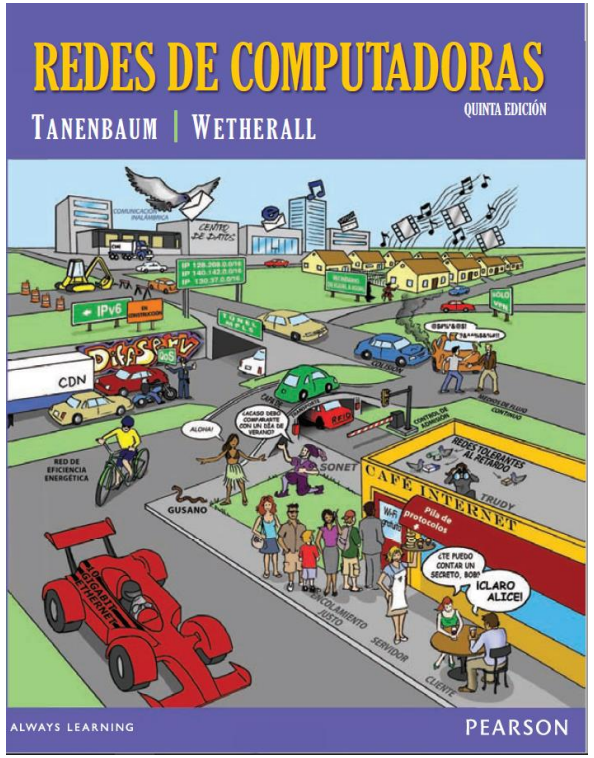
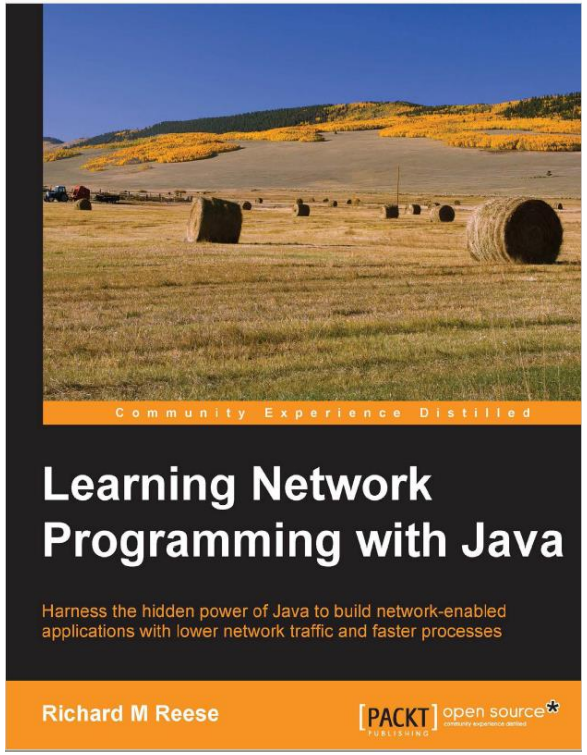
REDES DE COMPUTADORES Y LABORATORIO

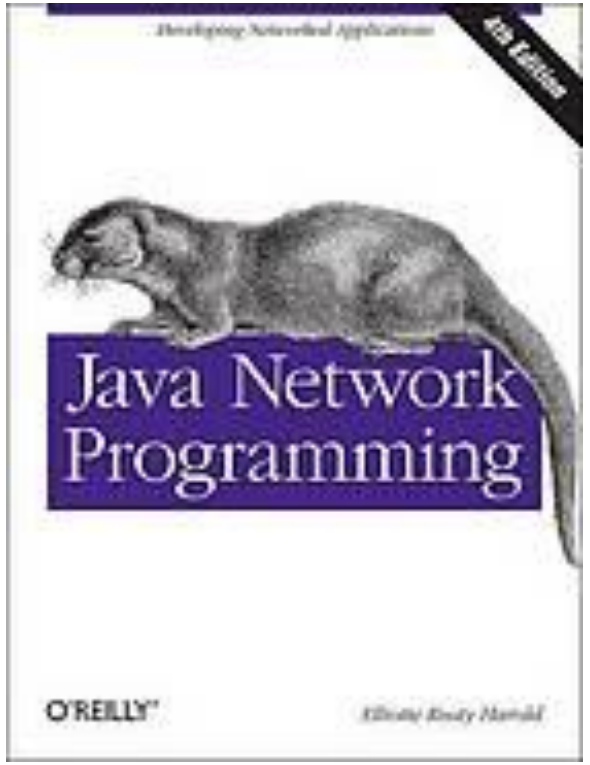
Christian Camilo Urcuqui López, MSc

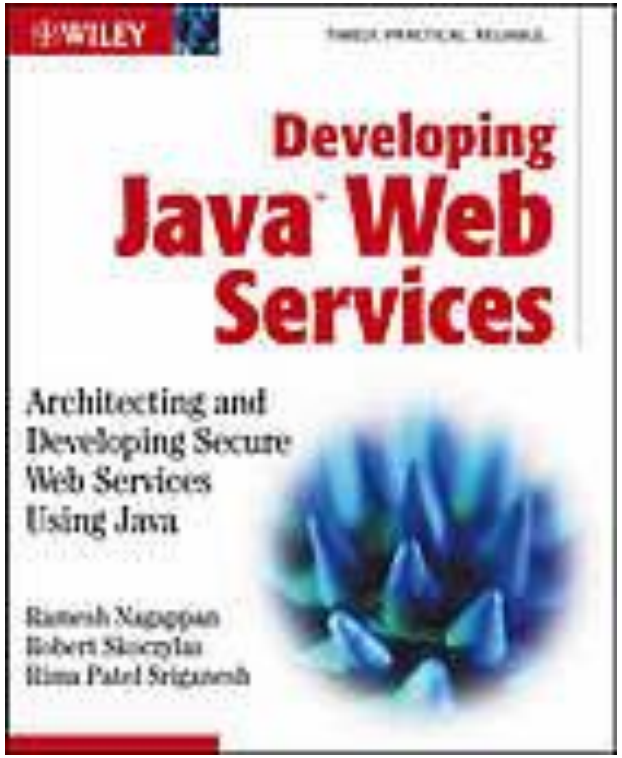
UNIVERSIDAD ICESI | A OTRO NIVEL

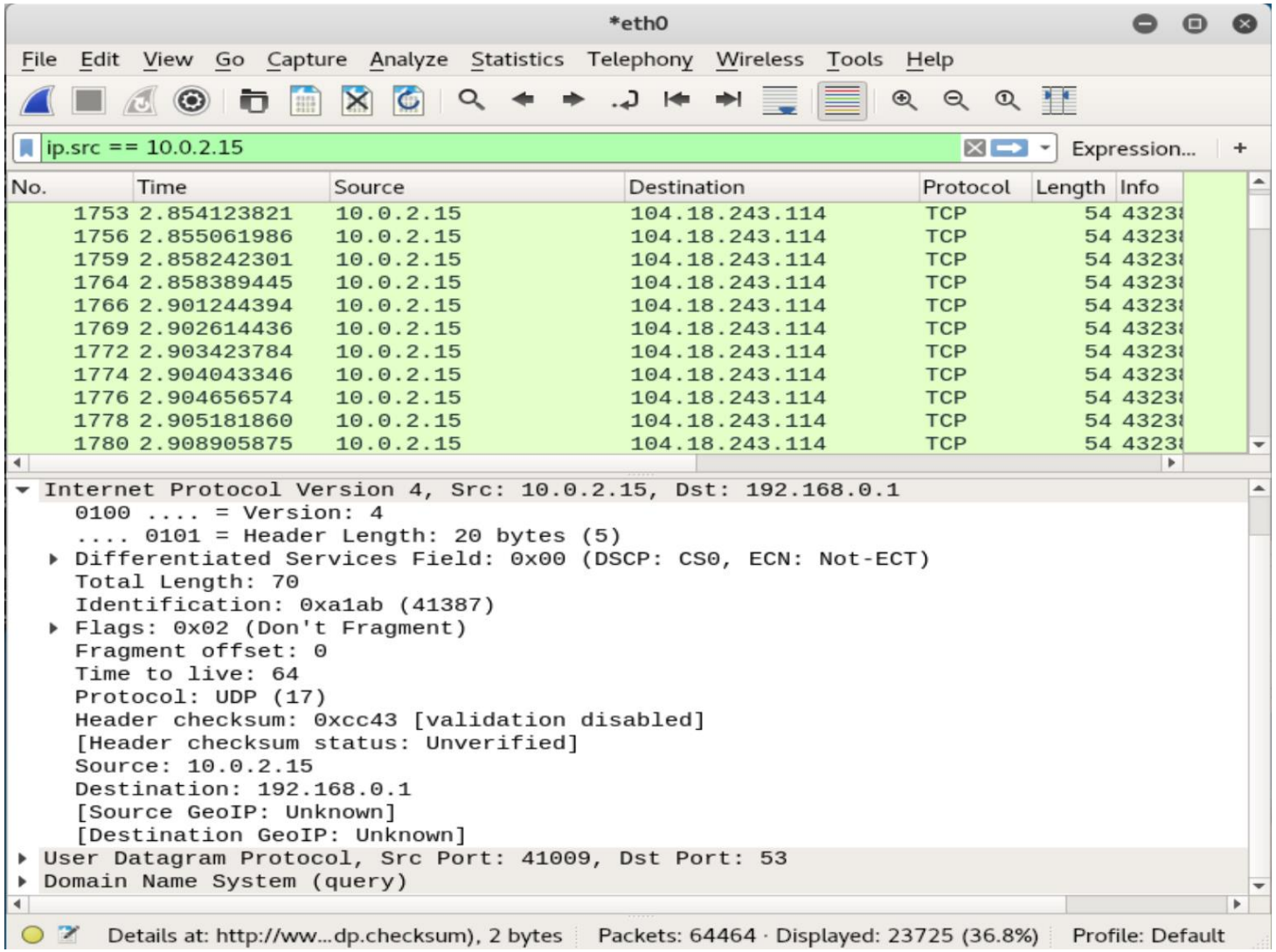
BIBLIOGRAFÍA











Se le ha suministrado una captura de red, realice una interpretación del paquete teniendo en cuenta el propósito de cada variable.

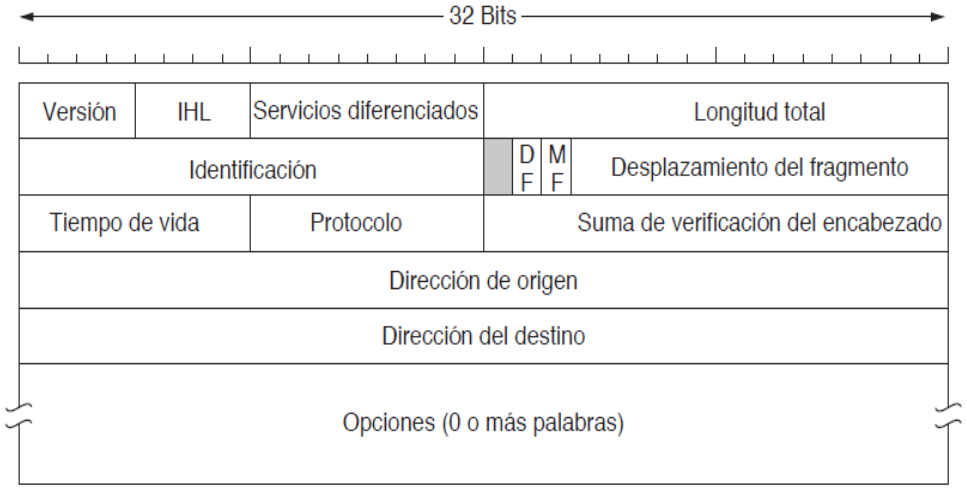


Figura 5-46. El encabezado de IPv4 (Protocolo de Internet).

COMPETENCIAS

- Aplicar de subredes
- Describir NAT
- Describir los protocolos ICMP, ARP y DHCP
- Describir TCP.

PREGUNTAS

- Suponga que su universidad comenzó con un prefijo de /24 para la red de los equipos administrativos de los edificios C, D y E. Estos edificios cuentan con un total de 100 equipos. La universidad ha construido el nuevo edificio M y requiere que cada uno de estos estén redes separadas.
- ¿Qué técnica aplicaría para resolver este problema?
- Vamos a aplicar la técnica a la dirección IP 192.168.170.10 y explicar el proceso para crear cuatro redes para cada edificio.
- ¿Por qué se utiliza NAT?

MÁSCARAS Y PREFIJOS

- Las máscaras y los prefijos representan lo mismo, es decir, la cantidad de bits de la dirección IP que representan a la red.

192.168.168.100 / 24 → 11111111111111111111111100000000

172.16.16.10 / 16 → 11111111111111110000000000000000

255.255.255.0

255.255.0.0

Máscara de red

MÁSCARAS Y PREFIJOS

Es lo mismo

192.168.168.100 / 24

Ó

192.168.168.100

255.255.255.0

DIRECCIÓN DE RED

Dirección IP = 192.168.55.100

Máscara = 255.255.255.0

Dirección de red = **192.168.55.**0 ← La porción de host siempre es 0

and

192.168.55.44 =11000000.10101000.00110111.00101100
255.255.255.0 =11111111.11111111.11111111.00000000
192.168.55.0 = 11000000.10101000.00110111.00000000

Los protocolos de enrutamiento transportan los prefijos hasta los enrutadores.

VENTAJAS Y DESVENTAJAS DE LOS PREFIJOS (CLASSFULL VS CLASSLESS)

Ventajas

- Los paquetes pueden ser reenviados con base a la porción de red de la dirección (permite que las tablas de enrutamiento sean más pequeñas y no se requiere un registro por cada host).

Desventajas

- La dirección de un host depende de su ubicación en la red y los enrutadores solo podrán entregar paquetes a esa dirección de red.
- La jerarquía desperdicia direcciones si no se administran con cuidado.

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

- Los números de red se administran a través de una corporación sin fines de lucro llamada **ICANN** (Internet Corporation for Assigned Names and Numbers) delega un espacio de direcciones a varias autoridades regionales, las cuales reparten las direcciones las direcciones IP a los ISP y otras compañías.
- El enrutamiento por prefijo requiere que todos los hots en una red tengan el mismo número de red y puede presentar problemas cuando la red tiende a aumentar su tamaño.

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

- Una subred es una división de una red más grande.
- Nace del desperdicio de bits subutilizados de la sección de host.

Suponga la dirección de red

10.0.0.0 (notación punteada)

00001010.00000000.00000000.00000000 (bits)

11111111.00000000.00000000.00000000 (bits)

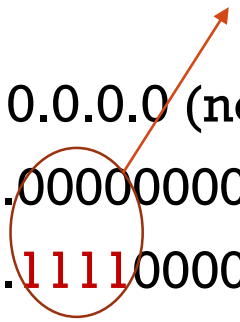
Máscara

255.0.0.0

- Para este caso tenemos un total de bits de host $2^{24} = 16.777.216 - 2 = 16.777.214$

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

- La idea es tomar bits de la porción de host y asignarlos a la porción de red.
- Suponga que vamos a utilizar 4 bits prestados, es decir, vamos a representar $2^4 = 16$ subredes



10.0.0.0 (notación punteada)

00001010.00000000.00000000.00000000 (bits)

11111111.11110000.00000000.00000000 (bits)

El resultado es una máscara de subred de

255.240.0.0

- Conclusión, estamos dividiendo la 10.0.0.0 en 16 subredes, mucho más pequeñas.
- La máscara define los bits para red y subred

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

- Retomemos la dirección IP 192.168.168.100 / 24

  Dirección de red

  192.168.168.0

- Vamos a crear 8 subredes ¿Cuántos bits necesitamos de host?

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

11000000.10101000.10101000.00000000

11111111.11111111.11111111.11100000

Máscara
255.255.255.224

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

IP inicial
192.168.168.100

11000000.10101000.10101000.00000000

11111111.11111111.11111111.11100000

Máscara
255.255.255.224

¿Cuántos host podemos crear por subred?
2^5 = 32

Subredes creadas

11000000.10101000.10101000.00000000
192.168.168.0

11000000.10101000.10101000.00100000
192.168.168.32

11000000.10101000.10101000.01000000
192.168.168.64

11000000.10101000.10101000.01100000
192.168.168.96

11000000.10101000.10101000.10000000
11000000.10101000.10101000.10100000
11000000.10101000.10101000.11000000
11000000.10101000.10101000.11100000

UNIVERSIDAD ICESI | A OTRO NIVEL

SUBREDES (SUBNET), MÁSCARAS DE RED O MÁSCARAS DE SUBRED

Subredes creadas

11000000.10101000.10101000.00000000
192.168.168.0

11000000.10101000.10101000.00100000
192.168.168.32

11000000.10101000.10101000.01000000
192.168.168.64

11000000.10101000.10101000.01100000
192.168.168.96

11000000.10101000.10101000.10000000
11000000.10101000.10101000.10100000
11000000.10101000.10101000.11000000
11000000.10101000.10101000.11100000

Cada una de las subredes tiene una capacidad para direccionar 5 bits de host:

11000000.10101000.10101000.01000001

Host1: 192.168.168.65

11000000.10101000.10101000.01000010

Host2: 192.168.168.66

.

.

.

11000000.10101000.10101000.11111111

Dirección de difusión: 192.168.168.255

SUBREDES

- El ejemplo del libro nos ilustra una universidad con un prefijo de /16 y donde se requiere crear tres áreas (subredes)

Ciencias Computacionales:	10000000	11010000	1Ixxxxxxx	xxxxxxxx
Ingeniería Eléctrica:	10000000	11010000	00Ixxxxxx	xxxxxxxx
Arte:	10000000	11010000	011Ixxxxx	xxxxxxxx

Aquí, la barra vertical (|) muestra el límite entre el número de la subred y la porción del host.

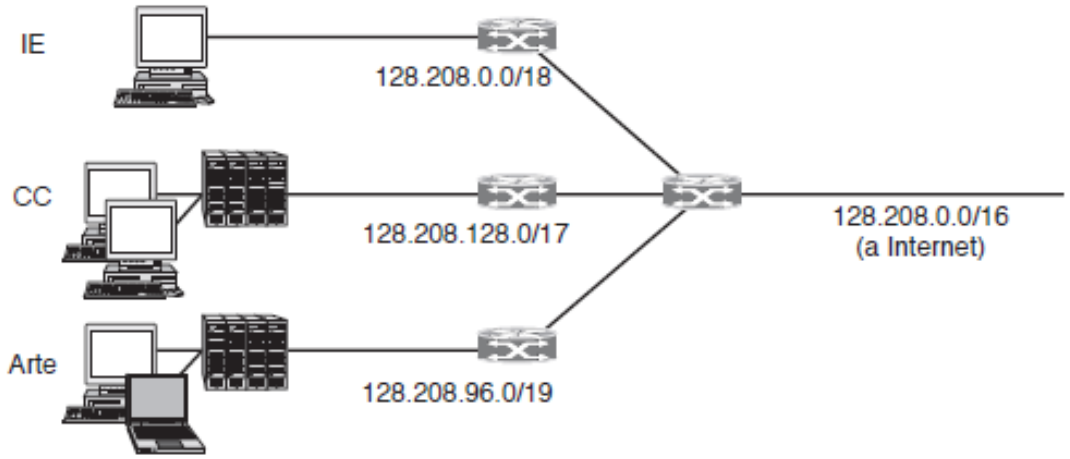
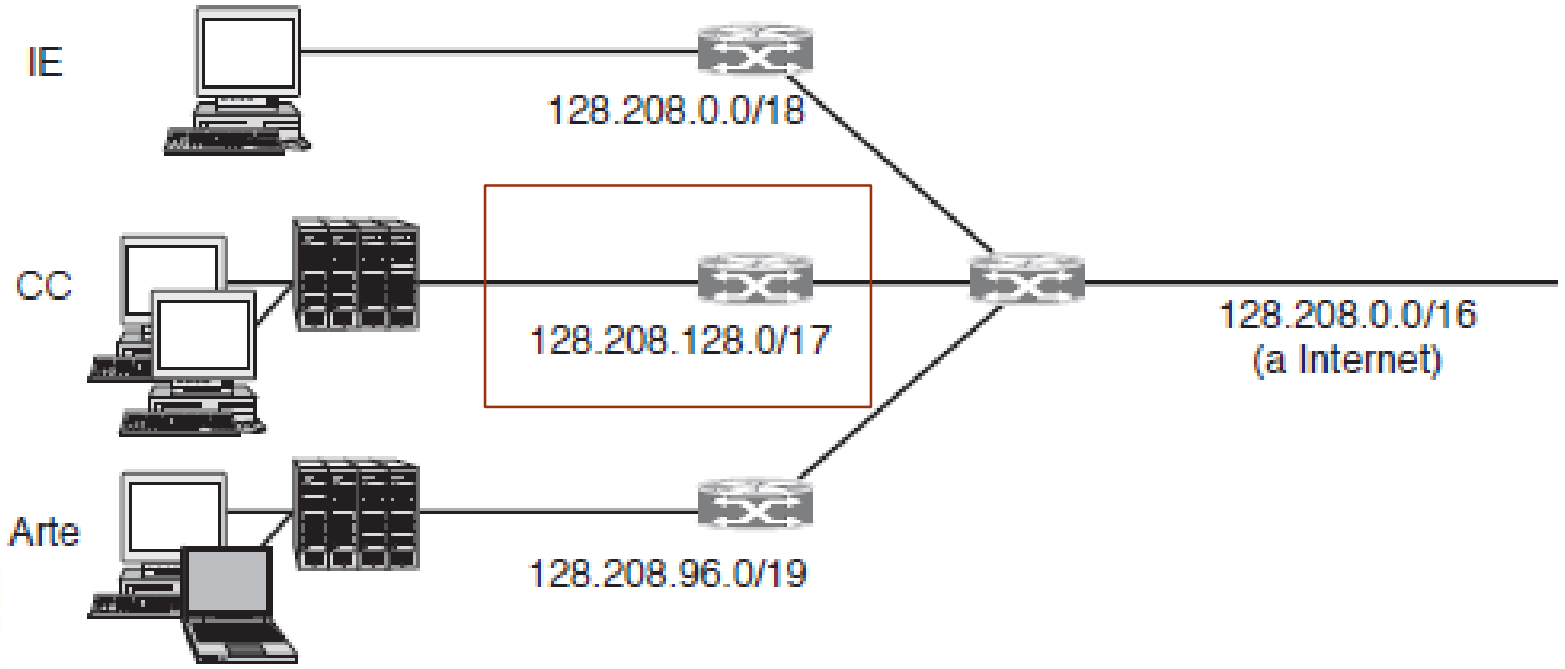


Figura 5-49. División de un prefijo IP en redes separadas mediante el uso de subredes.

SUBREDES

- El enrutador aplica un AND a la dirección del destino con la máscara para cada subred y verifica que el resultado sea el prefijo correspondiente.
- Suponga que se requiere enviar un paquete a la dirección IP 128.208.2.151. Verifiquemos si el destino es CC.



SUBREDES

128.208.2.151 → 10000000 11010000 00000010 10010111

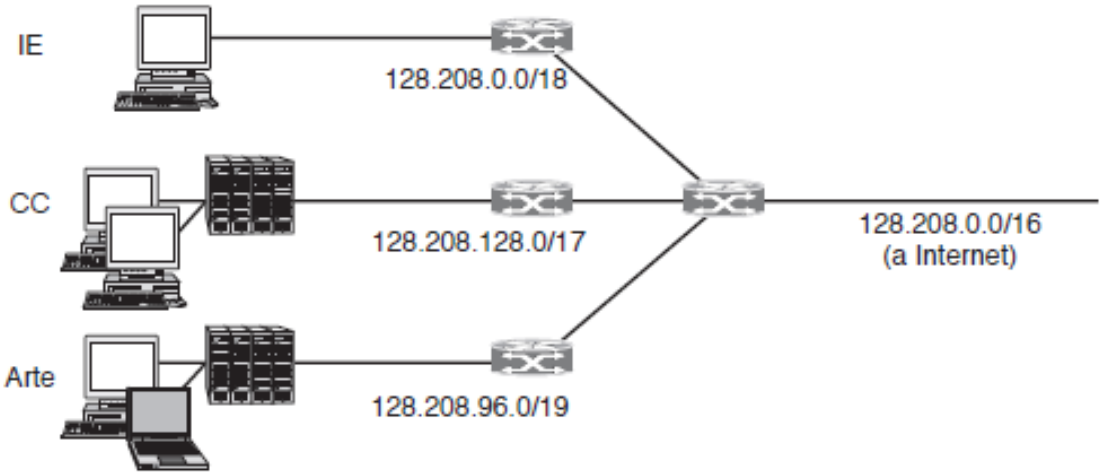
255.255.128.0 → 11111111 11111111 10000000 00000000

AND

10000000 11010000 00000000 00000000

↓

128.208.0.0



No coincide para la CC

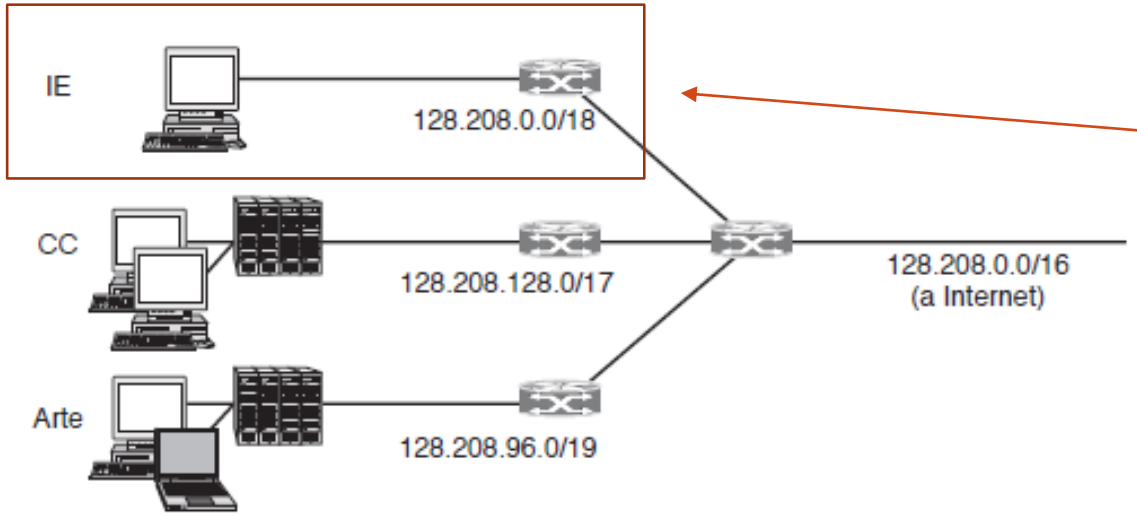
SUBREDES

Ahora probemos para el departamento de IE

128.208.2.151 → 10000000 11010000 00000010 10010111

255.255.0.0 → 11111111 11111111 00000000 00000000

AND 10000000 11010000 00000000 00000000

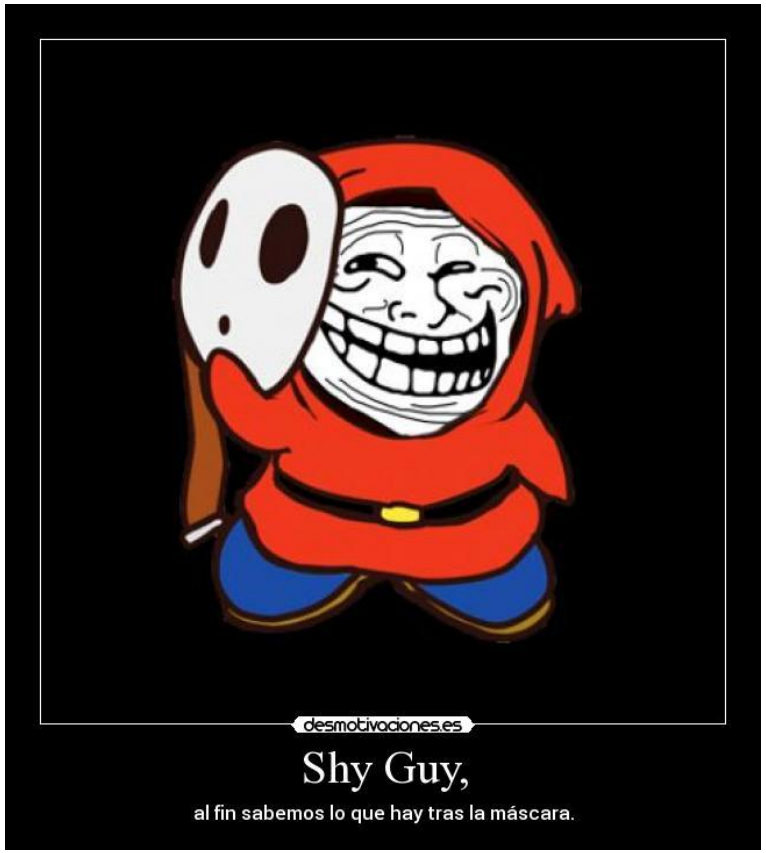


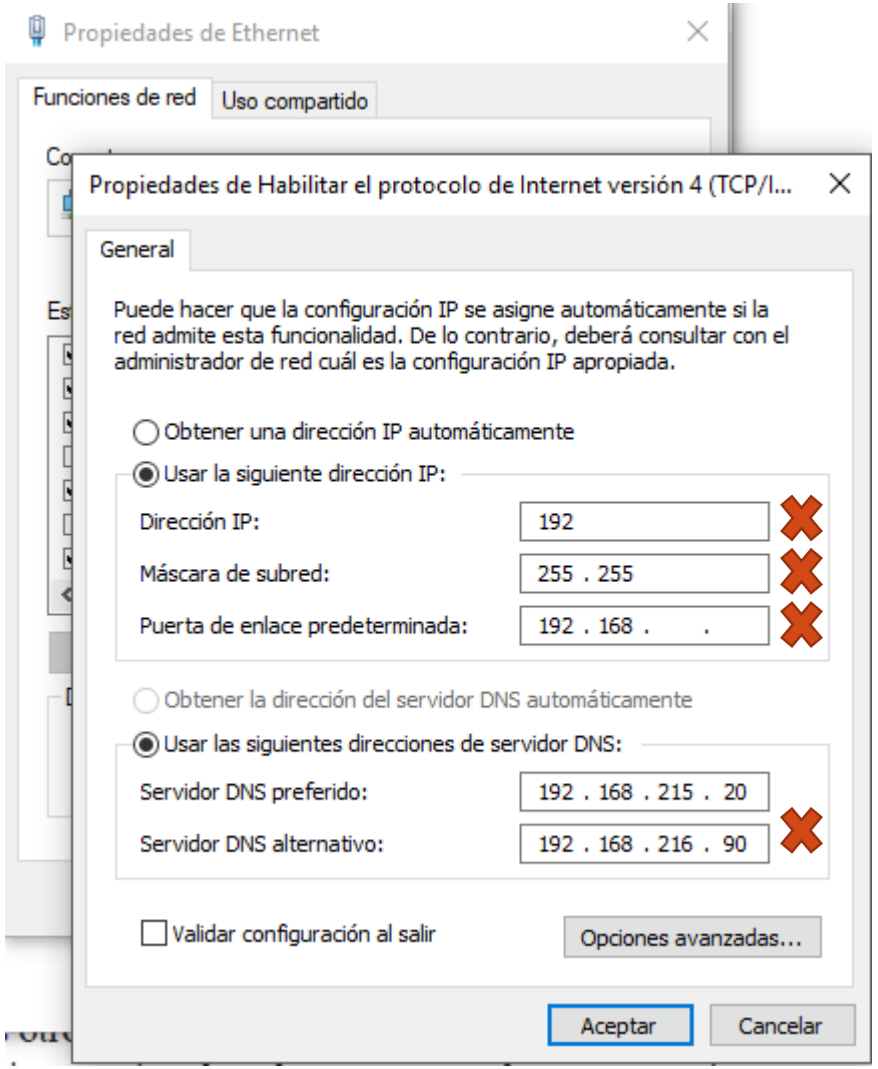
128.208.0.0

Coincide con IE

SUBREDES

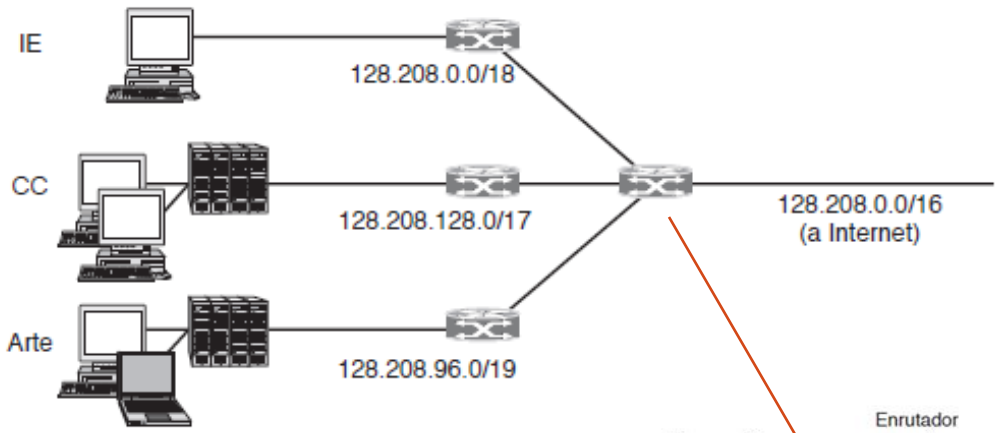
Las divisiones de las subredes se pueden cambiar a través de la máscara de red internamente en cada institución sin depender de la ISP y de la ICANN.



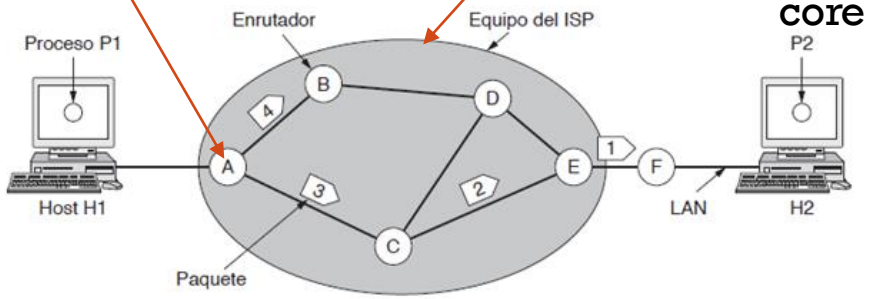


https://hipertextual.com/2018/05/servidores-dns-publicos-gratuitos

- Nadie sabe cuántas redes están conectadas a Internet
- Zona libre predeterminada, acá no funcionan las reglas predeterminada



Reglas predeterminadas



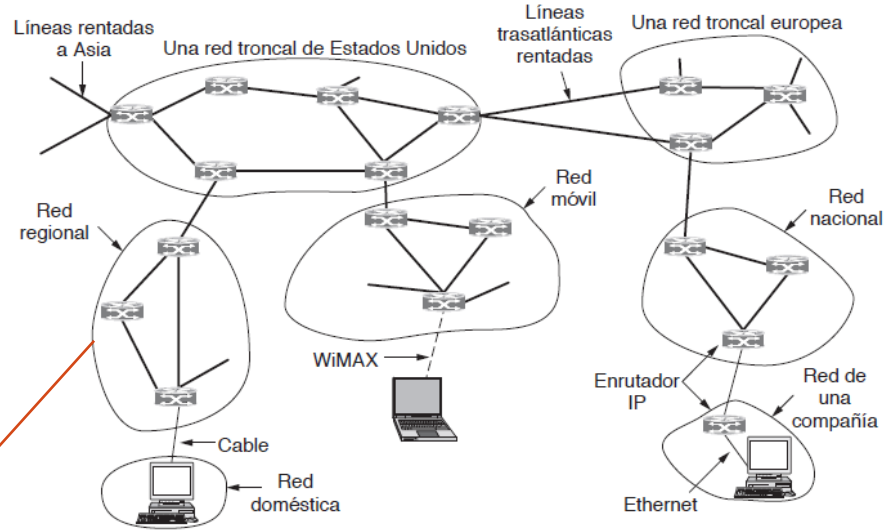


Figura 5-45. Internet es una colección interconectada de muchas redes.

Enrutadores especializados para trabajar con grandes cargas de paquetes en redes backbone – core routers

UNIVERSIDAD ICESI | A OTRO NIVEL

EL PROBLEMA DEL TAMAÑO DE LAS TABLAS DE ENRUTAMIENTO

- El procesamiento aumenta por lo menos en forma lineal con respecto al tamaño de la tabla. Una mayor comunicación aumenta la probabilidad de que algunas partes se pierdan, por lo menos en forma temporal, lo que tal vez conduzca a inestabilidades en el enrutamiento.
- Con el fin de reducir las tablas de enrutamiento se aplica una perspectiva parecida que en las subredes.
- Se combinan varios prefijos pequeños en un solo prefijo más grande. Este proceso se conoce como **agregación de rutas.** El prefijo más grande se le denomina **superred** para contrastar con las otras subredes resultantes. Es decir, la misma dirección IP que el enrutador trata como /22 (2^8 *direcciones*) puede ser tratada por otro enrutador como parte de un prefijo /20 más grande (2^{12} *direcciones*).
- La responsabilidad de tener el prefijo correspondiente es del enrutador.
- Este diseño se conoce como CIDR **(Classless InterDomain Routing)**

CIDR (CLASSLESS INTERDOMAIN ROUTING)

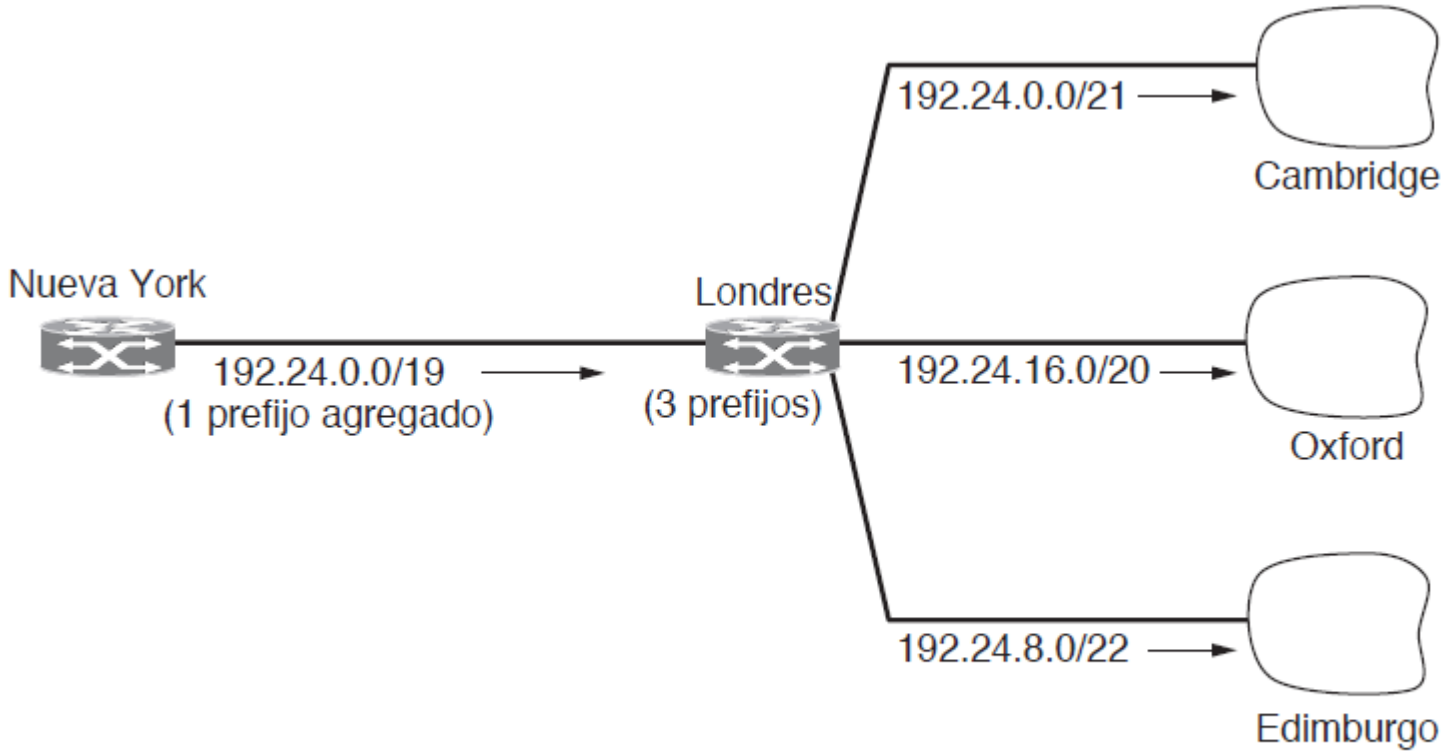


Figura 5-51. Agregación de prefijos IP.

Como hemos visto las direcciones IPv4 tienen un límite y estamos escasos…

NAT (NETWORK ADDRESS TRANSLATION)

- Las direcciones IP son escasas. Un ISP podría tener una dirección con un prefijo de /16, lo cual da 65534 números host. Si tiene más clientes que esos, tiene un problema.
- Una solución es migrar a IPv6, pero, se requerirá mucho tiempo e inversión para lograrlo.
- Mientras tanto, existe otra solución que es la aplicación de NAT (documentada en la RFC 3022).

NAT (NETWORK ADDRESS TRANSLATION)

- El objetivo de la NAT es que el ISP asigne a cada hogar o negocio una dirección IP (puede ser un grupo pequeño) para el tráfico de Internet.
- Dentro de la red del cliente hay solo una dirección IP para enrutar el tráfico interno y antes de salir a Internet esta es traducida a la dirección IP pública compartida.
- Las traducciones hacen uso de tres rangos de direcciones IP que se han declarado como privados.

10.0.0.0	– 10.255.255.255/8	(16,777,216 hosts)
172.16.0.0	– 172.31.255.255/12	(1,048,576 hosts)
192.168.0.0	– 192.168.255.255/16	(65,536 hosts)

NAT (NETWORK ADDRESS TRANSLATION)

- La caja NAT transforma la dirección IP interna, 10.0.0.1 a la dirección verdadera del cliente, 198.60.42.12.
- A menudo las NAT vienen incorporadas en los firewall para el análisis de las paquetes enviados y recibidos. También, se pueden encontrar en los enrutadores.

El puerto es importante para la NAT ya que le permite identificar el proceso emisor y al receptor.

La NAT en su proceso de identificación debe analizar un puerto origen y uno destino.

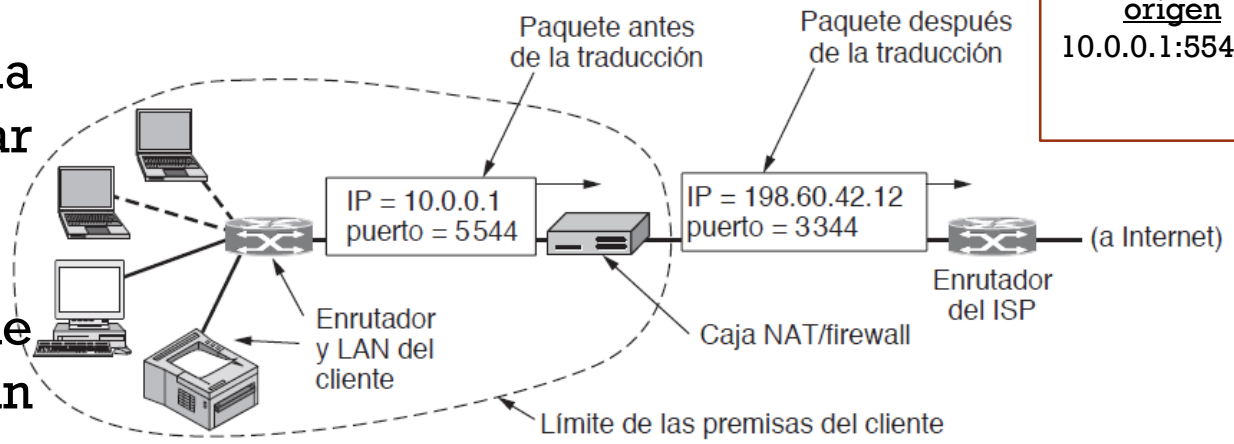


Tabla de la NAT

origen	salida
10.0.0.1:5544	198.60.42.12:3344

Figura 5-55. Colocación y funcionamiento de una caja NAT.

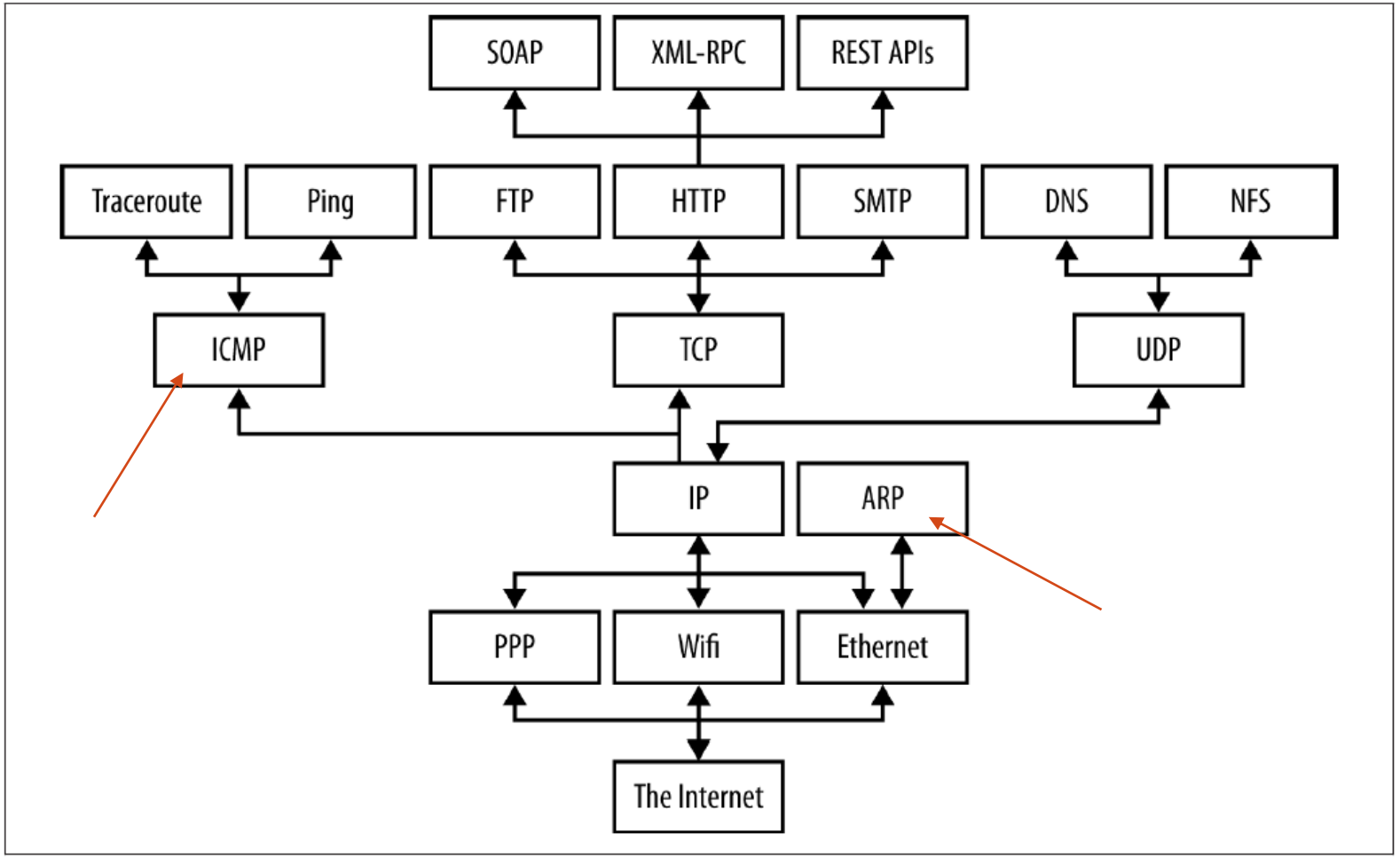
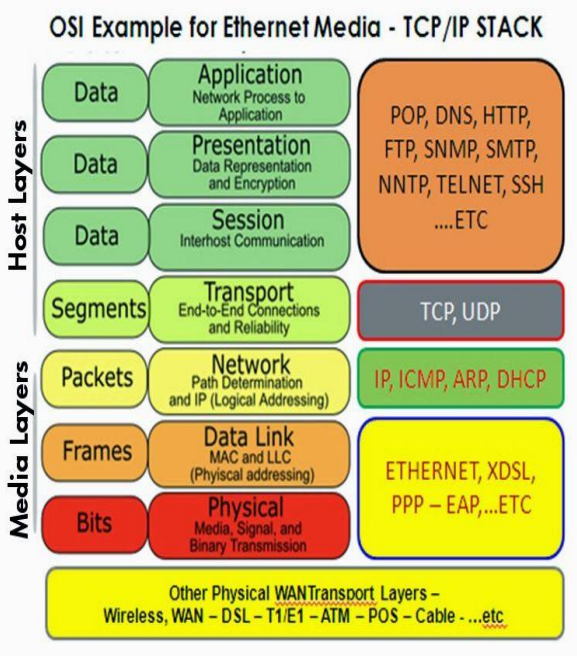


Figure 1-1. Protocols in different layers of a network

PROTOCOLOS DE CONTROL EN INTERNET



- **ICMP (Internet Control Massage Protocol**) es un protocolo que informa sobre un evento inesperado en el procesamiento de un paquete en un enrutador.
- También es utilizado para probar Internet.

Tipo de mensaje	Descripción
Destination unreachable (Destino inaccesible).	No se pudo entregar el paquete.
Time exceeded (Tiempo excedido).	El tiempo de vida llegó a cero.
Parameter problem (Problema de parámetros).	Campo de encabezado inválido.
Source quench (Fuente disminuida).	Paquete regulador.
Redirect (Redireccionar).	Enseña a un enrutador la geografía.
Echo and echo reply (Eco y respuesta de eco).	Verifica si una máquina está viva.
Timestamp request/reply (Estampa de tiempo, Petición/respuesta).	Igual que solicitud de eco, pero con marca de tiempo.
Router advertisement/solicitation (Enrutamiento anuncio/solicitud).	Busca un enrutador cercano.

Figura 5-60. Los principales tipos de mensajes ICMP.

```
     6 0.356980      ::                    ff02::16              ICMPv6     170 Multicast Listener Report Message v2
     7 0.587340      ::                    ff02::16              ICMPv6     170 Multicast Listener Report Message v2
```

```
> Frame 13: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
> Ethernet II, Src: OrientPo_a6:d7:0b (00:13:37:a6:d7:0b), Dst: Micro-St_14:84:e4 (30:9c:23:14:84:e4)
> Internet Protocol Version 4, Src: 172.16.32.1, Dst: 172.16.32.152
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x95f3 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.16.32.152, Dst: 172.16.32.1
  > User Datagram Protocol, Src Port: 58434, Dst Port: 53
  > Domain Name System (query)
```

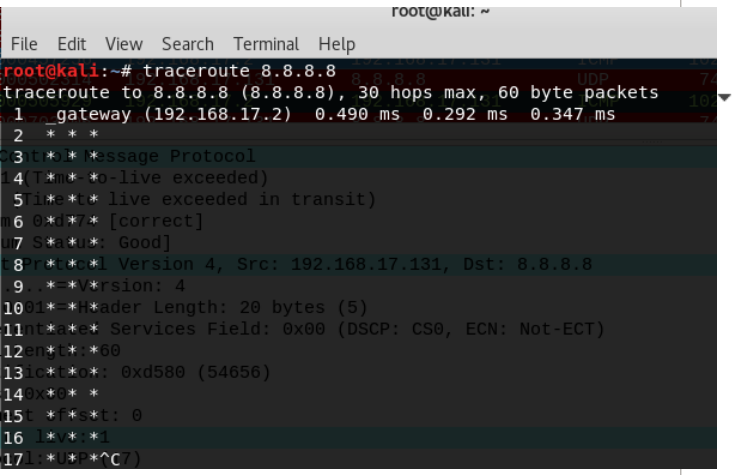
```
207 15.054887    8.8.8.8          192.168.0.103    ICMP    74 Echo (ping) reply    id=0x0001, seq=45/11520, ttl=117 (request in 206)
208 15.960318    192.168.0.103    8.8.8.8          ICMP    74 Echo (ping) request  id=0x0001, seq=46/11776, ttl=128 (reply in 209)
209 16.055713    8.8.8.8          192.168.0.103    ICMP    74 Echo (ping) reply    id=0x0001, seq=46/11776, ttl=117 (request in 208)
```

```
> Frame 206: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Micro-St_14:84:e4 (30:9c:23:14:84:e4), Dst: Tp-LinkT_5c:71:22 (c4:e9:84:5c:71:22)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d2e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 45 (0x002d)
    Sequence number (LE): 11520 (0x2d00)
    [Response frame: 207]
  > Data (32 bytes)
```

```
Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=99ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=95ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=109ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=107ms TTL=117

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 95ms, Máximo = 109ms, Media = 102ms
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=84.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=87.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=111 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=105 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=87.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=91.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=128 time=118 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=128 time=96.7 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=128 time=84.3 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=128 time=87.0 ms
```



1	0.000000000	192.168.17.131	8.8.8.8	UDP	74 44778 → 33434 Len=32
2	0.000241422	192.168.17.131	8.8.8.8	UDP	74 42596 → 33435 Len=32
3	0.000457256	192.168.17.2	192.168.17.131	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
4	0.000502314	192.168.17.131	8.8.8.8	UDP	74 35736 → 33436 Len=32
5	0.000505929	192.168.17.2	192.168.17.131	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)

```
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xd774 [correct]
    [Checksum Status: Good]
Internet Protocol Version 4, Src: 192.168.17.131, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xd580 (54656)
  ▸ Flags: 0x00
    Fragment offset: 0
  ▸ Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x01f6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.17.131
    Destination: 8.8.8.8
    [Source GeoIP: Unknown]
  ▾ [Destination GeoIP: United States, AS15169 Google Inc., United States, AS15169 Google Inc., 37.750999, -97.821999]
      [Destination GeoIP Country: United States]
      [Destination GeoIP AS Number: AS15169 Google Inc.]
      [Destination GeoIP Country: United States]
      [Destination GeoIP AS Number: AS15169 Google Inc.]
      [Destination GeoIP Latitude: 37.750999]
      [Destination GeoIP Longitude: -97.821999]
▸ User Datagram Protocol, Src Port: 44778, Dst Port: 33434
▾ Data (32 bytes)
    Data: 404142434445464748494a4b4c4d4e4f5051525354555657...
```

```
0000  00 0c 29 b3 d3 87 00 50  56 e3 c6 70 08 00 45 00   ..)....P V..p..E.
0010  00 58 01 a4 00 00 80 01  95 2b c0 a8 11 02 c0 a8   .X...... .+......
```

RECORDEMOS.... IPV4

Opción	Descripción
Seguridad.	Especifica qué tan secreto es el datagrama.
Enrutamiento estricto desde el origen.	Proporciona la ruta completa a seguir.
Enrutamiento libre desde el origen.	Proporciona una lista de enrutadores que no se deben omitir.
Registrar ruta.	Hace que cada enrutador adjunte su dirección IP.
Estampa de tiempo.	Hace que cada enrutador adjunte su dirección y su etiqueta de tiempo.

Figura 5-47. Algunas de las opciones del protocolo IP.

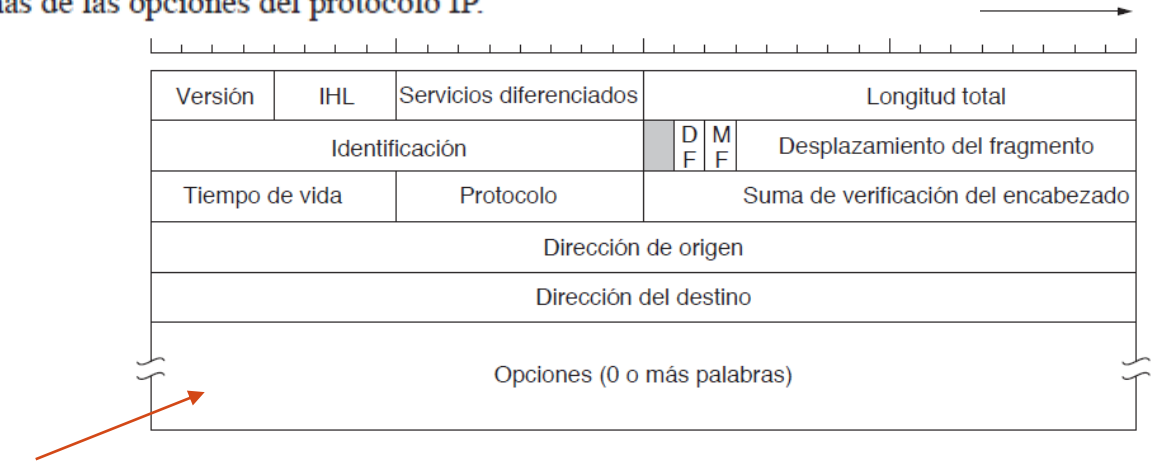
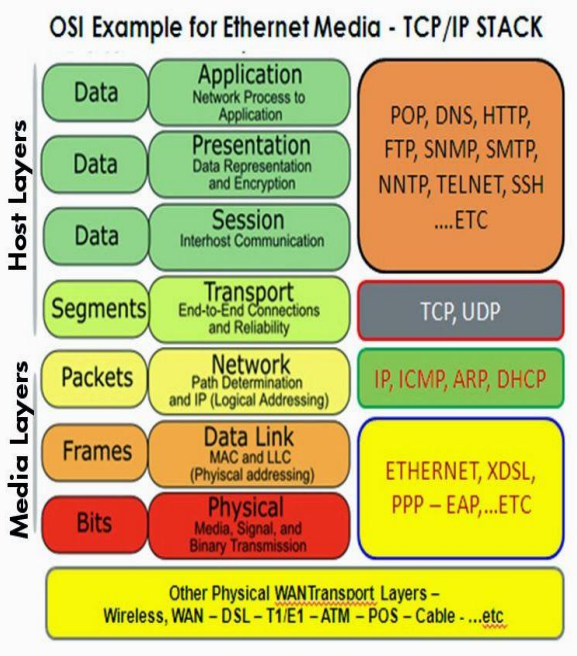


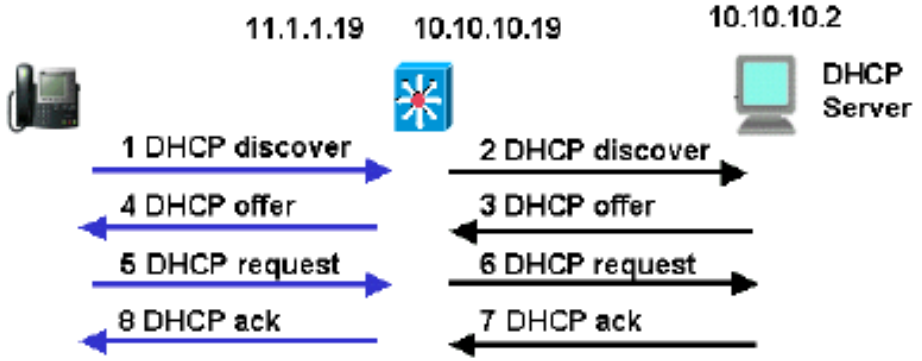
Figura 5-46. El encabezado de IPv4 (Protocolo de Internet).

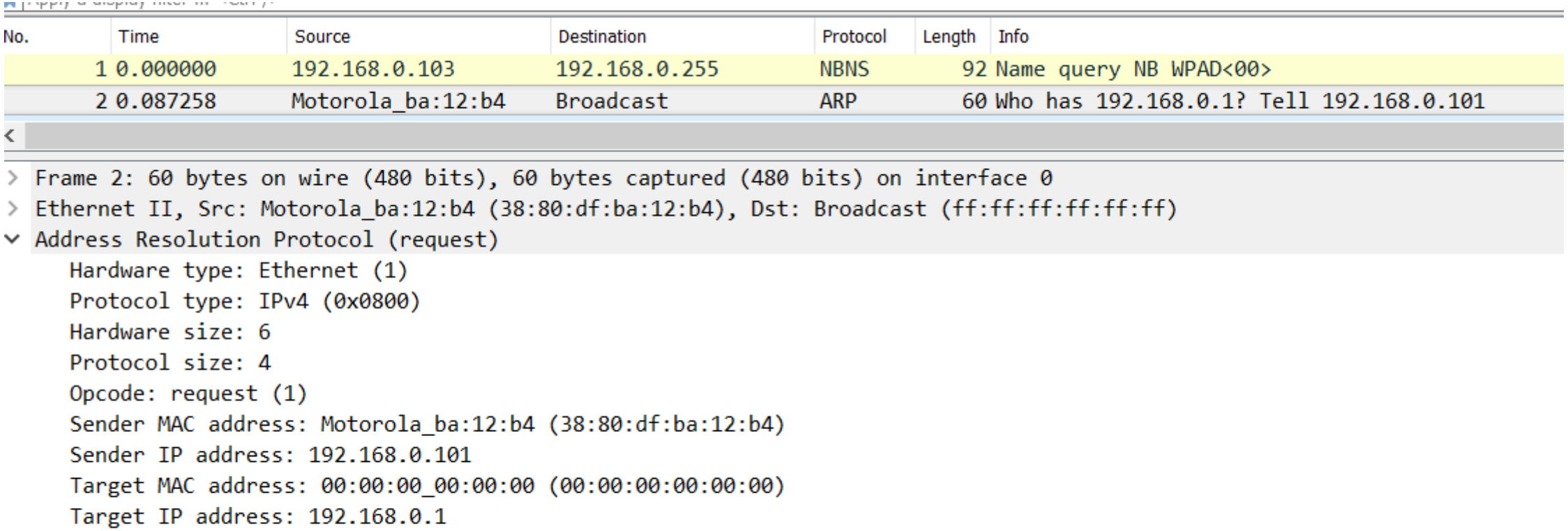
PROTOCOLOS DE CONTROL EN INTERNET



- **ARP (Address Resolution Protocol**) encargado de encontrar la dirección de hardware (MAC) que corresponde a una determinada dirección IP.
  - Las máquinas luego de ejecutar ARP almacenan sus resultados en cache.
- **DHCP (Dynamic Host Configuration Protocol).** Es un proceso para configuración dinámica de los host; para ello debe existir un servidor DHCP responsable

La técnica del arrendamiento





No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.103	192.168.0.255	NBNS	92	Name query NB WPAD<00>
2	0.087258	Motorola_ba:12:b4	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.101

LA CAPA DE TRANSPORTE

- Recordemos…. La capa de red provee entrega de paquetes punto a punto mediante el uso de datagramas o circuitos virtuales.
- El objetivo de la capa de transporte es proporcionar un servicio de transmisión de datos eficiente, confiable y económico a sus usuarios, procesos que normalmente son de la capa de aplicación.
- Gracias a esta capa, los programadores pueden escribir código de acuerdo con un conjunto estándar de primitivas; estos programas pueden funcionar en una amplia variedad de redes sin necesidad de preocuparse por lidiar con diferentes interfaces de red y distintos niveles de confiabilidad.

PRÓXIMA CLASES - COMPETENCIAS

- Describir capa de transporte

LECTURAS

Material utilizado	1. Arboleda, L. (2012). Programación en Red con Java. 2. Harold, E. (2004). Java network programming. " O'Reilly Media, Inc.". 3. Tanenbaum, A. S. (2003). Redes de computadoras. Pearson educación. 4. Reese, R. M. (2015). Learning Network Programming with Java. Packt Publishing Ltd.
Actividades DESPUÉS clase	A1. Leer del libro 3 el contenido desde la sección 6.1 hasta la 6.2.5

REFERENCIAS

1. https://www.google.com.co/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwju5o62x-vdAhXjtlkKHaouDcAQjRx6BAgBEAU&url=http%3A%2F%2Feltallerdelbit.com%2Fdireccionamiento-ip%2F&psig=AOvVaw3E_T5IpV-ANtL0eEQbHtkg&ust=1538700259199893
2. https://www.cisco.com/c/dam/en/us/support/docs/ip/dynamic-address-allocation-resolution/19580-dhcp-multintwk-4.gif