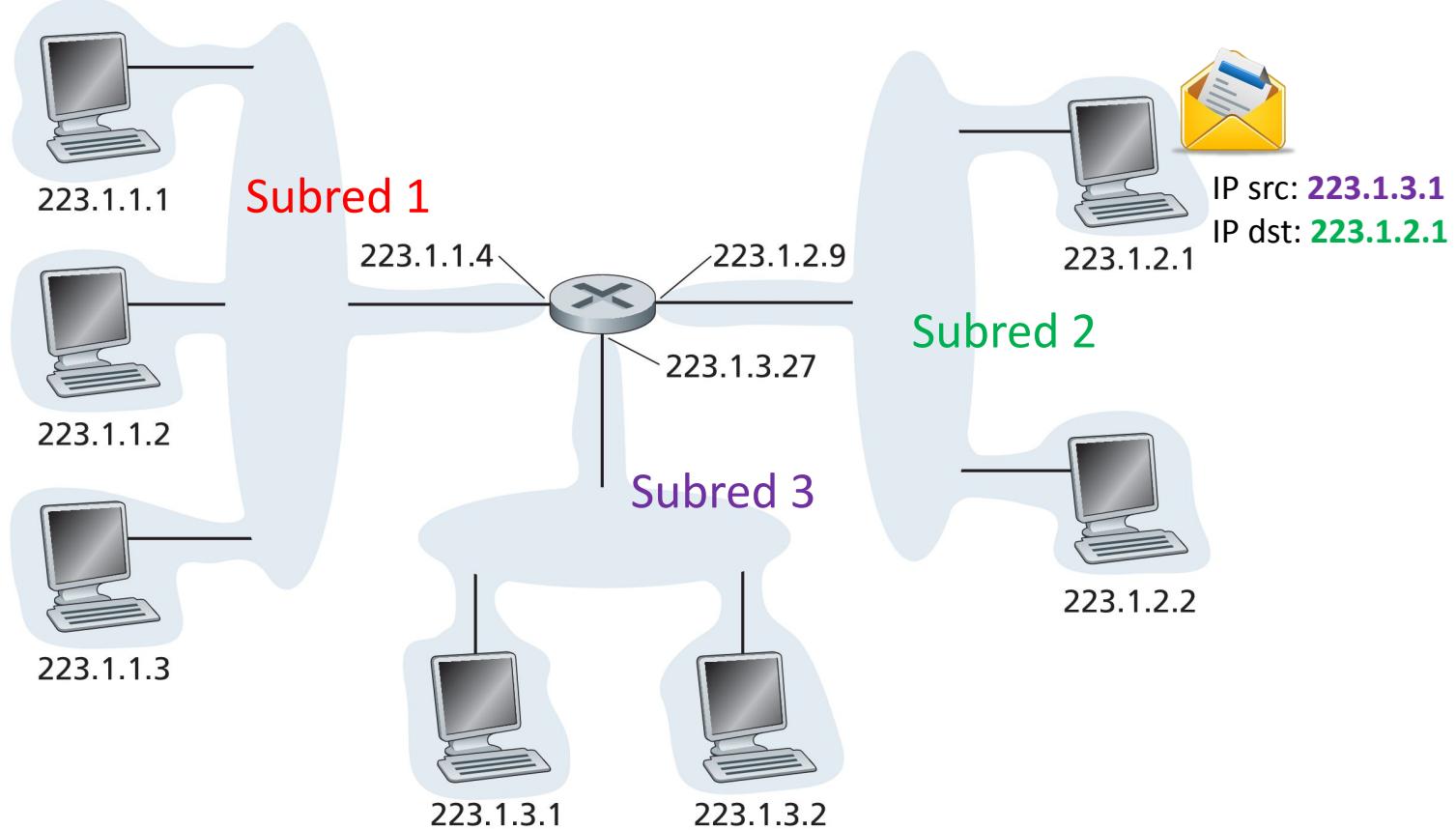
# Envío de mensajes entre subredes



Tres subredes diferentes conectadas entre sí con un Router [1]



# Envío de mensajes entre subredes



Tres subredes diferentes conectadas entre sí con un Router [1]



# Pila de protocolos de Internet (5 capas) [1]



datos  
(data, payload)

segmento  
(segment)

paquete  
(packet)

trama  
(frame)

bit



- Antes de continuar con los conceptos de la capa de Transporte, y una vez revisados los conceptos de la capa de Red, es momento de estudiar al protocolo ARP de la capa de Enlace, que relaciona las direcciones IP con las direcciones MAC.



## Address Resolution Protocol (ARP)

---

- La dirección IP es una dirección de software que se puede cambiar.
- La dirección MAC no puede modificarse en una tarjeta de red (NIC), sin embargo, puede variarse por software.
- Cuando la capa de Red o IP se comunica con la capa de enlace, se hace una asociación de direcciones. La capa de Red trata direcciones IP y la capa de Enlace direcciones MAC.



## Address Resolution Protocol (ARP)

---

- El protocolo de resolución de direcciones (ARP) es el responsable de hacer la asociación entre la dirección IP y la dirección MAC.
- El *host* que necesita enviar el paquete a la capa de Enlace, emitirá una solicitud al protocolo de resolución de direcciones para determinar la dirección MAC del destinatario.
- Una vez realizado esto, se construirá una trama o *frame* con la dirección MAC destino y origen.



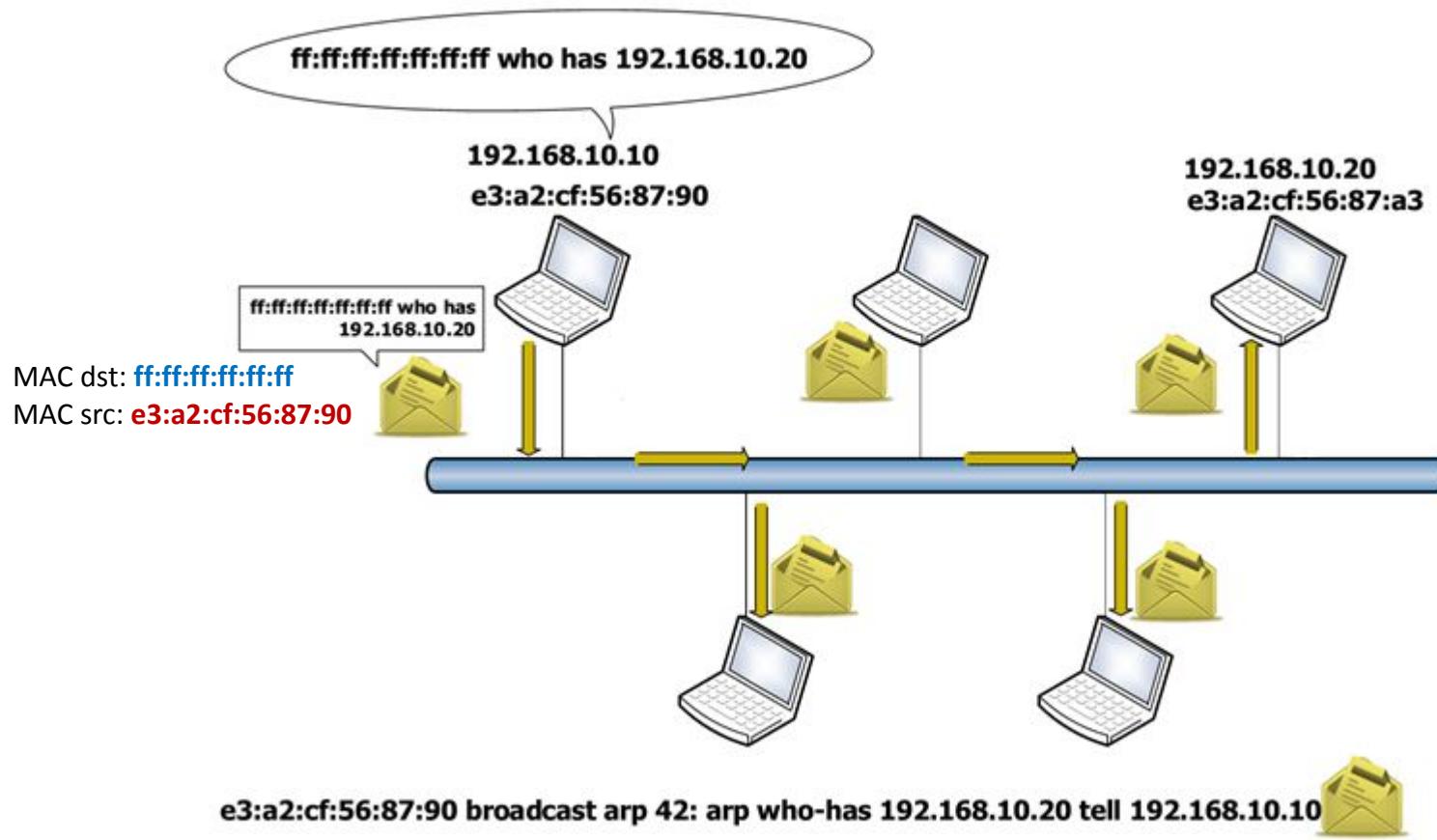
## Address Resolution Protocol (ARP)

---

- La dirección MAC se utiliza por los *host* encontrados en una misma subred local o LAN, la dirección IP de todos los *host* en la subred deben pertenecer a la misma dirección IP de red.
- Si necesita enviar tráfico de un equipo a otro en un segmento físico, tendrá que *rutear* utilizando la capa de Red, antes de entregarlo a la capa de Enlace.
- Esto significa que ARP no es un protocolo *ruteable*, ya que resuelve las direcciones MAC para los segmentos locales únicamente.



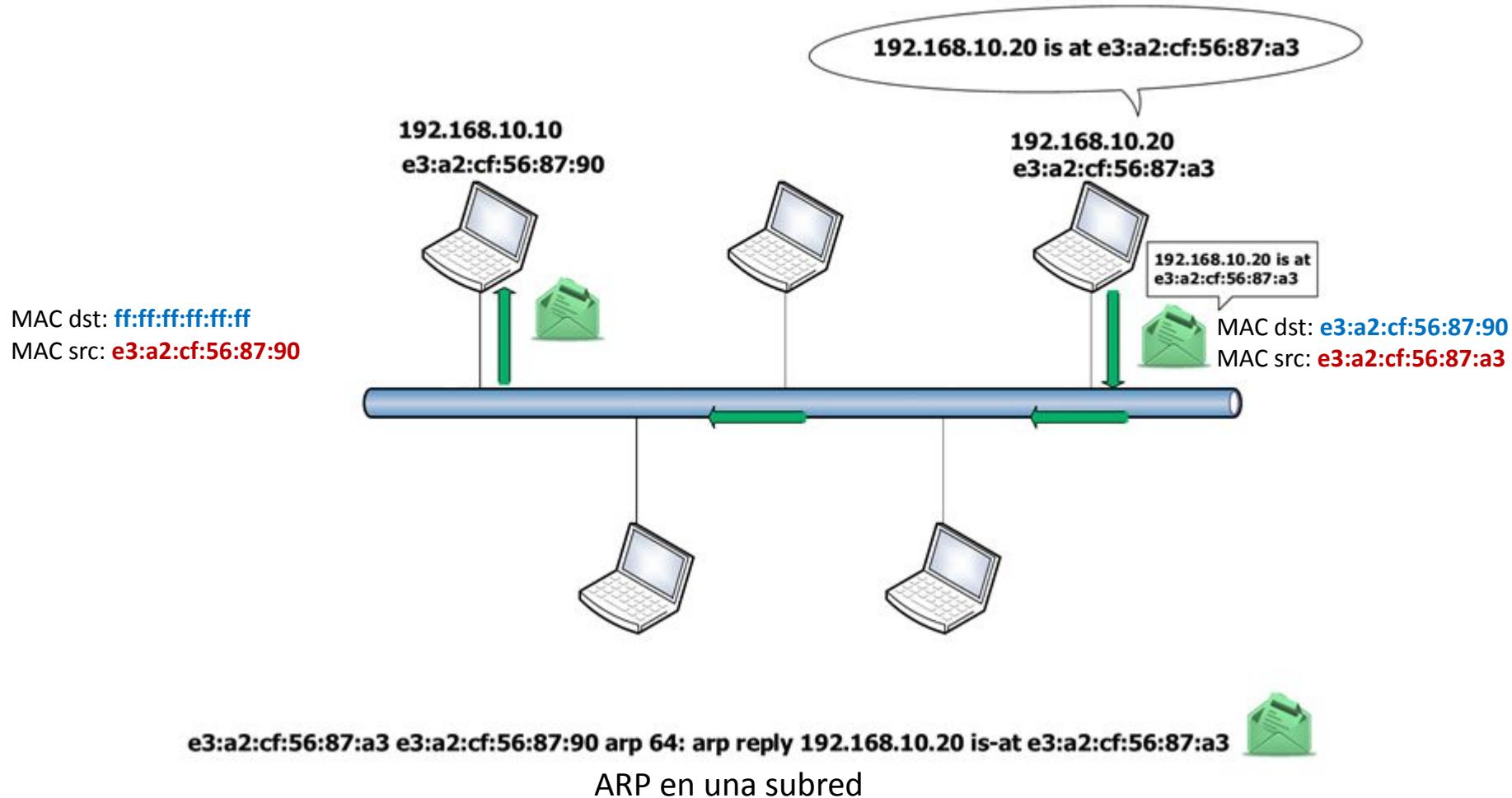
# Address Resolution Protocol (ARP)



ARP en una subred



# Address Resolution Protocol (ARP)





## Address Resolution Protocol (ARP)

---

- El host con la dirección IP 192.168.10.10, desea iniciar una comunicación con el host que está en el mismo segmento de red con la dirección IP 192.168.10.20.
- Debido a que están en el mismo segmento, se debe utilizar la capa de Enlace para enviar una trama del origen al destino. El equipo 192.168.10.10 no conoce la dirección MAC de 192.168.10.20.



## Address Resolution Protocol (ARP)

---

- Por este motivo, envía un mensaje de broadcast ARP que produce el envío de la trama a todas las direcciones MAC en el segmento de la subred local mediante una MAC destino ff:ff:ff:ff:ff:ff.
- El mensaje de broadcast ARP pregunta a cualquier equipo si responde a la dirección IP 192.168.10.20.



## Address Resolution Protocol (ARP)

---

- Cuando la trama de broadcast es leída por el host con la dirección IP 192.168.10.20, responderá con una trama de tipo unicast, es decir de *host* a *host*, a la dirección MAC de 192.168.10.10 ( e3:a2:cf:56:87:90 ). Éste conoce la dirección MAC de 192.168.10.10 porque fue incluida en el mensaje de broadcast ARP.
- Ahora que 192.168.10.10 sabe que la dirección MAC asociada con 192.168.10.20 es e3:a2:cf:56:87:a3, puede usarla en el encabezado de la trama y colocarla en la capa de Enlace, para iniciar una comunicación. De esta forma, los dos equipos se comunicarán de la misma manera.



# ARP table - Windows

```
Administrador: Símbolo del sistema
C:\WINDOWS\system32>arp -a

Interfaz: 192.168.1.68 --- 0x1e
          Dirección de Internet      Dirección física      Tipo
 192.168.1.65            e8-4e-84-d4-XXXXXXXXXX    dinámico
 192.168.1.71            00-27-0e-01-XXXXXXXXXX    dinámico
 192.168.1.254           a4-ba-76-51-XXXXXXXXXX    dinámico
 192.168.1.255           ff-ff-ff-ff-ff-ff    estático
 224.0.0.22              01-00-5e-00-00-16    estático
 224.0.0.251             01-00-5e-00-00-fb    estático
 224.0.0.252             01-00-5e-00-00-fc    estático
 224.0.1.60              01-00-5e-00-01-3c    estático
 239.255.255.250         01-00-5e-7f-ff-fa    estático
 255.255.255.255         ff-ff-ff-ff-ff-ff    estático
```



# ARP table - Linux

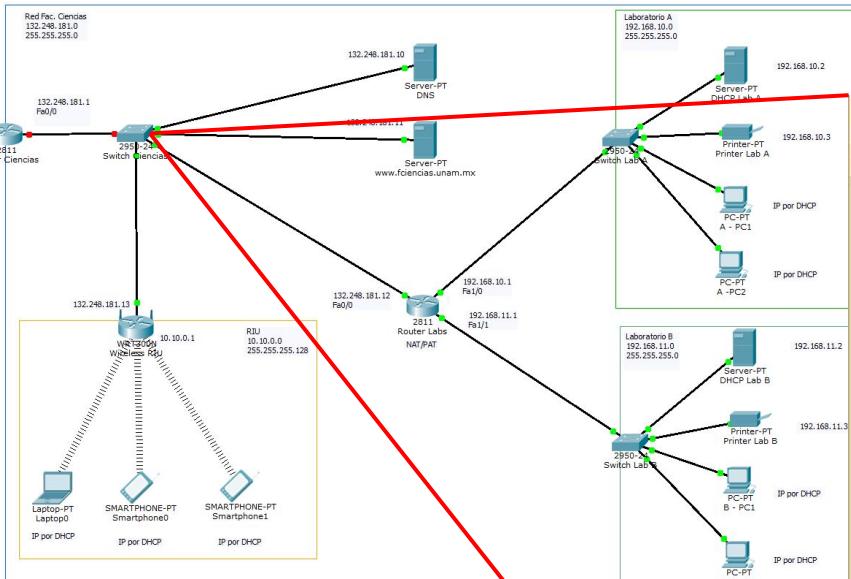
```
Terminal - curso@lab: ~
Archivo Editar Ver Terminal Pestañas Ayuda
root@lab:~# arp -n
Address          HWtype  HWaddress          Flags Mask Iface
192.168.1.254   ether    a4:ba:76:51:[REDACTED] C      eth1
192.168.1.71    ether    (incomplete)      C      eth1
192.168.1.65    ether    e8:4e:84:d4:[REDACTED] C      eth1
```

C – registro ARP completo

M – registro permanente



# MAC Address Table - switch



Switch Ciencias

Physical Config CLI

## IOS Command Line Interface

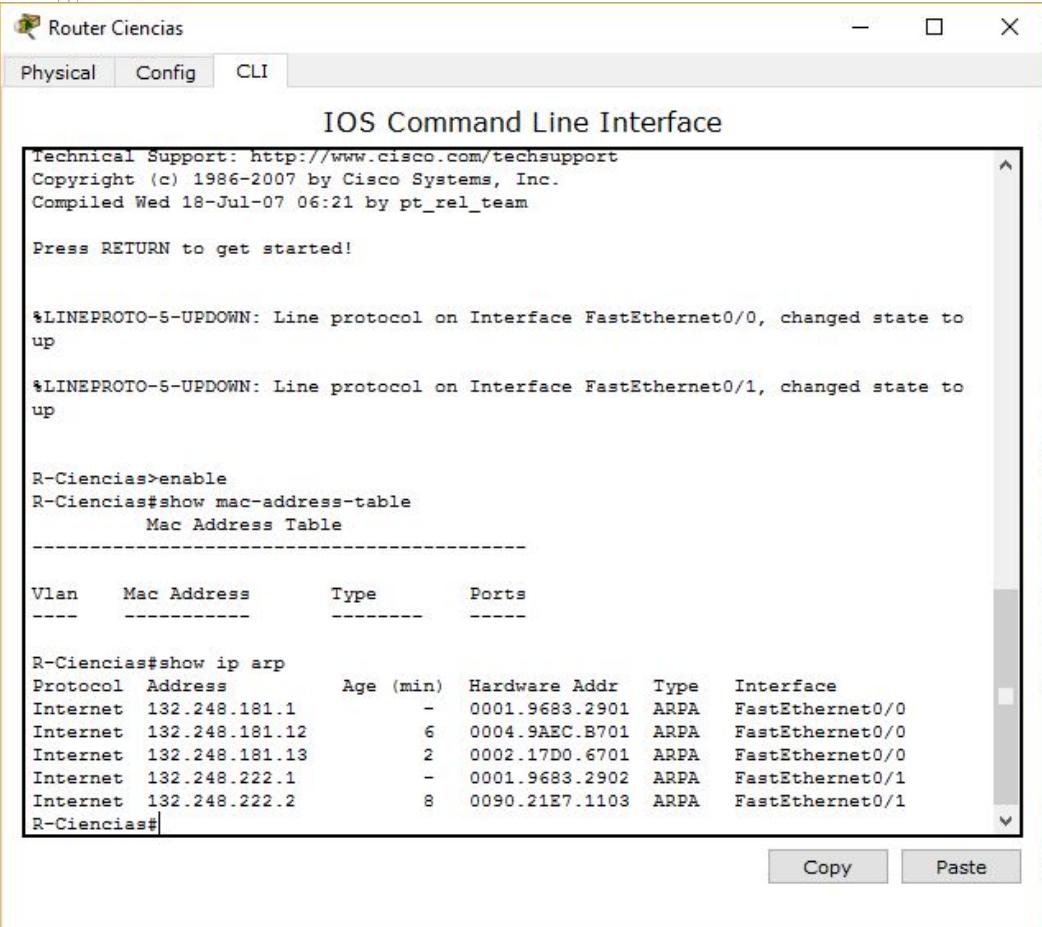
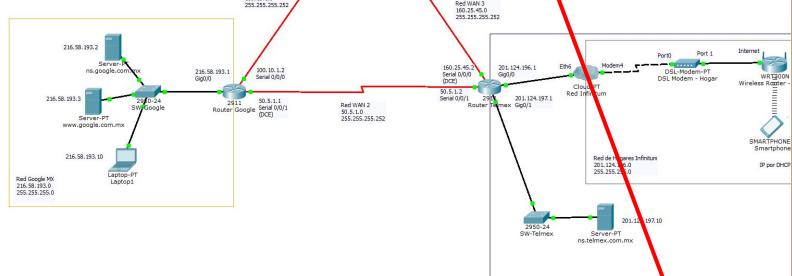
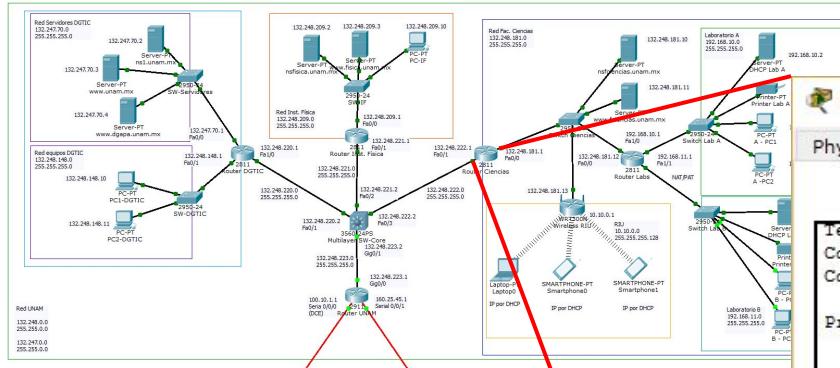
```
Switch#enable
Switch#show mac-address-table
^
% Invalid input detected at '^' marker.

Switch#show mac-address-table
  Mac Address Table
-----
  Vlan      Mac Address          Type      Ports
  ----      -----              -----      -----
    1        0002.17d0.6701    DYNAMIC   Fa0/5
    1        0004.9aec.b701    DYNAMIC   Fa0/4
    1        0030.f24c.6439    DYNAMIC   Fa0/2
    1        00e0.a306.6237    DYNAMIC   Fa0/3
```

Copy Paste



# ARP table - router





## Capa de Transporte

---

- Provee el servicio de transferencia de datos entre los *host* de manera transparente, confiable y eficiente. [3]
- Operan los protocolos encargados de establecer las comunicaciones de punto a punto (*end to end*). [3]
- Da confiabilidad en la conexión punto a punto, y permite el aprovechamiento de los recursos de red disponibles. [3]



## Multiplexación

---

- La multiplexación es el proceso mediante el cual un mismo *host* puede establecer diferentes comunicaciones con otros *host* de manera simultánea sin entorpecer el flujo de información de las conexiones. Esto se logra con el concepto de puertos lógicos. [3]
- Un puerto es un canal de comunicación. Se puede tener una misma dirección IP en un *host*, pero puede estar comunicándose con distintos host a la vez, a través de diferentes puertos. [3]



## Capa de transporte - Multiplexación

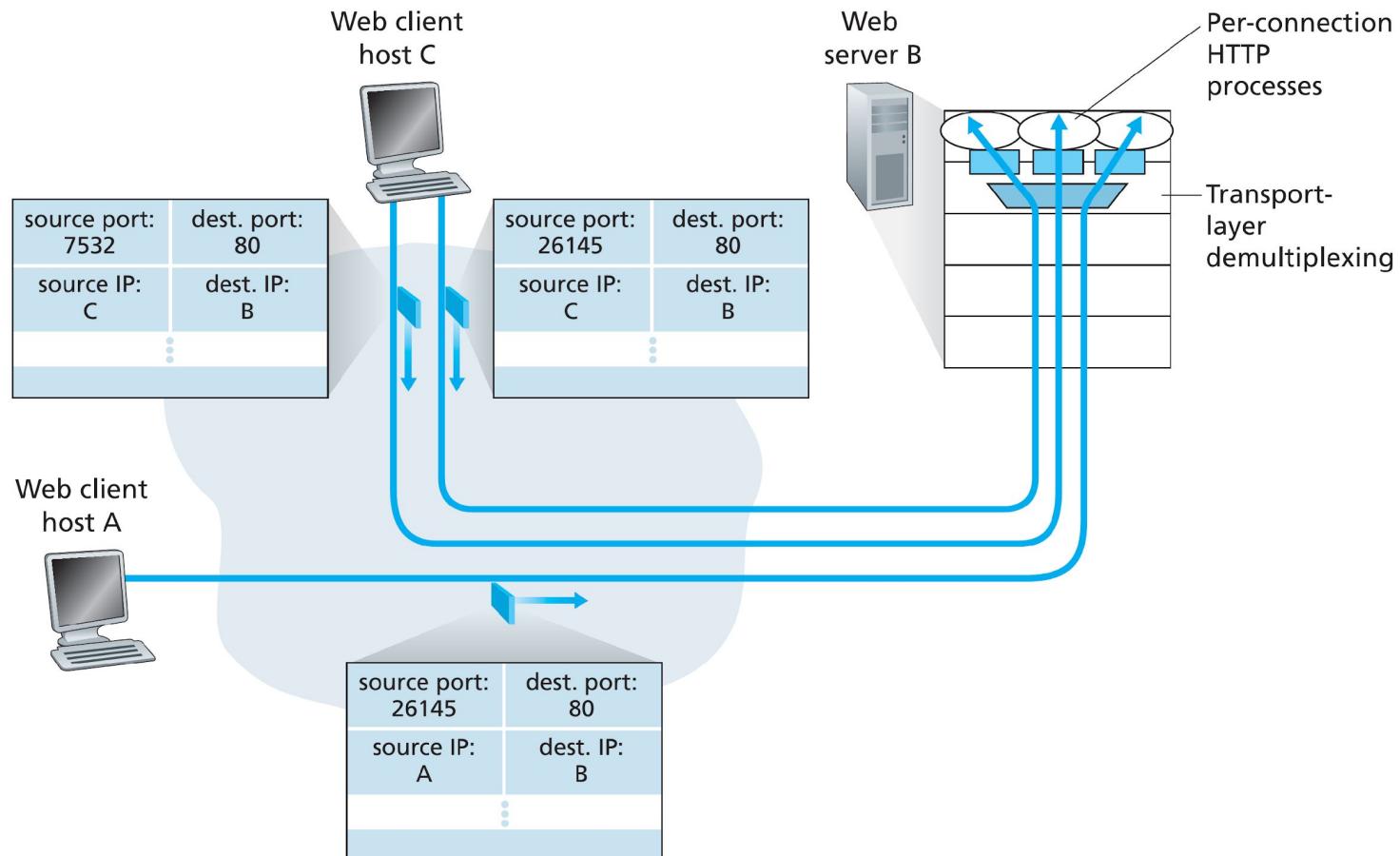
---

- Dos diferentes servicios no pueden hacer uso del mismo puerto de forma simultánea. [3]
- Si un servicio se ha iniciado utilizando un puerto específico, este puerto no podrá ser utilizado por otro proceso hasta que el servicio inicial se haya cerrado.
- Los puertos están representados por un número de 16 bits.

$$PORTS = \{port \mid 0 \leq port < 2^{16}, port \in \mathbb{Z}\}$$



## Capa de transporte - Multiplexación



Dos clientes usando el mismo puerto destino (80) para comunicarse con el mismo servidor Web. [1]



## Capa de transporte - Multiplexación

- De acuerdo a la IANA existen tres rangos de puertos.

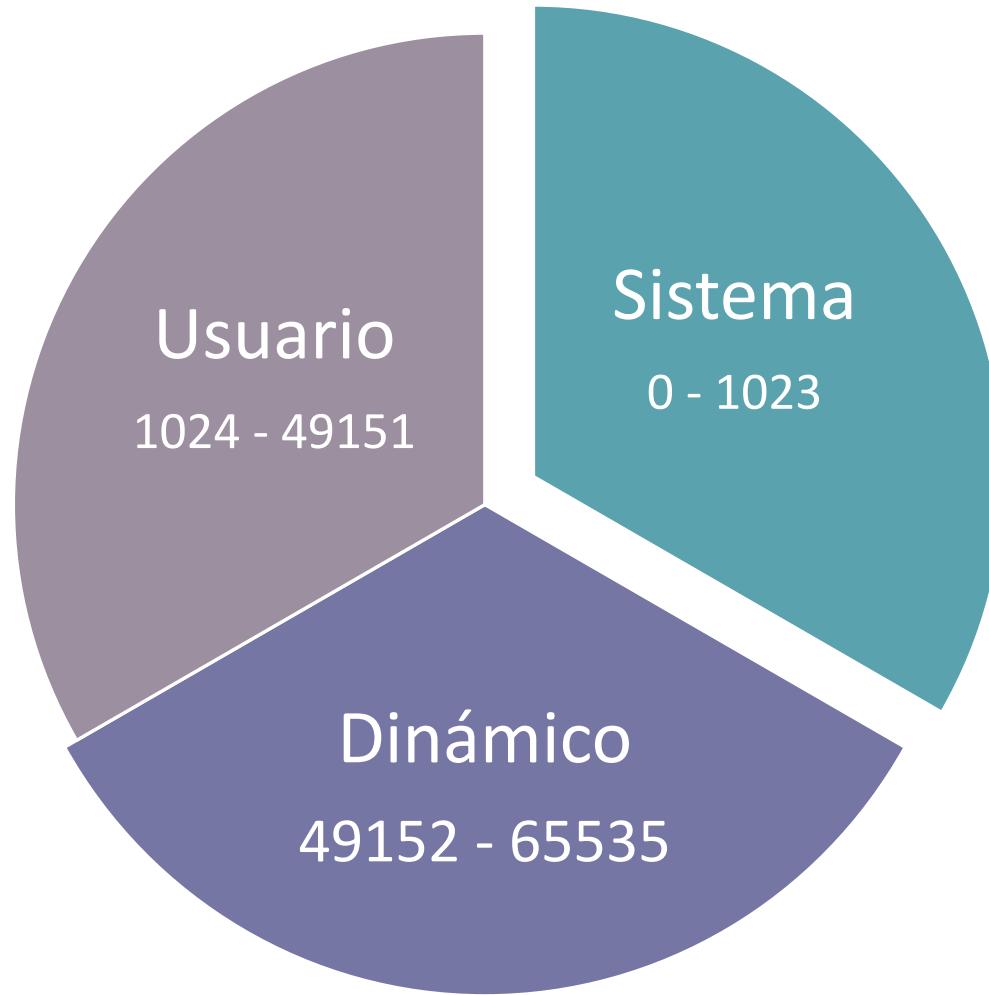
Rango	Categoría
0 - 1023	Puertos de sistema
1024 - 49151	Puertos de usuario
49152 - 65535	Puertos dinámicos o privados

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>



# Multiplexación

Puertos





## Multiplexación

---

- 0 – 1023, Puertos de sistema. También llamados “bien conocidos” (*well-known ports*) son utilizados principalmente por procesos del sistema operativo (SO) y los servicios más comunes de redes. Generalmente el SO exige credenciales administrativas para poder abrir uno de estos puertos. [3]
- 1024 – 49151, Puertos de usuario. También llamados “puertos registrados” (*registered ports*), fueron registrados ante la IANA por fabricantes de software. Un usuario de un SO puede abrir un puerto en este rango sin la necesidad de credenciales administrativas. [3]



## Multiplexación

---

- 49152 – 65535, Puertos dinámicos o privados. También llamados “puertos efímeros” (*ephemeral ports*), son utilizados por el SO que inicia una conexión, llamado cliente, al realizar una conexión hacia un equipo remoto. [3]



# Multiplexación

- Todas las comunicaciones deben poseer un puerto origen y puerto destino. [3]
- Ejemplos de servicios y puertos:

Servicio de la capa de aplicación	Puerto
HTTP ( <i>Hypertext Transfer Protocol</i> )	80
HTTPS ( <i>Hypertext Transfer Protocol Secure</i> )	443
SMTP ( <i>Simple Mail Transfer Protocol</i> )	25
MySQL	3306
Postgresql	5432
SQL Server	1433



## Orientado a Conexión

---

- Establece un camino lógico o virtual entre dos *host*, es confiable, resistente a las pérdidas y duplicación de información, la información es entregada a la capa de Aplicación en el mismo orden en el que se envía.
- El protocolo más común orientado a conexión es TCP (*Transmission Control Protocol*).



## No orientado a conexión

---

- No es confiable en la entrega de los datos, puede haber pérdidas y duplicación de información, y puede llegar en distinto orden del que se envía.
- La comunicación es más rápida respecto al esquema Orientado a conexión.
- El protocolo más común orientado a conexión es UDP (*User Datagram Protocol*).



# Conexiones TCP de un cliente en Windows

```
Administrator: Símbolo del sistema
C:\WINDOWS\system32>netstat -nabo -p tcp

Conexiones activas

  TCP    192.168.1.68:53646      149.154.175.50:443      ESTABLISHED      9476
  [Telegram.exe]
  TCP    192.168.1.68:53662      23.92.108.138:4070      ESTABLISHED      12844
  [Spotify.exe]
  TCP    192.168.1.68:53664      40.77.224.254:443      ESTABLISHED      580
  BITS
  [svchost.exe]
  TCP    192.168.1.68:53685      52.165.147.104:443      ESTABLISHED      11896
  [Skype.exe]
  TCP    192.168.1.68:53687      65.55.252.167:443      ESTABLISHED      11896
  [Skype.exe]
  TCP    192.168.1.68:53689      91.190.216.55:12350      ESTABLISHED      11896
  [Skype.exe]
  TCP    192.168.1.68:53704      157.55.56.155:40012      ESTABLISHED      11896
  [Skype.exe]
  TCP    192.168.1.68:53725      158.85.224.175:443      ESTABLISHED      3892
  [WhatsApp.exe]
  TCP    192.168.1.68:53729      104.79.181.53:443      CLOSE_WAIT       7200
  [SkypeBrowserHost.exe]
  TCP    192.168.1.68:53730      104.79.181.53:443      CLOSE_WAIT       7200
  [SkypeBrowserHost.exe]
  TCP    192.168.1.68:53760      52.200.41.11:443      ESTABLISHED      10056
  [Mattermost.exe]
  TCP    192.168.1.68:53784      104.154.164.197:443      ESTABLISHED      4688
  [firefox.exe]
  TCP    192.168.1.68:54080      65.52.108.210:443      ESTABLISHED      12428
  [Explorer.EXE]
  TCP    192.168.1.68:55666      108.160.172.204:443      CLOSE_WAIT       2888
  [Dropbox.exe]
```

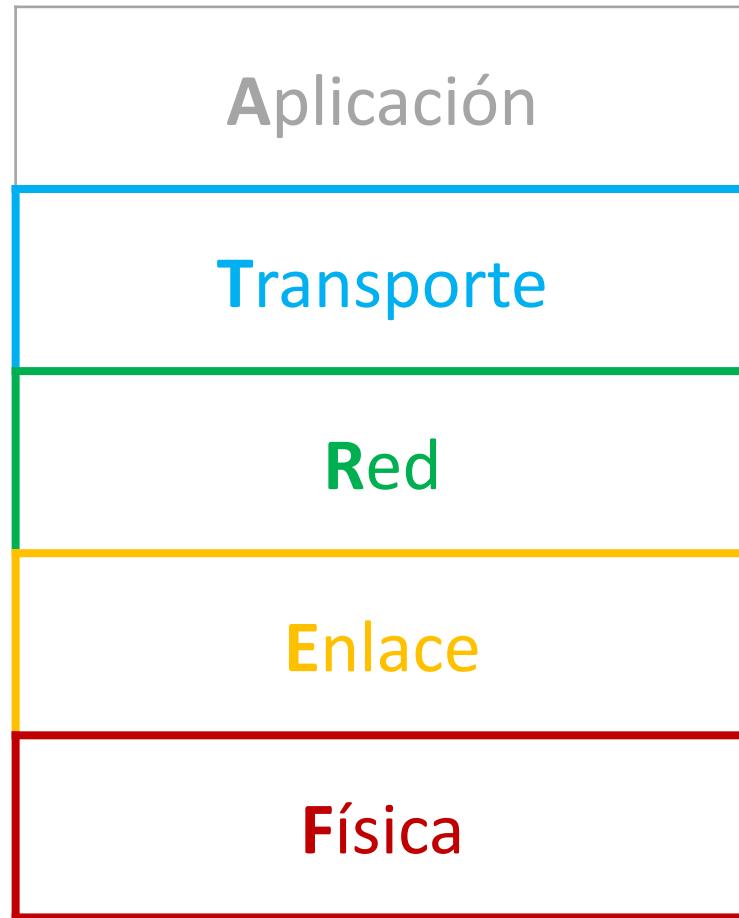


# Conexiones TCP de un cliente en Linux

```
Terminal - pauloc@debian: ~
Archivo Editar Ver Terminal Pestañas Ayuda
root@debian:~# netstat -napt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 192.168.1.66:44968       216.58.194.68:80    TIME_WAIT   -
tcp      0      0 127.0.0.1:55981         127.0.0.1:953       TIME_WAIT   -
tcp      0      0 192.168.1.66:36615       216.58.193.46:80    TIME_WAIT   -
tcp      0      0 192.168.1.66:44964       216.58.194.68:80    ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:36614       216.58.193.46:80    ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:41399       216.58.194.68:443   ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:42967       52.73.137.110:443   ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:37833       216.58.193.46:443   ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:55101       104.79.161.113:443  ESTABLISHED 9218/x-www-browser
tcp    70888    0 192.168.1.66:55103       104.79.161.113:443  ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:55102       104.79.161.113:443  ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:55099       104.79.161.113:443  ESTABLISHED 9218/x-www-browser
tcp      0      0 192.168.1.66:42969       52.73.137.110:443   ESTABLISHED 9218/x-www-browser
```



# Pila de protocolos de Internet (5 capas) [1]



datos  
(data, payload)

segmento  
(segment)

paquete  
(packet)

trama  
(frame)

bit



## Capa de Aplicación

---

- En esta capa operan todos los servicios y aplicaciones que le brindan al usuario los medios necesarios para poder acceder a los diferentes recursos disponibles a lo largo de todas las redes accesibles en el entorno. [3]
- La capa de Aplicación no está representada por las aplicaciones en sí, sino por los protocolos que operan por debajo de dichas aplicaciones. [3]



## Capa de Aplicación

---

- Por ejemplo, para el servicio Web, el protocolo que trabaja en la capa de Aplicación es HTTP, mientras que el navegador es el agente que comanda las operaciones de dicho protocolo. [3]
- La capa de Aplicación no puede “sobrevivir” trabajando sola, requiere de la colaboración de todas las capas inferiores. [3]



## Capa de Aplicación

---

- Los componentes de las capas inferiores siempre interactúan en el proceso que involucra a la capa de Aplicación. [3]



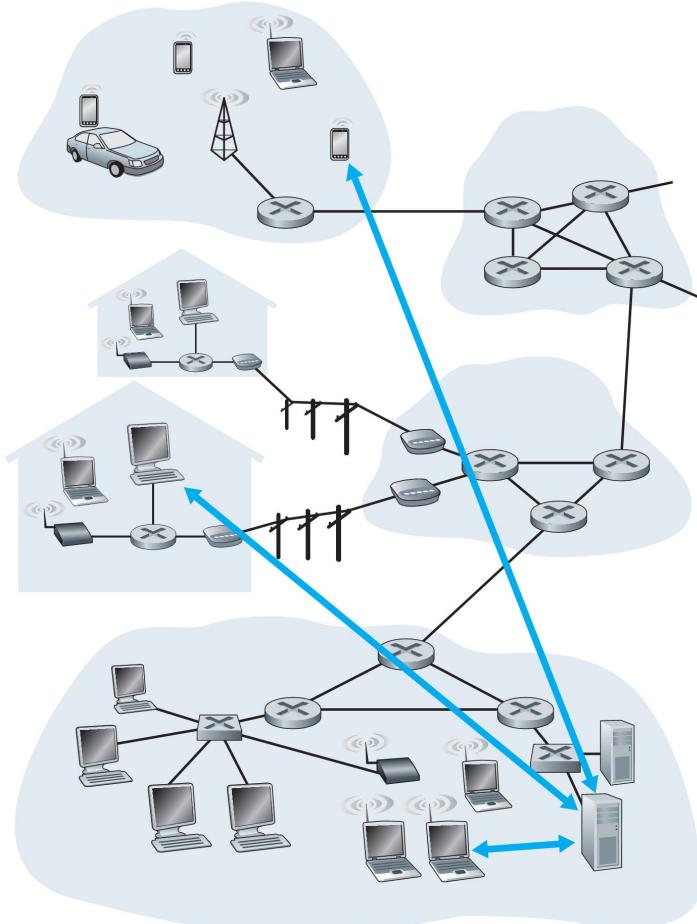
# Arquitecturas de la Capa de aplicación

---

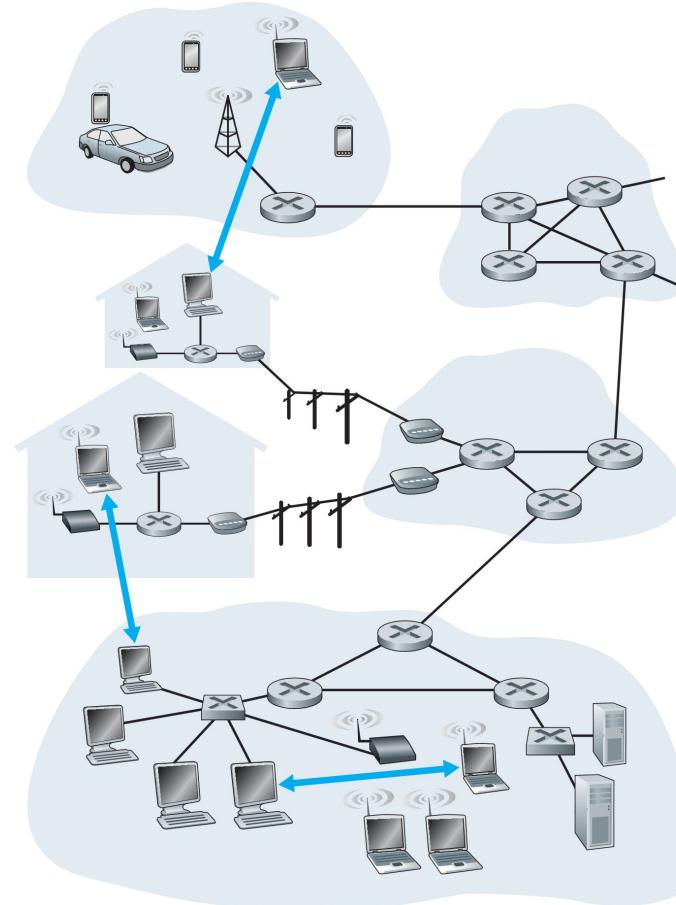
- En las aplicaciones existen dos arquitecturas predominantes [1]:
  - Cliente-servidor.
    - Web, FTP, Telnet, e-mail, SSH, DNS ...
  - De Igual-a-igual (*Peer-to-peer, P2P*)
    - BitTorrent, Skype ...



# Arquitecturas de la Capa de aplicación



Arquitectura cliente-servidor [1]



Arquitectura P2P [1]



# Arquitectura cliente-servidor

---

- **Servidor [1]**

- *Host* que recibe solicitudes de servicio de los clientes
- Tiene una dirección IP fija
- Siempre que tiene que estar “en línea” para atender las peticiones de los clientes
- Para gran cantidad de conexiones de los clientes se configuran varios *host* como servidor, para crear un “servidor virtual”, esto en un centro de datos (data center)

- **Cliente [1]**

- *Host* que envía solicitudes de un servicio al servidor
- Puede tener dirección IP fija o dinámica
- No tiene que estar “en línea” con un servidor permanentemente
- No se puede comunicar con otros clientes



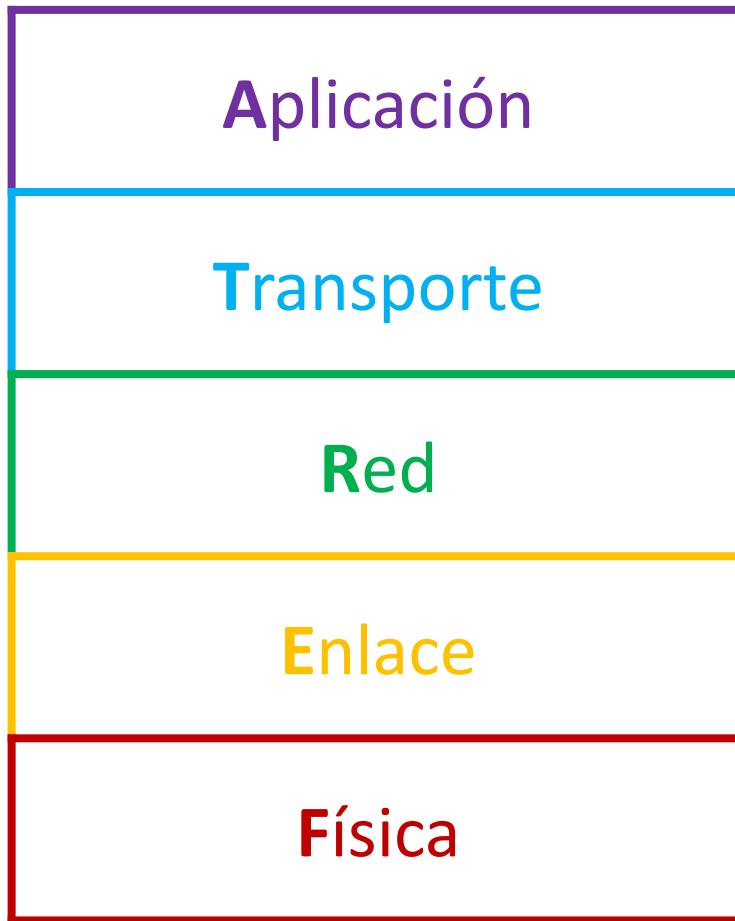
## Arquitectura P2P

---

- A cada host que actúa como punto de la conexión se le llama *peer*. [1]
- Los *peer* se comunican directamente entre sí, sin necesidad de pasar a través de un servidor dedicado. [1]
- Los *peer* solicitan el servicio a otros *peer*, y pueden a su vez proveer del servicio a otros *peer*. [1]
- Es autoescalable, pueden añadirse nuevos *peer* dando mayor capacidad al servicio, pero incrementando el uso de recursos. [1]



# Pila de protocolos de Internet (5 capas) [1]



datos  
(data, payload)

segmento  
(segment)

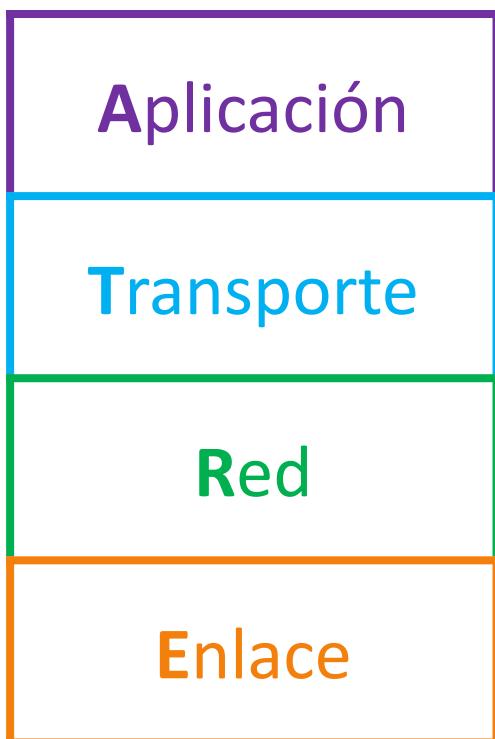
paquete  
(packet)

trama  
(frame)

bit



# Modelo TCP/IP



- Es el modelo de referencia utilizado en ARPANET. [2]
- Cuando se elaboró se pensó en que fuera una arquitectura flexible para aplicaciones con requerimientos diferentes. [2]
- Se conoce con este nombre debido a los dos protocolos que más se utilizan en él, TCP para la capa de Transporte e IP para la capa de Red. [2]



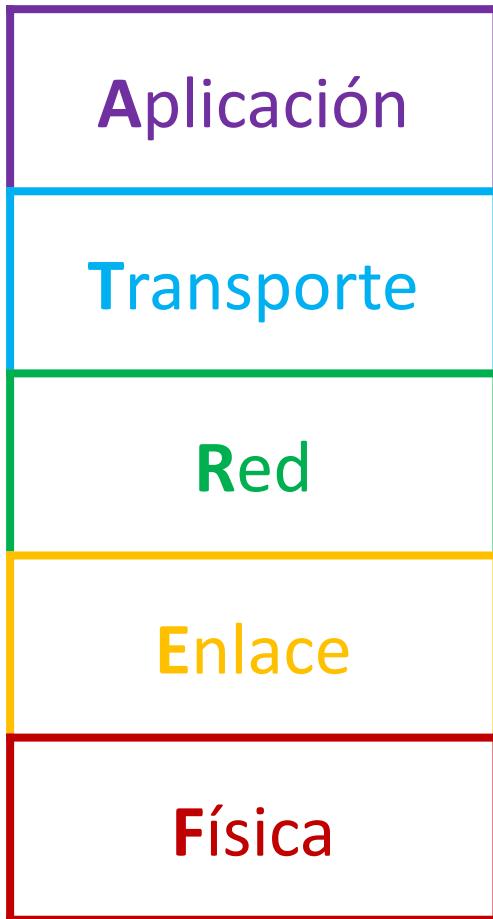
## Modelo OSI



- La ISO (*International Organization for Standardization*) propuso el modelo OSI (*Open Systems Interconnection*).
- La funcionalidad de las capas de nombre igual a la Pila de protocolos de Internet es muy similar en el modelo OSI. [1]
- La función de la capa de Presentación es proporcionar los servicios para interpretar los datos que se intercambian entre las aplicaciones. Por ejemplo, cifrado, compresión, convenciones específicas de alguna tecnología (la forma de tratar la información puede diferir de un *host* a otro). [1]
- La capa de Sesión permite la sincronización e intercambio de datos. Crea un esquema para recuperar datos a partir de un punto [1], es decir dada una sesión establecida entre dos *host*, puede reanudarla en caso de interrupción.



## Pila de protocolos de Internet (Modelo TCP/IP 5 capas)



- La Pila de Protocolos de Internet se conforma por 5 capas [1].
- Es el modelo que se estudiará en este curso.

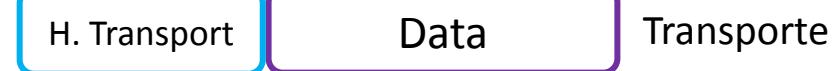


## Encapsulado de protocolos

Encabezado de Transporte  
*Transport header information*

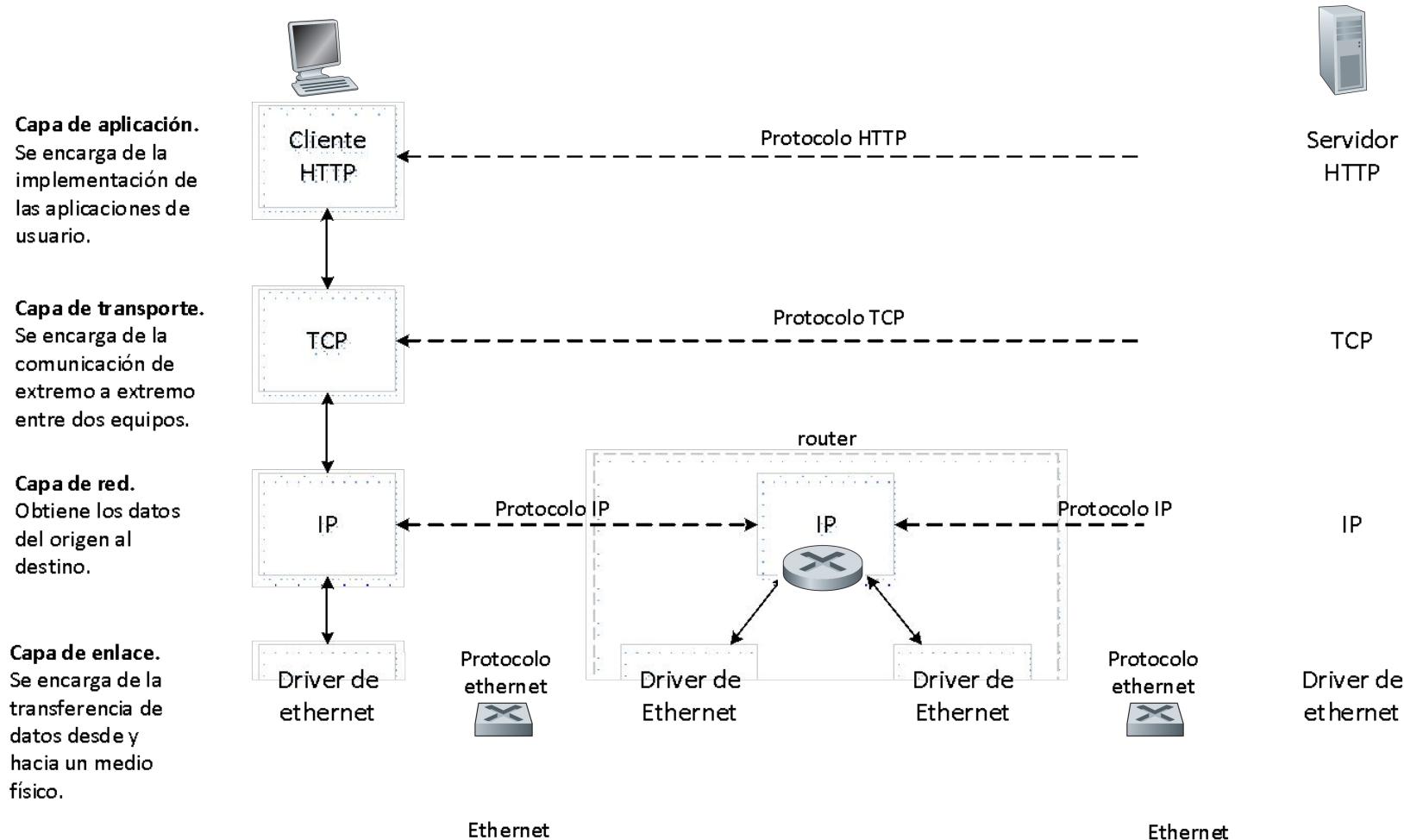
Encabezado de Red  
*Network header information*

Encabezado de Enlace  
*Link header information*





## Encapsulado de protocolos - Ejemplo





# Encapsulado de protocolos

---





# Encapsulado de protocolos





# Protocolo de red

---

- Un protocolo define el formato y el orden de los mensajes intercambiados entre dos o más entidades en una comunicación, así como también define las acciones llevadas a cabo en la transmisión y/o recepción de un mensaje u otro evento. [1]
- En un protocolo de red las entidades en la comunicación son componentes de software y hardware de algún dispositivo (computadoras, Smartphone, tableta, router, o cualquier dispositivo de red). [1]
- Toda actividad en Internet que involucra a dos o más entidades en una comunicación está regida por los protocolos. [1]



## Protocolo de red

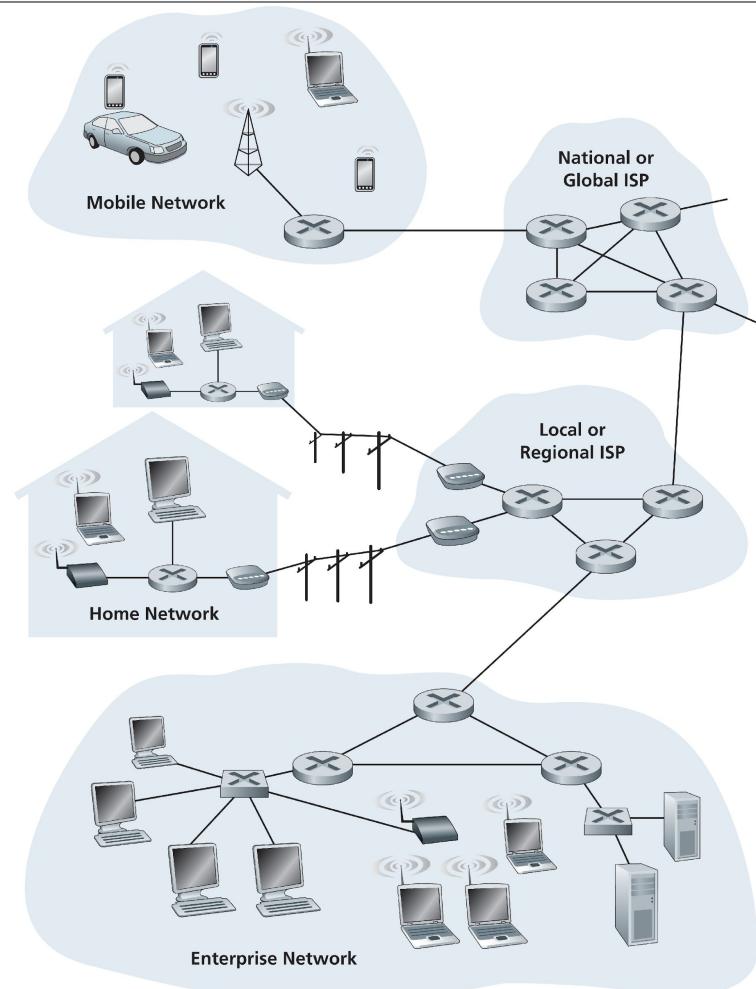
---

- Los protocolos implementados en el hardware de dos computadoras conectadas físicamente controlan el flujo de bits en el “cable” entre sus dos NIC. [1]
- Los protocolos de control de congestión en los host controlan la tasa de envío de paquetes entre el *host* que envía y el *host* que recibe. [1]
- Los protocolos en los router determinan la ruta a seguir de un paquete del origen al destino. [1]
- Los protocolos están presentes en todo el Internet, y en las redes de computadoras en general. [1]

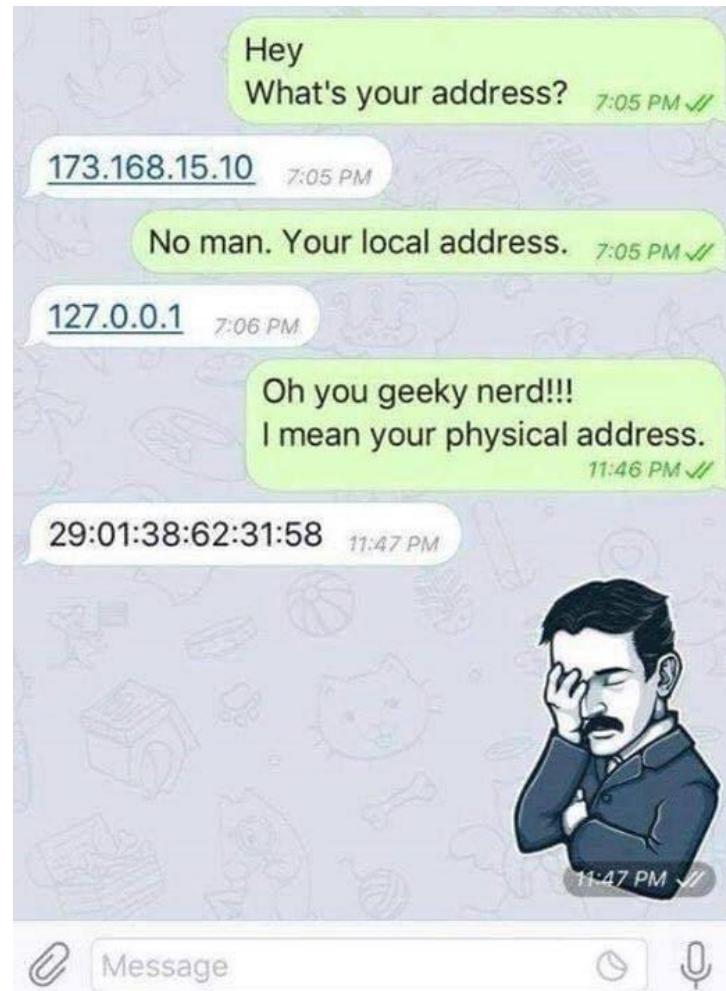


## Internet

- Es un gran conjunto de redes a lo largo del mundo, interconectadas entre sí mediante medios físicos y protocolos de comunicación. [3]
- Conecta miles de millones de dispositivos de cómputo alrededor del mundo. [1]
- Estos dispositivos de cómputo son PC de escritorio, laptop, servidores, smartphones, tabletas, televisiones, consolas de videojuegos, cámaras web, automóviles, dispositivos industriales, ...
- En términos de redes a los dispositivos anteriores se les llama host o dispositivo final (*end systems*). [1]



Algunos componentes de Internet [1]





## Referencias

---

- [1] J. Kurose and K. Ross, *Computer networking*. Boston: Pearson, 2013.
- [2] A. Tanenbaum and D. Wetherall, *Redes de computadoras*. México: Pearson Educación, 2012.
- [3] M. Katz, *Redes y seguridad*. Argentina: Alfaomega, 2013.
- [4] *Request For Comments 791*. IETF, 1981