



Tema 2 **Capa de red**

Fundamentos de Redes
Grado en Ingeniería Informática y dobles grados
Curso 3º

Jorge Navarro Ortiz

Departamento de Teoría de la Señal, Telemática y Comunicaciones
E.T.S. Ingenierías Informática y Telecomunicación – Universidad de Granada

C/ Periodista Daniel Saucedo Aranda, s/n - 18071 – Granada (Spain)

Teléfono: +34-958 241000, ext 20042 - Fax: +34-958 243032 - Email: jorgenavarro@ugr.es

© 2022



1

Tema 2. Capa de red



Esquema

1. Funcionalidades
2. Comutación
3. El protocolo IP
4. Asociación con la capa de enlace: el protocolo ARP
5. El protocolo ICMP
6. Autoconfiguración de la capa de red (DHCP)





Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

Tema 2. Capa de red

Objetivos del tema

- **Comprender las funcionalidades y servicios de la capa de red :**
 - Concepto de comutación de paquetes y datagramas
 - Direccionamiento en Internet
 - Encaminamiento salto a salto
 - Asociación con la capa de enlace a través del protocolo ARP
 - Señalización de errores mediante el protocolo ICMP

3

3

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

Tema 2. Capa de red

Bibliografía

Capítulo 6 y 9, Pedro García Teodoro, Jesús Díaz Verdejo y Juan Manuel López Soler. **TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES**, Ed. Pearson, 2017, ISBN: 978-0-273-76896-8

- Apuntes de direccionamiento IP en web de la asignatura

Para saber más...

Capítulo 4 James F. Kurose y Keith W. Ross. **COMPUTER NETWORKING. A TOP-DOWN APPROACH**, 5^a Edición, Addison-Wesley, 2010, ISBN: 9780136079675

4



Tema 2. Capa de red

Esquema

1. Funcionalidades
2. Conmutación
3. El protocolo IP
4. Asociación con la capa de enlace: el protocolo ARP
5. El protocolo ICMP
6. Autoconfiguración de la capa de red (DHCP)

5



Tema 2. Capa de red

1. Funcionalidades

- Funciones y servicios en TCP/IP
 - Encaminamiento → Proporcionan una función cuyo objetivo es el establecimiento de la ruta (secuencia de líneas y nodos) de comunicación en la subred a seguir desde un origen a un destino dados
 - Conmutación → Permiten un mayor aprovechamiento del canal dispuesto para la transmisión de datos, permitiendo gestionar de forma ordenada la transmisión de distintos paquetes a la vez
 - Interconexión de redes
 - En OSI: control de congestión → Los datos a transmitir entre 2 estaciones finales pueden sufrir retardos crecientes, lo cual puede provocar su retransmisión por la expiración del temporizador asociado en el emisor. Estas retransmisiones dan lugar a mover, provocando mayor congestión, pero existen funciones y servicios que solucionan esto
- Ejemplos de protocolos de red:
 - X.25 https://es.wikipedia.org/wiki/Norma_X.25
 - IP

6





Tema 2. Capa de red

Esquema

1. Funcionalidades
2. **Comutación**
3. El protocolo IP
4. Asociación con la capa de enlace: el protocolo ARP
5. El protocolo ICMP
6. Autoconfiguración de la capa de red (DHCP)

7



Tema 2. Capa de red

2. Comutación

- Comutación = acción de establecer o determinar un camino que permita transmitir información extremo a extremo
- Esquemas de comutación
 - Circuitos → Establecimiento de una conexión origen-destino previo a la transmisión de datos. Todos los datos se transmiten de forma secuencial, no se fragmentan. Consta de 3 fases: 1. Establecimiento conexión: Se reservan los recursos necesarios (cada nodo desde el siguiente en base a la dirección de destino). 2. Transmisión, intercambio de datos de forma secuencial y no se produce retraso salvo los de propagación. Los datos se reciben en el orden de emisión. 3. Cierre de la conexión: Se liberan los recursos asociados a la comunicación.
 - Paquetes: datagramas o circuitos virtuales
 - Comutación de circuitos
- Ej. Teléfono
- Es un servicio orientado a conexión → exige un establecimiento de conexión previo a la transmisión

nodo 1: central final nodo 2: central de larga distancia nodo 3: central de larga distancia nodo 4: central final

- Pasos: (i) Conexión, (ii) Transmisión, (iii) Desconexión
- Recursos dedicados. Facilita comunicaciones tiempo-real. No hay contención (contienda por acceder al medio).
- Retraso para establecimiento de la llamada. Poca flexibilidad para adaptarse a cambios. Poco tolerante a fallos.

8



Tema 2. Capa de red

2. Conmutación

- **Comutación de circuitos**

💡 **Ventajas**

- La transmisión se realiza en tiempo real, adecuado para voz
- Uso permanente de recursos, el circuito se mantiene durante toda la sesión
- No hay contención, no hay contienda para acceder al medio
- El circuito es fijo, no hay decisiones de encaminamiento una vez establecido
- Simplicidad en la gestión de los nodos intermedios.

💡 **Desventajas**

- Retraso en el inicio de la comunicación.
- En ocasiones uso no eficiente de recursos.
- El circuito es fijo. No se reajusta la ruta de comunicación.
- ↳ Si falla un nodo, se cae todo
- ↳ Los recursos reservados no pueden ser usados por otra comunicación, incluso si están mal aprovechados

9

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz





- 9
- a) No se establece conexión previa a la transmisión
 b) El mensaje se divide en bloques más pequeños (paquetes o datagramas)
 c) Cada paquete se transmite independientemente del resto, pueden seguir caminos distintos y llegar desordenadas al receptor. Tienen información diversa, como su destino.
 d) La transmisión se realiza en forma de almacenamiento y envío. Los nodos intermedios deben almacenar temporalmente cada paquete y procesarlo antes de su retransmisión.
- Por los tiempos de procesamiento intermedios implicados en las reenvíos, es poco adecuado para servicios interactivos que precisan velocidad. Por ello surge comutación de paquetes mediante circuitos virtuales, que mezclan los datagramas con la comutación de circuitos

Tema 2. Capa de red

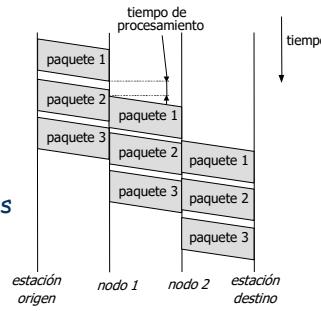
2. Conmutación

Comutación de paquetes:

- Envío en bloques (paquetes)
- Comutación mediante datagramas:
 - ej. IP
 - No hay conexión
 - Envío independiente, pueden seguir rutas diferentes
 - En cada salto: Almacenamiento y envío
 - Cada paquete debe contener las direcciones origen y destino
- Comutación de paquetes con circuitos virtuales:
 - ej. ATM (troncales)
 - Pasos: (i) Conexión, (ii) Transmisión, (iii) Desconexión
 - Recursos no dedicados

10

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz







Tema 2. Capa de red

2. Comutación

4. Estime el tiempo involucrado en la transmisión de un mensaje de datos para la técnica de comutación de paquetes mediante datagramas (CDP) considerando los siguientes parámetros:

- M: longitud en bits del mensaje a enviar.
- V: velocidad de transmisión de las líneas en bps.
- P: longitud en bits de los paquetes.
- H: bits de cabecera de los paquetes.
- N: número de nodos intermedios entre las estaciones finales.
- D: tiempo de procesamiento en segundos en cada nodo.
- R: retardo de propagación, en segundos, asociado a cada enlace.

11

Universidad de Granada

11

En circuitos virtuales, el establecimiento de la conexión es de la misma forma que en comutación de circuitos (cada nodo decide el siguiente de la ruta en base a la dirección de destino). A diferencia de la comutación de circuitos, los circuitos virtuales pueden ser compartidos entre varias comunicaciones (la única reserva de recursos es la asignación de la línea de salida, de forma que la retransmisión de un paquete de un nodo a otro a veces requiere esperar si la línea está ocupada). La estación destino responde con un mensaje de aceptación que puede tardar en volver si la línea está ocupada por otras comunicaciones (el camino de vuelta puede ser distinto del de ida). Dividido el mensaje en paquetes, siguen cada uno su ruta (cada paquete tiene un identificador de camino virtual) como en comutación de circuitos, aunque en forma de almacenamiento y reenvío como en los datagramas.

Tema 2. Capa de red

Esquema

1. Funcionalidades
2. Comutación
3. **El protocolo IP**
4. Asociación con la capa de enlace: el protocolo ARP
5. El protocolo ICMP
6. Autoconfiguración de la capa de red (DHCP)

12

Universidad de Granada



Tema 2. Capa de red

3. El protocolo IP

IPv4 está especificado en el RFC 791:

- Es un protocolo para la **interconexión** de redes (también llamadas subredes).
- Resuelve el **direcccionamiento** en Internet.
- Realiza la **retransmisión salto a salto** entre hosts y routers. Ofrece un servicio **no orientado a conexión y no fiable**:
 - No hay negociación o "handshake", no hay una conexión lógica entre las entidades.
 - No existe control de errores ni control de flujo.
- La unidad de datos (paquete) de IP se denomina **datagrama**.
- IP es un protocolo de **máximo esfuerzo** ("best-effort"), es decir los datagramas se pueden perder, duplicar, retrasar, llegar desordenados.
- IP gestiona la "**fragmentación**": adaptar el tamaño del datagrama a la diferentes *Maximum Transfer Units (MTUs)* de las subredes hasta llegar al destino.

13

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

13

Tema 2. Capa de red

3. El protocolo IP

➤ Direcciones IP:

Microsoft Hotmail	Servidor Webmail	www.youtube.com
	130.206.192.39	172.194.34.206
Google España	Servidor Spotify	
	78.31.8.101	78.31.8.101
www.google.com = 172.194.34.209		Universidad de Granada www.ugr.es = 150.214.204.25 dns3.ugr.es = 150.214.191.10 pop.ugr.es = 150.214.20.3

14

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

14

3. El protocolo IP

- Internet adopta un **direcciónamiento jerárquico** para simplificar el **routing**.
 - Las direcciones IP (32 bits) tienen dos partes bien diferencias:
un identificador de la subred y un identificador del dispositivo dentro de esa subred.
 - Cada subred tiene un identificador único en la intranet.
 - Cada dispositivo tiene un identificador único en la subred.
 - La **máscara de red** es un patrón que determina qué bits pertenecen al identificador de subred
a) Dirección IP → $200.27.4.112 = 11001000.00011011.00000100.01110000$
Máscara → $255.255.255.0 = 11111111.11111111.11111111.00000000$
b) La máscara se puede representar de forma compacta, por ejemplo $200.27.4.112/24$
 - Para obtener la dirección o identificador de la subred:
$$\begin{array}{rcl} 200.27.4.112 & = & 11001000.00011011.00000100.01110000 \\ & \& \\ 255.255.255.0 & = & 11111111.11111111.11111111.00000000 \\ & \hline & \end{array}$$

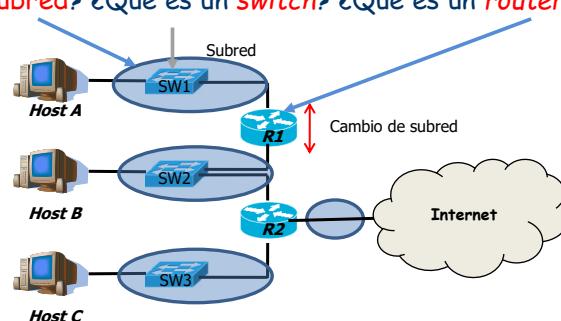
↓
Cuenta unos (van seguidos)

Subred → $200.27.4.0 = 11001000.00011011.00000100.00000000$



3. El protocolo IP

- Podemos considerar Internet como un conjunto de subredes interconectadas
 - ¿Qué es una **subred**? ¿Qué es un **switch**? ¿Qué es un **router**?



Computer Networking. A Top-down Approach. de James F. Kurose y Keith W. Ross

“Para determinar las subredes, separe cada interfaz de los hosts y routers creando redes aisladas. Dichas redes aisladas se corresponden con las subredes.”



Tema 2. Capa de red

3. El protocolo IP

➤ ¿Qué es una **subred**? ¿Qué es un **switch**? ¿Qué es un **router**?

¿Quién tiene direcciones IP?
Los *hosts* y los *routers* tienen 1 IP por cada interfaz.
Los *switches* NO tienen direcciones IP

Computer Networking. A Top-down Approach. de James F. Kurose y Keith W. Ross:
"Para determinar las subredes, separe cada interfaz de los hosts y routers, creando redes aisladas. Dichas redes aisladas se corresponden con las subredes."

17

17

Tema 2. Capa de red

3. El protocolo IP

➤ ¿Cómo se elige la máscara? ➔ Según el **número de dispositivos** previsibles en la subred tal que se ajusta para no desaprovechar direcciones. Recuérdese: cada subred tiene un identificador único en nuestra intranet.

Dirección IP ➔ 200.27.4.112 = 11001000.00011011.00000100.01110000
Máscara ➔ 255.255.255.0 = 11111111.11111111.11111111.00000000

➤ # dispositivos = $2^{\# \text{ ceros}} - 2$ ➔ ej. 8 ceros (/24) permite 254 dispositivos

➤ El -2 viene de que la primera (000...0) y última (111...1) están reservadas.
Por ejemplo en la subred 200.27.4.0/24 no se pueden asignar como id. de dispositivo

- > 200.27.4.0 = 11001000.00011011.00000100.00000000 ➔ Reservada (subred)
- > 200.27.4.1 = 11001000.00011011.00000100.00000001 ➔ Dispositivo #1
- > ...
- > 200.27.4.254 = 11001000.00011011.00000100.11111110 ➔ Dispositivo #254
- > 200.27.4.255 = 11001000.00011011.00000100.11111111 ➔ Reservada (difusión)

18

18

Tema 2. Capa de red

3. El protocolo IP

➤ Direcciones **públicas**

- Cada dirección se asigna a sólo 1 dispositivo en Internet.
Se asignan centralizadamente

➤ Direcciones **privadas** No cuestan dinero

- Sólo en intranets. Se pueden repetir en distintas intranets.
Las asigna el usuario según su criterio.

A → 10.x.y.z/8
B → 172.16-31.x.y/16
C → 192.168.x.y/24

19

Universidad de Granada

19

!! DESPERDICIO DE DIRECCIONES!!

NAT → dir. privadas que se pueden repetir
192.168.0.0/24 ? Investigar si 1.0/24 Jen casa
Direcciónamiento sin clase subredes teníamos eso
superredes

Tema 2. Capa de red

3. El protocolo IP

➤ Direcciones IP: CLASES (ver RFC 1166)

- Los hosts y routers tienen una IP por cada una de sus interfaces.
- 32 bits, notación decimal con puntos. Ejemplo: 192.168.212.60
- 5 clases de direcciones IP
- Clases A,B,C → Jerárquicas a dos niveles:
identificador de red + identificador de dispositivo (host)

Clase A	0	red (7 bits)	host (24 bits)	/8 → 128 redes 2^{24} equipos 0...127.x.y.z
Clase B	1 0	red (14 bits)	host (16 bits)	/16 → 2^{14} redes 2^{16} equipos 128...
Clase C	1 1 0	red (21 bits)	host (8 bits)	/24 → 2^{21} redes 2^8 equipos
Clase D	1 1 1 0	dirección grupo multicast (28 bits)		No tienen máscara
Clase E	1 1 1 1 0	uso futuro		Utilizadas de forma experimental, para fines de investigación

Utilizadas con fines de multicisión (difusión general a más de un dispositivo)

20

Universidad de Granada

Tema 2. Capa de red

3. El protocolo IP

5 clases de direcciones (cont.):

Rangos:

A → 0.0.0.0-127.255.255.255 ⇒	128 redes x 16.777.216 hosts
B → 128.0.0.0-191.255.255.255 ⇒	16.384 redes x 65.536 hosts
C → 192.0.0.0-223.255.255.255 ⇒	2.097.152 redes x 256 hosts
D → 224.0.0.0-239.255.255.255 ⇒	para multicast
E → 240.0.0.0-255.255.255.255 ⇒	usos futuros

Reglas especiales:

- host = 00..0** ⇒ identifica a una red, nunca es una dirección origen, no se usa para dispositivos
- host = 11..1** ⇒ difusión en la red especificada, es una dirección destino, no se usa para dispositivos
- 127.0.0.0** ⇒ autobucle (*loopback*) → Sirve para que un proceso pueda comunicarse con un proceso de la misma máquina

Para evitar ambigüedades el identificativo de dispositivo no debe ser ni 255 ni 0

Reserva de direcciones privadas (RFC1918):

- Clase A → 10.0.0.0 → 1 Red privada clase A
- Clase B → 172.16.0.0 - 172.31.0.0 → 16 redes privadas clase B
- Clase C → 192.168.0.0 - 192.168.255.0 → 256 redes privadas clase C

Gestión/asignación: IANA (www.iana.org) ahora gestionada por ICANN (www.icann.org)

21

Tema 2. Capa de red

3. El protocolo IP

NAT (Network Address Translation) (RFC 1631, 2663, 3022)

Diagram illustrating the NAT process:

- Host** (IP: 10.0.0.1) is connected to a **Private network**.
- The **Private network** is connected to a **Router + NAT** (IP: 150.150.0.1).
- The **Router + NAT** is connected to the **Internet** (IP: 200.100.10.1).
- A **Server** (IP: 200.100.10.1) is also connected to the **Internet**.
- When the Host sends a packet to the Server, the Router + NAT changes the Source IP address from 10.0.0.1 to 150.150.0.1 and the Destination IP address from 200.100.10.1 to 150.150.0.1.
- When the Server responds, the Router + NAT changes the Source IP address from 200.100.10.1 to 10.0.0.1 and the Destination IP address from 150.150.0.1 to 200.100.10.1.

Cuando el servidor trata de responder con un destino que está en una red privada, no se sabe adónde mandarlo porque las IP privadas no son únicas en el mundo

es un método para reasignar un espacio de direcciones IP (típicamente privadas) a otro (públicas) modificando la dirección IP de los paquetes mientras se retransmiten a través de un router

22

Tema 2. Capa de red

3. El protocolo IP

Network Address Translation (RFC 1631, 2663, 3022)

- Optimiza el uso de direcciones públicas mediante la utilización de direcciones privadas.
- Reemplaza las direcciones privadas origen salientes por públicas y al revés con las entrantes.

■ Tabla de traducciones.

■ **IMPORTANTE:** No se pueden implementar servidores detrás de un NAT. Por ello, se establece la zona pública (DMZ) y la zona privada.

23

Universidad de Granada

23

Tema 2. Capa de red

3. El protocolo IP

Problema de escasez de direcciones IP

- Se necesitan m direcciones pero se disponen de n , siendo $n < m$.
- Si $n = 1$ se denomina enmascaramiento (**masquerading**).
- Se usa en ISPs, para así poder dar acceso a más usuarios que direcciones IP tenga el ISP. Se supone que no todos los usuarios acceden simultáneamente. Las direcciones se asignan a los usuarios de forma dinámica.
- **SNAT:** Source NAT → el origen de los datos está en la red privada; cambia la dirección IP de origen; se realiza tras el encaminamiento (*postrouting*)
- **DNAT:** Destination NAT → el origen de los datos está en la red pública; cambia la dirección IP de destino; requiere configurar en el router qué puerto irá dirigido a qué máquina; se realiza antes del encaminamiento (*prerouting*)

24

Universidad de Granada

24

Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortíz

PROTO TCP
SADDR 10.0.0.3
DADDR 128.32.32.68
SPORT 1049 (se le da el sistema)
DPORT 80 (puerto de destino)
FLAGS SYN
CKSUM 0x1636

1. El cliente intenta conectarse al servidor web 128.32.32.68 y envía un paquete SYN con su dirección IP interna 10.0.0.3 (privada).

Para darle cuenta de si un paquete es erróneo lo corrige, pero los deshace.

Cliente 10.0.0.3

NAT interna 10.0.0.1

NAT externa 24.1.70.210

INTERNET

Servidor web 128.32.32.68

PROTO TCP
SADDR 24.1.70.210
DADDR 128.32.32.68
SPORT 40960
DPORT 80
FLAGS SYN
CKSUM 0x2436

2. El dispositivo NAT ve la configuración del paquete, añade una nueva entrada a su tabla de traducción. Luego modifica el paquete usando su dirección IP externa (pública), cambia el puerto y el chequeo de integridad del paquete.

Se calcula porque se han producido cambios en la cabecera.

3. El dispositivo NAT mira su tabla de traducción, y encuentra la que corresponde a direcciones y puertos origen/destino. Reescribe el paquete utilizando los puertos y direcciones internas.

4. El dispositivo NAT manda el paquete a través de la red pública.

Tabla de traducción

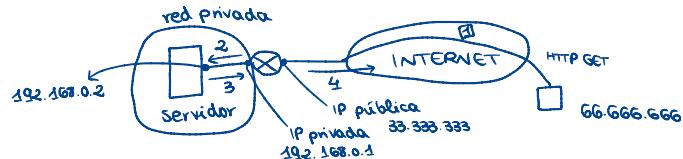
Original	NAT
10.0.0.3:1049	24.1.70.210:40960
...	...

PROTO TCP
SADDR 128.32.32.68
DADDR 24.1.70.210
SPORT 80
DPORT 40960
FLAGS SYN, ACK
CKSUM 0x8041

3. El dispositivo NAT responde con un paquete SYN, ACK. El paquete se envía a la dirección IP externa (pública) del dispositivo NAT.

25

25



Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortíz

➤ Ejercicio: Asignar direcciones

- Subredes corporativas: 30 dispositivos, direcciones privadas 192.168.0.0
- Subred de acceso: dirección pública (ISP)

Host A, Host B, Host C connected to R1, R1 connected to R2, R2 connected to Internet.

1. saddr 66666666
sport 1060
daddr 33333333
dport 1080
HTTP GET

2. saddr 66666666
sport 1060
daddr 192.168.0.2
dport 80
HTTP GET

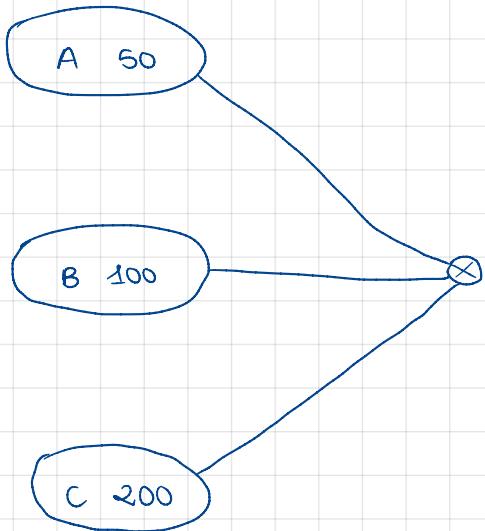
3. saddr 192.168.0.2
sport 80
daddr 66.666.666
dport 1060
HTTP RESPONSE

4. saddr 33333333
sport 1080
daddr 66666666
dport 1060
HTTP RESPONSE

Universidad de Granada

26

26



Dir. públicas $\rightarrow 33.33.0.0/23$

Dir. privadas \rightarrow

$$C \rightarrow 200 + 1 \text{ dr. router} + 1 \text{ dr. red} + 1 \text{ dr. difusión} = 203 \leq 256 = 2^8 \Rightarrow 32 - 8 = 24 \Rightarrow /24$$

$33.33.0.0/24$ red
 $33.33.0.255/24$ difusión

$$B \rightarrow 100 + 1 \text{ dr. router} + 1 \text{ dr. red} + 1 \text{ dr. difusión} = 103 \leq 128 = 2^7 \Rightarrow 32 - 7 = 25$$

$33.33.1.0/25 \rightarrow 1.0$
" " red " " difusión

$$A \rightarrow 50 + \dots = 53 \leq 64 = 2^6 \Rightarrow 32 - 6 = 26$$

1.128
" " red " " difusión

$$C \rightarrow 200 + 1 \text{ dr. red} + 1 \text{ dr. router} + 1 \text{ dr. difusión} = 203 \leq 256 = 2^8 \Rightarrow /24$$

$192.168.0.0$ red $192.168.0.255$ difusión

$$B \rightarrow 100 + 3 = 103 \leq 128 = 2^7 \Rightarrow /25$$

$192.168.1.0$ red $192.168.1.127$

$$A \rightarrow 53 \leq 64 = 2^6 \Rightarrow /26$$

$192.168.1.128$ red $192.168.1.191$

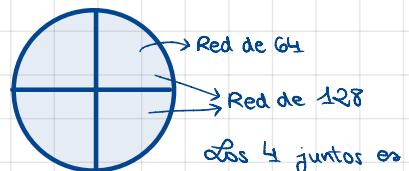
De chico a grande

$$A \rightarrow 53 \leq 64 = 2^6 \Rightarrow /26$$

$192.168.0.0$ red $192.168.0.63$ difusión

$$B \rightarrow 103 \leq 128 = 2^7 \Rightarrow /25$$

$192.168.0.64$ red $192.168.0.191$
 ↘ $192.168.0.0$! Esto no es una dirección de red!



Los 4 juntos es una red de 256. Solo se puede partir de esa forma

$$C \rightarrow 203 \leq 256 = 2^8 \Rightarrow /24$$

$192.168.0.192$ red $192.168.1.191$ difusión
 ↘ $192.168.0.11000000$ Tampoco es dir. red

$192.168.1.10111111$

Y encima la parte de red cambia ¡MAL!

Tema 2. Capa de red

3. El protocolo IP

➤ Ejercicio: Asignar direcciones

- Subredes corporativas: 30 dispositivos, direcciones privadas 192.168.0.0 → 5 ceros, /27
- Subred de acceso: dirección pública (ISP) → 2 ceros, /30, 150.214.190.0 (UGR)

192.168.0.2 Subred = 192.168.0.0

Host A

192.168.0.35 192.168.0.33 Subred = 192.168.0.32

Host B

192.168.0.66 192.168.0.65 Subred = 192.168.0.64

Host C

R1

R2

150.214.190.1 Subred = 150.214.190.0

Internet

27

Universidad de Granada

27

Tema 2. Capa de red

3. El protocolo IP

➤ El encaminamiento

- Encontrar el mejor camino para llevar la información (paquetes) de un origen a un destino dado.
- Se decide paquete a paquete y salto a salto en función de la IP destino del paquete y de las tablas de encaminamiento residentes en cada uno de los routers.

Host A

Host B

Host C

R1

R2

Internet

Encaminamiento

Almacenamiento & Retransmisión

28

Universidad de Granada

28

TABLA DE ENCAMINAMIENTO

R_1	Dir. destino	Máscara	Sig. salto
	192.168.0.0 (red A)	/27	*
	192.168.0.32 (red B)	/27	*
	192.168.0.64 (red C)	/27	192.168.0.34 (router 2)
	Default	/0	192.168.0.34 (router 2)

R_2	Dir. destino	Máscara	Sig. salto
	192.168.0.0 (red A)	/27	192.168.0.33 (router 1)
	192.168.0.32 (red B)	/27	*
	192.168.0.64 (red C)	/27	*
	Default	/0	IP gateway operador

	Dir. dest.	Máscara	Sig. salto
equipo A →	192.168.0.0	/27	*
	Default	/0	192.168.0.1 (R_1) → Sirve para comunicarse con los demás hosts de la red Si no está en su red, siempre sale por R_1
equipo B →	192.168.0.32	/27	*
	Default	/0	192.168.0.34 (R_2) → También podríamos haber puesto R_1
equipo C →	192.168.0.64	/27	*
	Default	/0	192.168.0.65 (R_2)

Tema 2. Capa de red

3. El protocolo IP

➤ Retransmisión salto-a-salto:

- Resolución local del camino
- En el dispositivo origen y todos los intermedios

Host A → R1 → R2 → Host C

Internet

29

Universidad de Granada

29

Tema 2. Capa de red

3. El protocolo IP

El encaminamiento se realiza **salto a salto** y **datagrama a datagrama** (IP es no orientado a conexión).

❑ Modos de encaminamiento: **directo y no directo.**

❑ Cada dispositivo (*host* o *router*) tiene una tabla de encaminamiento.

❑ Un *router* suele estar en varias redes distintas, un *host* suele estar en solo una

30

Tabla de R1, * = routing directo

¿Falta algún destino?
↳ Si, falta una ruta directa hacia Internet

i	Destino (D_i)	Salto siguiente (S_i)	Máscara (M_i)	Flags	Interfaz(I_i)	
1	127.0.0.1	*	255.255.255.255	H	lo	192.100.15.0
2	192.100.12.0	*	255.255.255.0	-	eth0	En caso de conflicto se elige la ruta con máscara más larga
..	192.100.13.0	*	255.255.255.0	-	eth1	
..	192.100.15.0	192.100.12.1	255.255.255.0	G	eth0	
N	Default	150.100.0.222	0.0.0.0	G	eth2	

30

Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

31

- Si no hay fragmentación y no hay "traducción de direcciones" (NAT) el datagrama (salvo el TTL, las opciones y el campo de comprobación) no se modifica en el camino.
- Proceso de encaminamiento en los nodos IP (salto a salto) por cada datagrama:
 - Se extrae la dirección destino: IP_DESTINO del datagrama
 - Por cada entrada i con $i = 1, \dots, N$, de la tabla de encaminamiento se calcula
$$IP_i = IP_DESTINO \text{ AND}(\&) \text{ MASCARA}_i$$
 - Si $IP_i = Di$ y si es routing directo (*) → reenviar el datagrama al destino final por la interfaz i o si no es routing directo → reenviar el datagrama al salto siguiente por la interfaz i
 - Si hay varias coincidencias se elige el destino con la máscara más larga
 - Si se ha barrido toda la tabla y no hay coincidencia con ninguna fila → error (posible mensaje ICMP)
 - Para encapsular el datagrama en la trama física correspondiente, se debe consultar la tabla ARP (ver más adelante) y en caso de no conocer la dirección física se envía un broadcast con protocolo ARP para obtener la dir. física.

Protocolo que avisa al origen

Universidad de Granada

31

Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

32

➤ Tabla de encaminamiento:

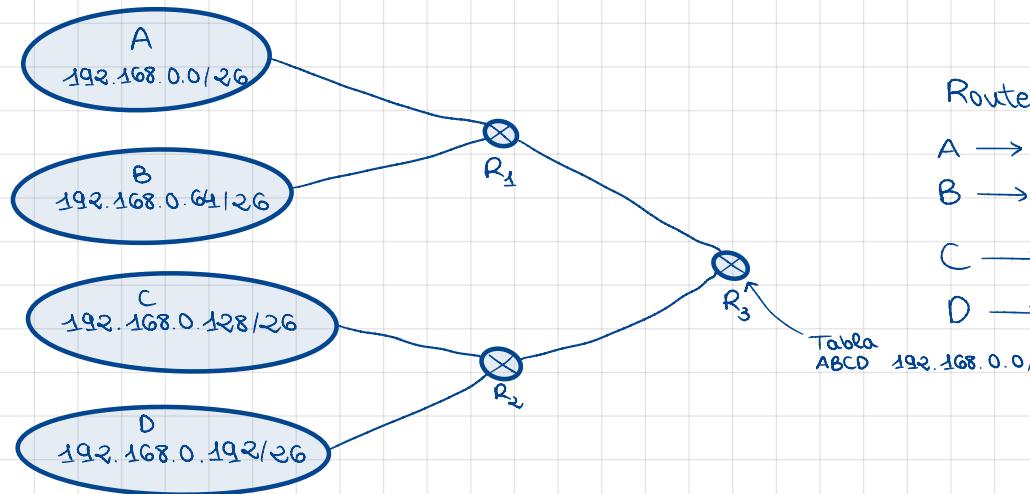
Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
192.168.0.32	/27	192.168.0.1
192.168.0.64	/27	192.168.0.1
150.214.190.0	/30	192.168.0.1

1 dr.router + 1 dr.red + 1 dr.difusión = $3 \leq 4 = /30$

Host A: 192.168.0.2
Host B: 192.168.0.1
Host C: 192.168.0.66
Subred = 192.168.0.32
Subred = 192.168.0.64
R1: 192.168.0.1
R2: 192.168.0.0
Internet

Universidad de Granada

32



Router 3 → tabla

A → 192.168.0.0 /26

B → 192.168.0.64 /26

R₁

R₁

} Se pueden agrupar con 192.168.0.0 /25

C → 192.168.0.128 /26

R₂

D → 192.168.0.192 /26

R₂

} Se pueden agrupar con 192.168.0.128 /25

Tabla
ABCD 192.168.0.0/24



Tema 2. Capa de red

3. El protocolo IP

En el origen y en cada router se coteja la tabla:

- Dirección de destino (DD): 192.168.0.66
- Para cada entrada (fila en la tabla)
 - DD & Máscara = A
 - ¿A = Dirección de destino?
SI → elegir el "Siguiente Nodo" → consultar TABLA ARP
NO → seguir buscando
 - 192.168.0.66 & /27 =
11000000.10101000.00000000.010**00010** & /27 = 192.168.0.64
➤ ¿192.168.0.64 = 192.168.0.0? NO
 - 192.168.0.66 & /27 =
11000000.10101000.00000000.010**00010** & /27 = 192.168.0.64
➤ ¿192.168.0.64 = 192.168.0.32? NO
 - 192.168.0.66 & /27 =
11000000.10101000.00000000.010**00010** & /27 = 192.168.0.64
➤ ¿192.168.0.64 = 192.168.0.64? SÍ ➔ Siguiente Nodo = 192.168.0.1
 - 192.168.0.66 & /30 =
11000000.10101000.00000000.01000010 & /30 = 192.168.0.64
➤ ¿192.168.0.64 = 150.214.190.0? NO
- 33 ➤ Si hay más de una coincidencia (colisión) se elige la entrada de máscara más restrictiva (+ 1s)

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
192.168.0.32	/27	192.168.0.1
192.168.0.64	/27	192.168.0.1
150.214.190.0	/30	192.168.0.1

Universidad de Granada

33

Tema 2. Capa de red

3. El protocolo IP

➤ Tabla de encaminamiento:

- Problemas:
 - La tabla del ejemplo NO direcciona Internet (ej. www.google.com = 172.194.34.209)
 - La topología implica sólo un camino de salida desde A ➔ ¿necesitamos 4 entradas?

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
192.168.0.32	/27	192.168.0.1
192.168.0.64	/27	192.168.0.1
150.214.190.0	/30	192.168.0.1

!!Usar la entrada por defecto!! ➔ /0

Universidad de Granada

34

Tema 2. Capa de red

3. El protocolo IP

➤ Tabla de encaminamiento:

➤ Problemas:

- La tabla del ejemplo NO dirige Internet (ej. www.google.com = 172.194.34.209)
- La topología implica sólo un camino de salida desde ➤ ¿necesitamos 4 entradas?

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
0.0.0.0	0.0.0.0	192.168.0.1

R1 192.168.0.1 Host C 192.168.0.66

- www.google.com** = 172.194.34.209
- Microsoft Hotmail**, Servidor Webmail 130.206.192.39
- YouTube** 172.194.34.206
- Google**
- Servidor Spotify** 78.31.8.101
- ugr Universidad de Granada**
dns3.ugr.es = 150.214.191.10
pop.ugr.es = 150.214.20.3
- Universidad de Granada**

35

35

Tema 2. Capa de red

3. El protocolo IP

➤ Ejercicio: Diseñar la Tabla de encaminamiento en R2

- Incorporar todas las redes directamente conectadas.
- Incorporar la entrada por defecto
- Añadir todas las entradas adicionales necesarias.

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.32	/27	-
192.168.0.64	/27	-
150.214.190.0	/30	-
0.0.0.0	/0	150.214.190.2
192.168.0.0	/27	192.168.0.33

Host A: Subred = 192.168.0.0

Host B: Subred = 192.168.0.32

Host C: Subred = 192.168.0.64

R1: Subred = 192.168.0.0

R2: Subred = 150.214.190.0

Internet

36

36

Tema 2. Capa de red

3. El protocolo IP

7. Imagine una situación donde hay cinco routers RA-RE. RA, RB y RC se conectan cada uno a una red local A, B y C, siendo cada router única puerta de enlace de cada red. RA, RB y RD están conectados entre sí a través de un switch. RC, RD y RE están conectados entre sí a través de un switch. RE conecta a Internet a través de la puerta de acceso especificada por el ISP. Especifique tablas de encaminamiento en los routers. Asigne a voluntad las direcciones IP e interfaces necesarias.

37

Universidad de Granada

37

Tema 2. Capa de red

3. El protocolo IP

Para facilitar la administración y aumentar la escalabilidad Internet se jerarquiza en **Sistemas Autónomos (SA)**.

- Un **SA** es un conjunto de redes y routers administrados por una autoridad.
- Cada SA informa a los otros SA de las redes accesibles. Existe un router responsable, denominado **router exterior** (R_1, R_2, R_n).
- Cada SA se identifica por un entero de 16 bits (DESDE 2007 ES 32-BITS). Rediris = AS766

38

38

Tema 2. Capa de red

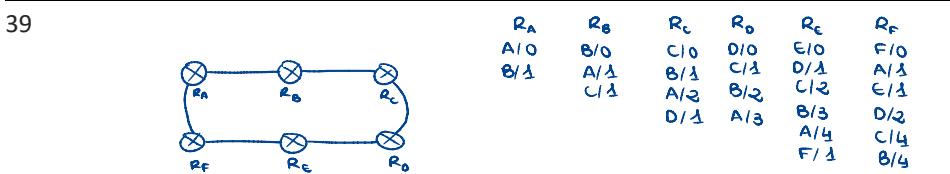
3. El protocolo IP

➤ Intercambio de tablas

- Internet se jerarquiza en **Sistemas Autónomos**
- Se definen 2 niveles de encaminamiento (intercambio de tablas):
 - Algoritmos IGP (el administrador tiene libertad de elección):
RIP, OSPF, HELLO, IS-IS, IGRP, EIGRP
 - Algoritmos EGP (norma única en Internet): **BGP**

39

Universidad de Granada



Tema 2. Capa de red

3. El protocolo IP

• **RIP** ("Routing Information Protocol" RFC 1058, 2453, 4822)

- Protocolo de la capa de aplicación (opera sobre UDP puerto 520)
- Adopta un algoritmo **vector-distancia** (métrica basada en número de saltos)
- Periódicamente (por defecto cada 30 segundos) cada router RIP recibe de todos sus vecinos (dirección multicast 224.0.0.9) los vectores-distancia para todos los posibles destinos
- De entre ellos, para un destino dado, se selecciona como sato siguiente el vecino que anuncie el menor coste, actualizando la métrica para ese destino sumando uno al coste anunciado
- Problema de la convergencia lenta: las malas noticias tardan en propagarse
- Problema de la "cuenta al infinito". → Si se pierde el enlace entre red 1 y R3, R1 buscará cómo llegar, se lo pedirá a R2 el cual le dirá que es a través de R1 y se entra en bucle
- Soluciones:
 - Split horizon
 - Hold down
 - Poison reverse → R1 avisa a R2 de que ya no conecta con la red R2
- Ver > man routed (SO Linux)

40

Universidad de Granada

Tema 2. Capa de red

3. El protocolo IP

→ Es mucho más escalable que RIP

OSPF (RFC 2328)

- Basado en estado del enlace (coste $\alpha 1 / \text{velocidad del enlace}$)
- Permite rutas alternativas y balanceo de carga
- Gestión en base a áreas independientes
- Minimiza difusión mediante routers designados
- Mensajes: hello, database description, link status request/update/ack

Ejemplo para RIP y OSPF → Sirve para determinar los vecinos

41

41



Universidad de Granada

Tema 2. Capa de red

3. El protocolo IP

➤ Formato de datagrama

V	LC	TS	longitud total
0	4	8	16 19 31
identificación	I	desplazamiento	
TTL	protocolo	comprobación	
dirección IP origen			
dirección IP destino			
opciones	relleno		
datos			

Este es el tipo que ver con la fragmentación. Si vale 0, se descarta el paquete. Si se decrementa en 1 u.d. al pasar de un router a otro.

Tiempo de vida

Si vale 0, se descarta el paquete. Se decrementa en 1 u.d. al pasar de un router a otro.

Suma las filas de la cabecera en complemento a 3, de forma que cuando elige un paquete, debería dar resto unos 1...1

Si se quedan bytes vacíos, se rellena hasta que se tenga un múltiplo de 4

42



Universidad de Granada

42

Tema 2. Capa de red

3. El protocolo IP

➤ Formato de datagrama

0	4	8	16	19	31
V	LC	TS	longitud total		
			identificación	I	desplazamiento
		TTL	protocolo	comprobación	
dirección IP origen					
dirección IP destino					
opciones			relleno		
datos					

cabecera

➤ Fragmentación IPv4:

- Tamaño máximo del datagrama: $2^{16}-1 = 65.535$ bytes.
- Es necesario adaptarse a la **MTU** (Maximum Transfer Unit) de cada subred
- El ensamblado sólo se puede hacer en el destino final
- desplazamiento**: offset respecto del comienzo del paquete.
- indicadores (I)**: "Don't Fragment", "More Fragments".

Nivel de enlace	MTU (bytes)
PPP normal	1500
PPP bajo retardo	296
X.25	1600 (RFC 1356)
Frame Relay	1600 (normalmente)
Ethernet DIX	1500
Ethernet LLC-SNAP	1492
Token Ring 4 Mb/s	4440 (THT 8ms)
Classical IP over ATM	9180

43

43

Tema 2. Capa de red

3. El protocolo IP

➤ Fragmentación IPv4:

red Ethernet MTU=1.500

red 1

red 2

cabecera 20 bytes identificación = n datos 4.180 bytes

cabecera 20 bytes identificación = n offset = 0 datos 1.480 bytes

cabecera 20 bytes identificación = n offset = 1.480 datos 1.480 bytes

cabecera 20 bytes identificación = n offset = 2.960 datos 1.220 bytes

Pueden seguir rutas distintas

fragmento 1, MF =1 Despl.: Ø (0 ... 1479)

fragmento 2, MF =1 Despl.: 1480 (1480 ... 2959)

fragmento 3, MF =0 Despl.: 2960

44

44

¿Y si MTU = 1400?

1º	MF = 1	Desp: 0	1380
2º	MF = 1	Desp: 1380	100

3º	MF = 1	Desp: 1380	1380
4º	MF = 1	Desp: 1380	100



Universidad de Granada

5º	MF = 0	Desp: 2960	1380
----	--------	------------	------

Tema 2. Capa de red

Esquema

1. Funcionalidades

2. Comutación

3. El protocolo IP

4. **Asociación con la capa de enlace: el protocolo ARP**

5. El protocolo ICMP

6. Autoconfiguración de la capa de red (DHCP)

45

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

45

Tema 2. Capa de red

4. Protocolo ARP

➤ Direcciones MAC

- Tras la redirección IP → Enviar a la MAC del siguiente nodo

The diagram illustrates the flow of an ARP request from Host A to Host C. The path goes from Host A to Router R1, then to Router R2, and finally to Host C. The packet is shown at each node, with a green arrow indicating its movement. To the right, a callout shows the internal structure of the network stack. It shows the layers from top to bottom: Capa de Aplicación, Capa de Transporte, Capa de Red, and Red Subyacente. A dashed line connects the 'Capa de Red' and 'Red Subyacente' layers to the 'Subcapa de enlace' layer of the IEEE 802 stack, which includes the Subcapa MAC and Capa Física.

46

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

46

Tema 2. Capa de red

4. Protocolo ARP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

- Direcciones MAC
 - Tras la redirección IP → Enviar a la Medium Access Control (MAC) del siguiente nodo. Se usan en redes Ethernet (cableadas) y WiFi
 - Formato (6 bytes): HH-HH-HH-HH-HH-HH → ej. 00-24-21-A8-F7-6A
 - Son únicas, asignadas por IEEE en lotes de 2^{24} para cada fabricante
 - Dirección de difusión (broadcast) FF-FF-FF-FF-FF-FF
- Protocolo: Address Resolution Protocol (ARP)
 - Obtener MAC a partir de IP: (a) y (b)
- Protocolo: Reverse ARP (RARP)
 - Obtener IP a partir de MAC: (a) y (c)

(a)

(b)

(c)

47

Universidad de Granada

47

Tema 2. Capa de red

4. Protocolo ARP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

- Formato ARP:

0	8	16	31
Htipo		Ptipo	
Hlen	Plen	Operación	
Hemisor (bytes 0-3)			
Hemisor (bytes 4-5)		Pemisor (bytes 0-1)	
Pemisor (bytes 2-3)		Hsol (bytes 0-1)	
		Hsol (bytes 2-5)	
		Psol (bytes 0-3)	

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: arp

No.	Time	Source	Destination	Protocol	Info
6	0.106885	AsustekC_a2:68:bd	Broadcast	ARP	who has 150.214.191.10? Tel

```

Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: AsustekC_a2:68:bd (90:e6:ba:a2:68:bd), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  EtherType: ARP (0x0806)
  Address resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
  [Is grat播 (Fwd)]
  Sender MAC address: AsustekC_a2:68:bd (90:e6:ba:a2:68:bd)
  Sender IP address: 150.214.191.178 (150.214.191.178)
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 150.214.191.10 (150.214.191.10)

```

48

Universidad de Granada

48



Tema 2. Capa de red

Esquema

1. Funcionalidades
2. Comutación
3. El protocolo IP
4. Asociación con la capa de enlace: el protocolo ARP
5. **El protocolo ICMP**
6. Autoconfiguración de la capa de red (DHCP)

49



49

Tema 2. Capa de red

5. El protocolo ICMP

➤ ICMP (Internet Control Message Protocol)

- Informa sobre situaciones de error en IP → es un protocolo de señalización
- Suelen ir (excepto eco y solicitudes) hacia el origen del datagrama IP original
- ICMP se encapsula en IP
- Cabecera de 32 bits
 - Tipo (8 bits): tipo de mensaje
 - Código (8 bits): subtipo de mensaje
 - Comprobación (16 bits)

0	8	16
tipo	código	comprobación

50

Campo tipo	Mensaje ICMP
8/0	Solicitud/respuesta de eco (ping)
3	Destino inalcanzable
4	Ralentización del origen
5	Redirecciónamiento
11	Tiempo de vida excedido
12	Problema de parámetros
13/14	Solicitud/respuesta de sello de tiempo
17/18	Solicitud/respuesta de máscara de red

50

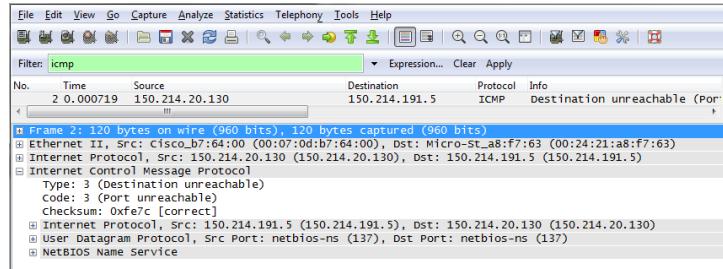


Tema 2. Capa de red

5. El protocolo ICMP

➤ ICMP (Internet Control Message Protocol)

- Informa sobre situaciones de error → señalización
- Hacia el origen del datagrama IP.
- Se encapsula en IP
- Cabecera de 32 bits. Incluye la cabecera del datagrama que ha disparado el mensaje



51

51

Tema 2. Capa de red

Esquema

1. Funcionalidades
2. Comutación
3. El protocolo IP
4. Asociación con la capa de enlace: el protocolo ARP
5. El protocolo ICMP
6. Autoconfiguración de la capa de red (DHCP)
 - ↳ Dynamic host configuration protocol

52

52

Tema 2. Capa de red

6. Autoconfiguración de la capa de red (DHCP)

DHCP (Dynamic Host Configuration Protocol)

Servidor DHCP
147.156.192.5

Para asignar las direcciones se usa DHCP (RFC 2131-3396), protocolo usuario de UDP (**puerto 67**)

- El host (cliente) envía un mensaje broadcast: "DHCP discover"
- El server DHCP responde con un mensaje "DHCP offer"
- El host solicita una dirección IP, mensaje "DHCP request"
- El server DHCP envía la dirección IP: mensaje "DHCP ack"

DHCP

Cliente DHCP
IP: ?

Org: 0.0.0. , puerto = 68
Dest: 255.255.255.255, 67
DHCPOFFER → Te ofrezco esta dirección
SudirIP: 0.0.0.0
ID: 654

Org: 147.156.192.5, 67
Dest: 255.255.255.255, 68
DHCPOFFER → Te ofrezco esta dirección
SudirIP: 147.156.192.10
ID: 654
Tiempo de vida: 3600 s

Org: 0.0.0.68
Dest: 255.255.255.255, 67
DHCPOREQUEST
SudirIP: 147.156.192.10
ID: 655
Tiempo de vida: 3600 s

Org: 147.156.192.5, 67
Dest: 255.255.255.255, 68
DHCPOFFER → El servidor asigna una dirección IP
SudirIP: 147.156.192.10
ID: 655
Tiempo de vida: 3600 s

A la hora hay que volver a pedir la dirección IP

Universidad de Granada

53

DHCP → { IP + Máscara
DNS
Ruta por defecto/pasarela } } Estas son las cosas que se piden con DHCP

Tema 2. Capa de red

6. Autoconfiguración de la capa de red (DHCP)

DHCP

Configuración de un cliente MS Windows:

Wireless Network Connection Properties

Networking tab

Internet Protocol Version 4 (TCP/IPv4) Properties

General tab

Obtain an IP address automatically (radio button selected)

Obtain DNS server address automatically (radio button selected)

Universidad de Granada

54



Tema 2. Capa de red

6. Autoconfiguración de la capa de red (DHCP)

DHCP

Configuración de un cliente Linux (Fedora Core distribution):

```
# Sample /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:CE:63:E3
ONBOOT=yes
TYPE=Ethernet
```

Configuración de un servidor de Linux (dhcpd):

```
# Sample /etc/dhcpd.conf
default-lease-time 600;max-lease-time 7200;
option subnet-mask 255.255.255.0; tiempo en el que se mantiene la IP
option broadcast-address 192.168.1.255; máscara de red
option routers 192.168.1.254; dir. difusión
option domain-name-servers 192.168.1.1, 192.168.1.2; DNS
option domain-name "mydomain.org";
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.100;
    range 192.168.1.150 192.168.1.200;
}

# Static IP address assignment
host haagen {
    hardware ethernet 08:00:2b:4c:59:23;
    fixed-address 192.168.1.222;
}
```

Universidad de Granada