

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

© 2024



1



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)

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

2



2



Tema 2. Capa de red

Objetivos del tema

Comprender las funcionalidades y servicios de la capa de red :

- Concepto de conmutación 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



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**, 5ª Edición, Addison-Wesley, 2010, ISBN: 9780136079675

4



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



5



Tema 2. Capa de red

1. Funcionalidades

- Funciones y servicios en TCP/IP
 - Encaminamiento
 - Conmutación
 - Interconexión de redes
 - En OSI: control de congestión
- Ejemplos de protocolos de red:
 - X.25 https://es.wikipedia.org/wiki/Norma_X.25
 - IP

6



6



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)

7



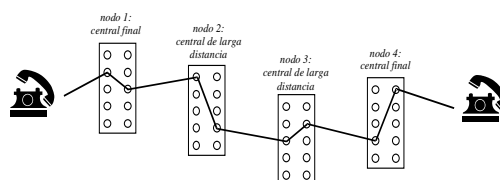
7



Tema 2. Capa de red

2. Conmutación

- Conmutación = acción de establecer o determinar un camino que permita transmitir información extremo a extremo
- Esquemas de conmutación
 - Circuitos
 - Paquetes: datagramas o circuitos virtuales
- Conmutación de circuitos
 - Ej. Teléfono
 - Es un servicio orientado a conexión → exige un establecimiento de conexión previo a la transmisión



- 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



8



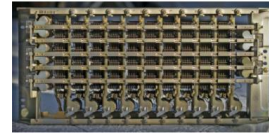
Tema 2. Capa de red

2. Conmutación

➤ Conmutación 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.

9



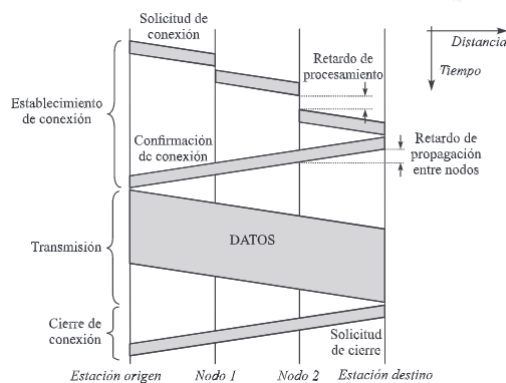
9



Tema 2. Capa de red

2. Conmutación

➤ Conmutación de circuitos



10



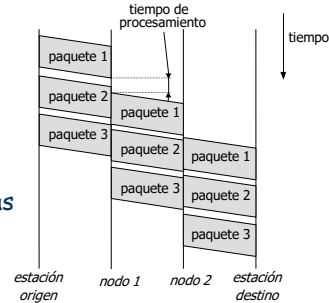
10



2. Conmutación

Conmutación de paquetes:

- Envío en bloques (paquetes)
- Conmutación 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
- Conmutación de paquetes con **circuitos virtuales**:
 - ej. ATM (troncales)
 - Pasos: (i) Conexión, (ii) Transmisión, (iii) Desconexión
 - Recursos no dedicados



2. Conmutación

4. Estime el tiempo involucrado en la transmisión de un mensaje de datos para la técnica de conmutación 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.



Tema 2. Capa de red

2. Conmutación

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

Para
conmutación
de paquetes,
¿es válida la
respuesta de
ChatGPT?

13

Fórmula de tiempo total involucrado:

- Fragmentación del mensaje: Primero, el mensaje total M se fragmenta en paquetes de tamaño $P - H$ (donde H es la cabecera).
 - El número de paquetes sería aproximadamente $\lceil M / (P - H) \rceil$.
- Tiempo de transmisión por paquete: Cada paquete tendrá un tiempo de transmisión en cada enlace de $\frac{P}{V}$ segundos.
- Retardo de propagación: En cada enlace (entre nodos), habrá un retardo de propagación de R segundos.
- Procesamiento en cada nodo: En cada nodo intermedio (total N nodos), hay un tiempo de procesamiento D .

Tiempo total estimado:

El tiempo total T sería:

$$T = \left(\frac{M}{P - H} \right) \times \left(\frac{P}{V} + R \right) + N \times D$$

Esto incluye:

- La transmisión de los paquetes a través de los enlaces, considerando el retardo de propagación R y la velocidad de transmisión V .
- El tiempo de procesamiento D en cada nodo intermedio.

13



Tema 2. Capa de red

2. Conmutación

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

Para
conmutación
de circuitos,
¿es válida la
respuesta de
ChatGPT?

14

1. Retardo de propagación total para el establecimiento del circuito:

El circuito debe establecerse entre los nodos antes de que se pueda transmitir el mensaje. Este proceso implica que la señal viaje de extremo a extremo.
El retardo total de propagación para el establecimiento sería:

$$T_{\text{establecimiento}} = (N + 1) \times R$$

Aquí, N es el número de nodos intermedios, y R es el retardo de propagación entre cada par de nodos.

2. Transmisión del mensaje:

Una vez que el circuito está establecido, se transmite el mensaje completo a través del enlace de datos sin dividirlo en paquetes. El tiempo de transmisión del mensaje será:

$$T_{\text{transmisión}} = \frac{M}{V}$$

Donde M es la longitud en bits del mensaje y V es la velocidad de transmisión de los enlaces en bits por segundo (bps).

3. Procesamiento en cada nodo:

Aunque no hay procesamiento de paquetes, puede haber un pequeño tiempo de procesamiento en cada nodo para manejar el paso de datos a través del circuito. Este tiempo sería:

$$T_{\text{procesamiento}} = N \times D$$

Donde D es el tiempo de procesamiento en cada nodo, y N es el número de nodos intermedios.

Tiempo total involucrado:

El tiempo total para la transmisión del mensaje usando conmutación de circuitos sería la suma de los tres componentes:

$$T_{\text{total}} = T_{\text{establecimiento}} + T_{\text{transmisión}} + T_{\text{procesamiento}}$$

Sustituyendo las expresiones:

$$T_{\text{total}} = (N + 1) \times R + \frac{M}{V} + N \times D$$

Este tiempo incluye:

- El retardo de propagación para establecer el circuito.
- El tiempo de transmisión del mensaje a través del circuito.
- El tiempo de procesamiento en cada nodo.



14



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)

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

15



15



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 **direccionamiento** 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.

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

16



16



Tema 2. Capa de red

3. El protocolo IP

➤ Direcciones IP:



Microsoft
Hotmail

Servidor
Webmail

130.206.192.39



Google
España

www.google.com =
172.194.34.209



Servidor
Spotify

78.31.8.101



www.youtube.com
172.194.34.206




ugr Universidad
de Granada

www.ugr.es =
150.214.204.25
dns3.ugr.es =
150.214.191.10
pop.ugr.es = 150.214.20.3

17



17



Tema 2. Capa de red

3. El protocolo IP

➤ Internet adopta un **direccionamiento jerárquico** para simplificar el routing.

➤ Las direcciones IP (32 bits) tienen dos partes bien diferenciadas:
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:

200.27.4.112

&

255.255.255.0

= 11001000.00011011.00000100.01110000


= 11111111.11111111.11111111.00000000

= 11001000.00011011.00000100.00000000

Subred → 200.27.4.0

18

18



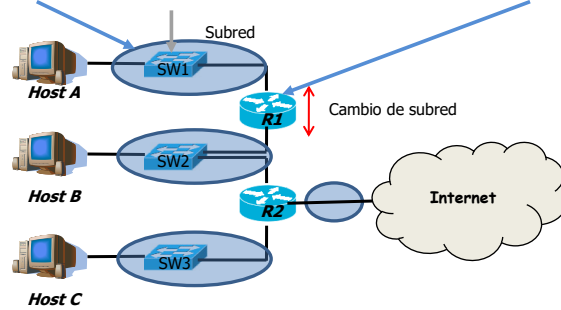
18



Tema 2. Capa de red

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."



19

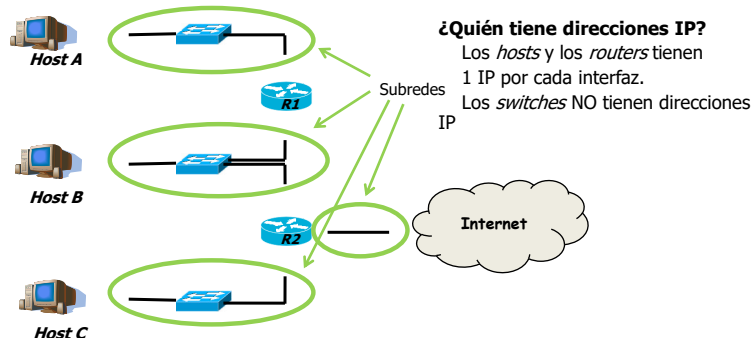
19



Tema 2. Capa de red

3. El protocolo IP

- ¿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."



20

20



Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

- ¿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)

21



21

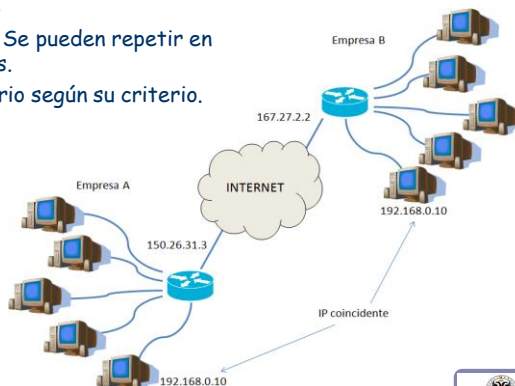


Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

- Direcciones **públicas**
 - Cada dirección se asigna a sólo 1 dispositivo en Internet.
Se asignan centralizadamente
- Direcciones **privadas**
 - Sólo en intranets. Se pueden repetir en distintas intranets.
Las asigna el usuario según su criterio.



22



22



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)
Clase B	1 0	red (14 bits)	host (16 bits)
Clase C	1 1 0	red (21 bits)	host (8 bits)
Clase D	1 1 1 0	dirección grupo <i>multicast</i> (28 bits)	
Clase E	1 1 1 1 0	uso futuro	

23



23



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 <i>hosts</i>
B →	128.0.0.0-191.255.255.255	⇒	16.384 redes x 65.536 <i>hosts</i>
C →	192.0.0.0-223.255.255.255	⇒	2.097.152 redes x 256 <i>hosts</i>
D →	224.0.0.0-239.255.255.255	⇒	para <i>multicast</i>
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*)

Para evitar ambigüedades el identificador 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)

24



24



Tema 2. Capa de red

3. El protocolo IP

- Los bloques de direcciones IPv4 se "agotaron" ya (Nov. 2019)!!!
- Sólo quedan disponibles bloques /24 (256 direcciones) a /32 (1 dirección).
- Se van recopilando direcciones de sitios obsoletos, empresas que hayan desaparecido, proyectos terminados, hosting que ya no está en uso...

IPv6

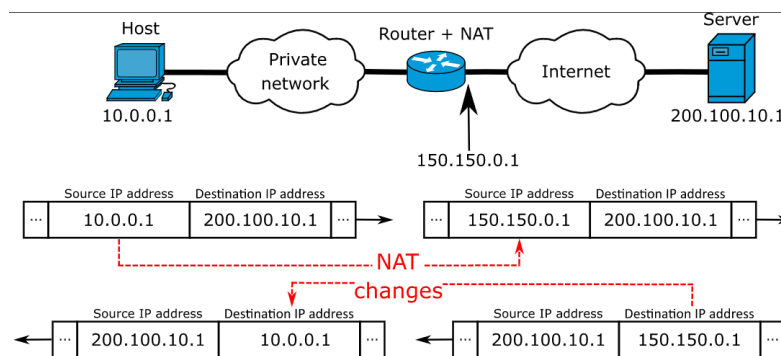
- IPv6 usa un esquema de direccionamiento de 128 bits.
- Notación hexadecimal. 8 grupos de 4 dígitos, separados por ":".
- Cada dígito hexadecimal corresponde a 4 dígitos en binario (4 bits).
- Rango: 0000:0000:0000:0000:0000:0000:0000:0000 a FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
- 340.282.366.920.938.463.463.374.607.431.768.211.456 (340 sextillones) direcciones diferentes.
- Compatible con IPv4.



Tema 2. Capa de red

3. El protocolo IP

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



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



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.

27



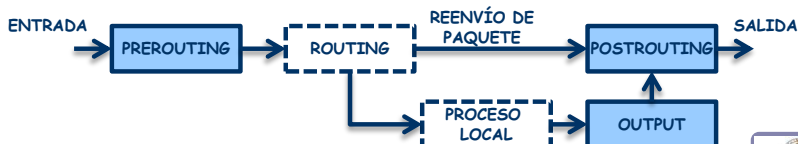
27



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*)



28



28



Tema 2. Capa de red

3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

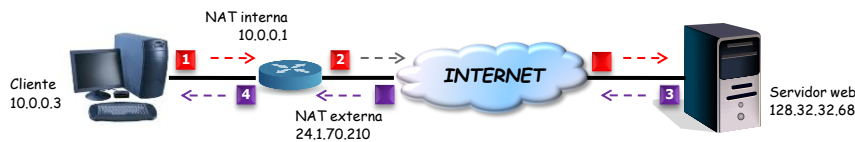
29

PROTO	TCF
SADDR	10.0.0.3
DADDR	128.32.32.68
SPORT	1049
DPORT	80
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).

PROTO	TCF
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.



PROTO	TCF
SADDR	128.32.32.68
DADDR	10.0.0.3
SPORT	80
DPORT	1049
FLAGS	SYN, ACK
CKSUM	0x7841

4. 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.

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

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

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

29



Tema 2. Capa de red

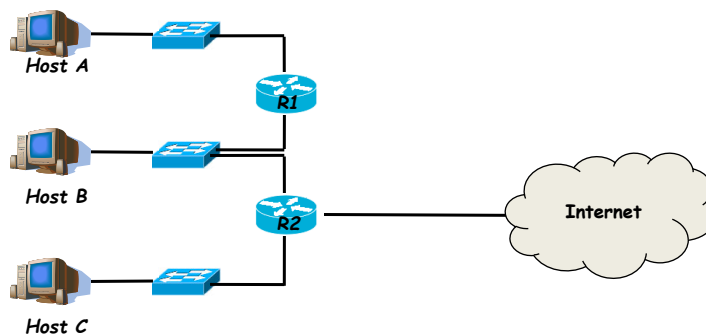
3. El protocolo IP

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

30

➤ Ejercicio: Asignar direcciones

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



30

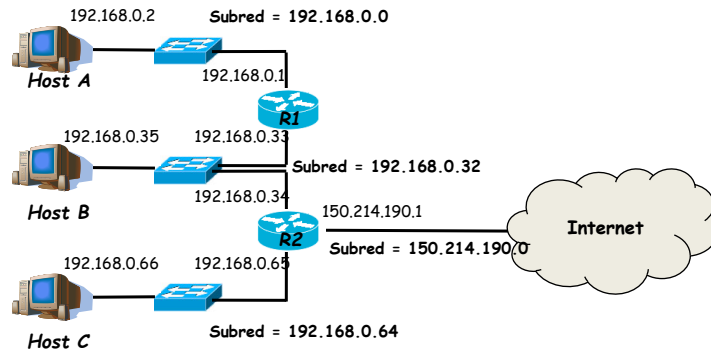


Tema 2. Capa de red

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)



31

31

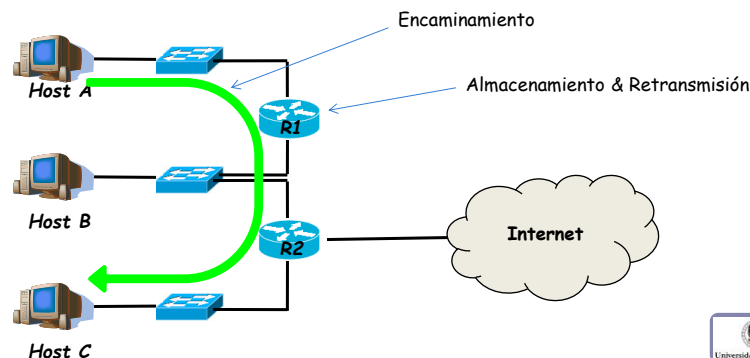


Tema 2. Capa de red

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**.



32

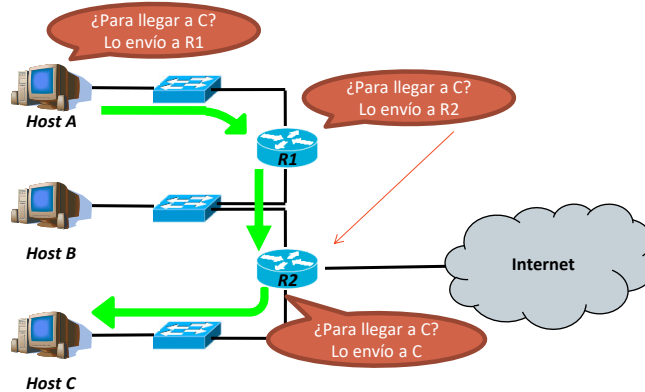
32



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



33

33



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

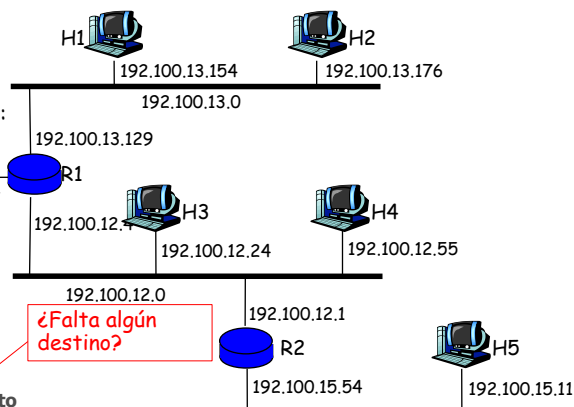


Tabla de R1, * = routing directo

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
2	192.100.12.0	*	255.255.255.0	-	eth0
.	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

192.100.15.0

- ❑ En caso de conflicto se elige la ruta con máscara más larga

34

34



Tema 2. Capa de red

3. El protocolo IP

- 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 $IP_i = D_i$ 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.

35



35

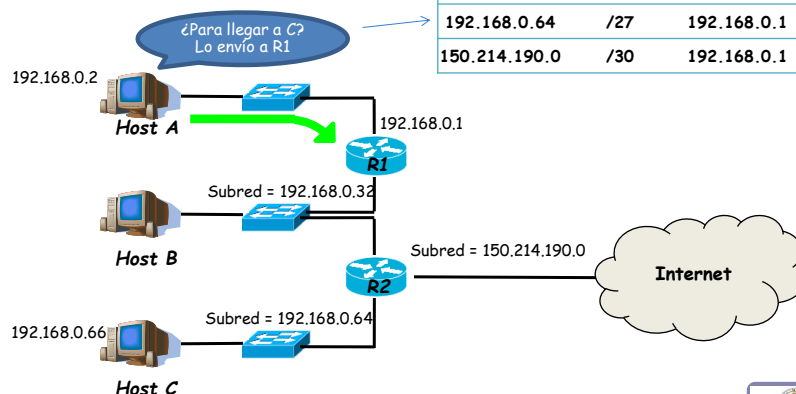


Tema 2. Capa de red

3. El protocolo IP

- 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



36



36



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

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

- $192.168.0.66 \ \& \ /27 \ =$
 $11000000.10101000.00000000.01000010 \ \& \ /27 \ = 192.168.0.64$
 - ¿192.168.0.64 = 192.168.0.0? NO
- $192.168.0.66 \ \& \ /27 \ =$
 $11000000.10101000.00000000.01000010 \ \& \ /27 \ = 192.168.0.64$
 - ¿192.168.0.64 = 192.168.0.32? NO
- $192.168.0.66 \ \& \ /27 \ =$
 $11000000.10101000.00000000.01000010 \ \& \ /27 \ = 192.168.0.64$
 - ¿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

- 37 ➤ Si hay más de una coincidencia (colisión) se elige la entrada de máscara más restrictiva (+ 1s)



37



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

38



38



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 → ¿necesitamos 4 entradas?



39

39

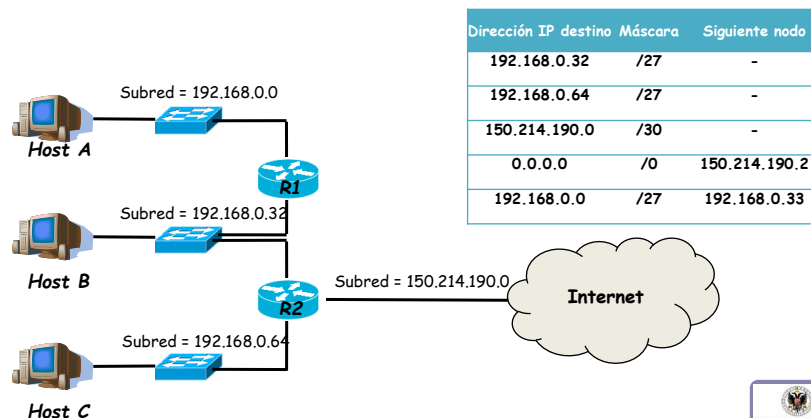


Tema 2. Capa de red

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.



40

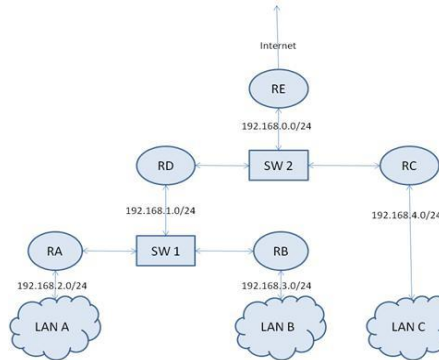
40



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.



41

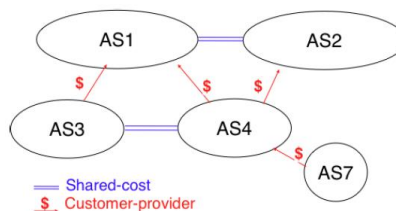
41



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** (R1, R2, Rn).
- Cada SA se identifica por un entero de 16 bits (DESDE 2007 ES 32-BITS). Rediris = AS766



42

42

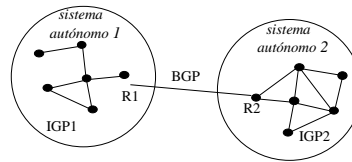


Tema 2. Capa de red

3. El protocolo IP

➤ Intercambio de tablas

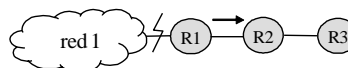
- Internet se jerarquiza en **Sistemas Autónomos**
- Se definen 2 niveles de encaminamiento (intercambio de tablas):
 - Algoritmos IGP (el administrador tiene libertad de elección):
RIP, OSPF, HELLO, IS-IS, IGRP, EIGRP
 - Algoritmos EGP (norma única en Internet): **BGP**



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".
 - Soluciones:
 - Split horizon*
 - Hold down*
 - Poison reverse*
 - Ver > man routed (SO Linux)





Tema 2. Capa de red

3. El protocolo IP

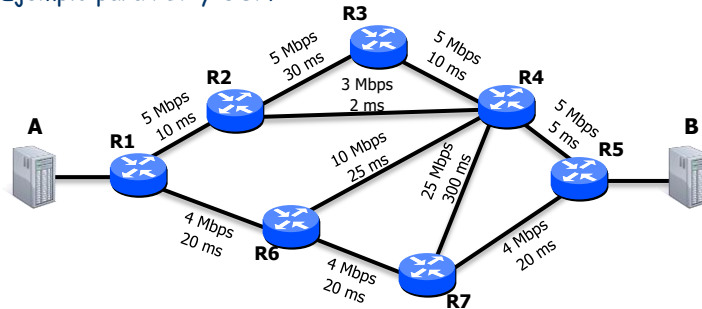


OSPF (RFC 2328)

- Basado en estado del enlace ($\text{coste} \propto 1 / \text{velocidad del enlace}$)
- 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



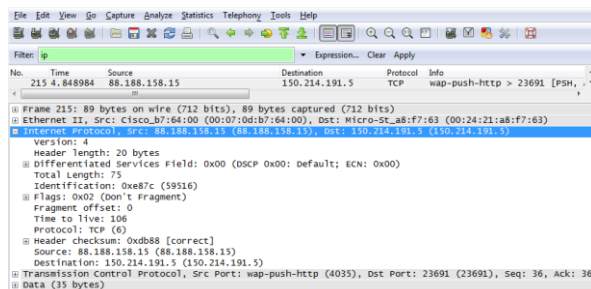
Tema 2. Capa de red

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

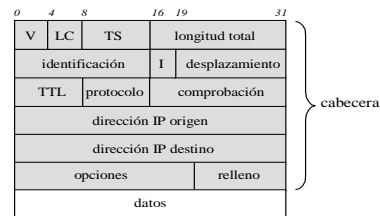




Tema 2. Capa de red

3. El protocolo IP

➤ Formato de datagrama



➤ 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".

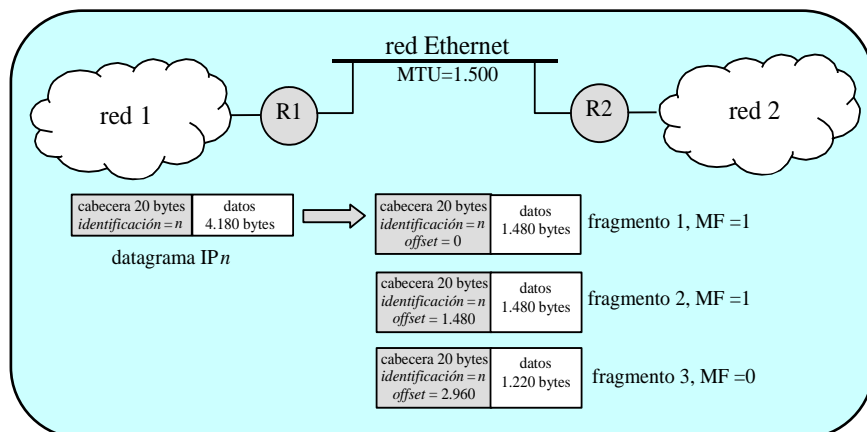
Nivel de enlace	MTU (bytes)
PPP normal	1500
PPP bajo retardo	296
X.25 (RFC 1356)	1600
Frame Relay (normalmente)	1600
Ethernet DIX	1500
Ethernet LLC-SNAP	1492
Token Ring 4 Mb/s (THRT 8ms)	4440
Classical IP over ATM	9180



Tema 2. Capa de red

3. El protocolo IP

➤ Fragmentación IPv4:



TSTC

Tema 2. Capa de red

3. El protocolo IP

Diferencias entre IPv4 e IPv6:

Característica	IPv4	IPv6
Longitud de la dirección	32 bits	128 bits
Espacio de direcciones	~4,3 mil millones	340 undecillones (casi ilimitado)
Formato	Decimal (ej. 192.168.0.1)	Hexadecimal (ej. 2001:0db8::8a2e:0370:7334)
Configuración	Manual o DHCP	Autoconfiguración sin estado (SLAAC)
Seguridad	Opcional (IPsec)	IPsec obligatorio
Fragmentación	Los routers pueden fragmentar	Solo el dispositivo emisor fragmenta
Encabezado de paquetes	Complejo y variable	Simplificado y fijo
QoS	Limitado (TOS)	Optimizado (Flow Label)
Compatibilidad	Amplia, pero limitado por direcciones	No compatible directamente con IPv4
Optimización para móviles	Menos eficiente	Mejor rendimiento en redes móviles

TSTC

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)

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

50

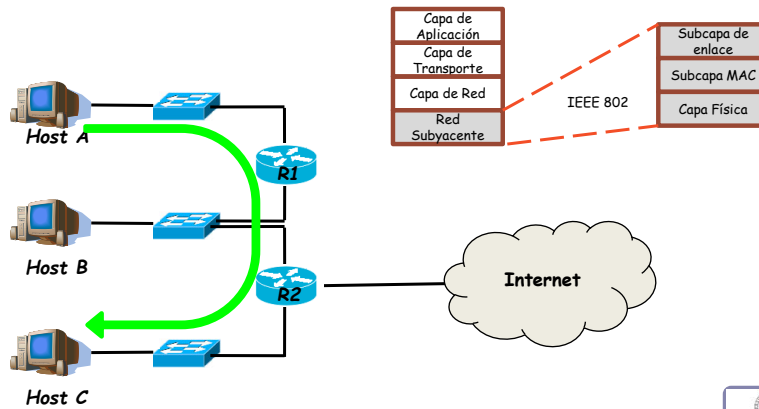




Tema 2. Capa de red

4. Protocolo ARP

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



51



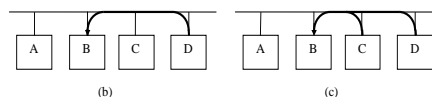
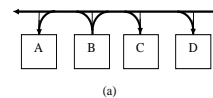
51



Tema 2. Capa de red

4. Protocolo ARP

- 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)



52



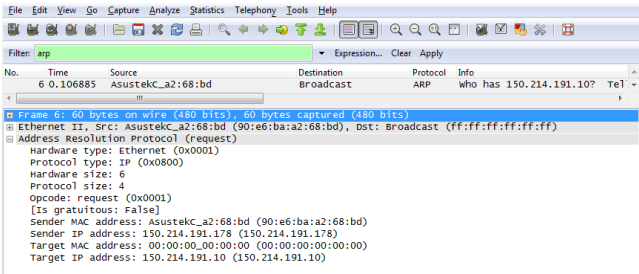
52



4. Protocolo ARP

➤ 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)							



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. 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)
- Mensajes ICMP:

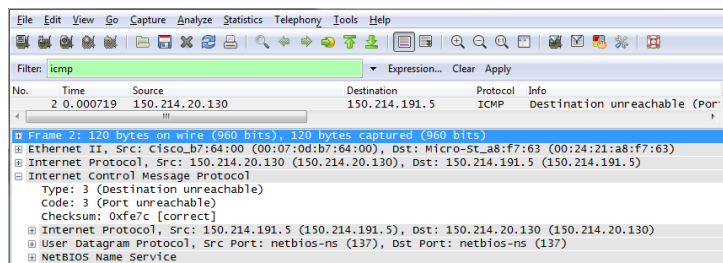
Campo tipo	Mensaje ICMP
8/0	Solicitud/respuesta de eco (ping)
3	Destino inalcanzable
4	Ralentización del origen
5	Redireccionamiento
11	Tiempo de vida excedido
12	Problema de parámetros
13/14	Solicitud/respuesta de sello de tiempo
17/18	Solicitud/respuesta de máscara de red

0	8	16
tipo	código	comprobación



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



The image shows a Wireshark packet capture. The filter is set to 'icmp'. The packet list shows a packet from 150.214.20.130 to 150.214.191.5, protocol ICMP, with info 'Destination unreachable (Port unreachable)'. The packet details pane shows the following structure:

- Frame 2: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface
- Ethernet II, Src: Cisco_b7:64:00 (00:07:0d:b7:64:00), Dst: Micro-St_a8:f7:63 (00:24:21:a8:f7:63)
- Internet Protocol, Src: 150.214.20.130 (150.214.20.130), Dst: 150.214.191.5 (150.214.191.5)
- Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 3 (Port unreachable)
 - Checksum: 0xf7e7 (correct)
 - Internet Protocol, Src: 150.214.191.5 (150.214.191.5), Dst: 150.214.20.130 (150.214.20.130)
 - User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
 - NetBIOS Name Service



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)**

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

57



57



Tema 2. Capa de red

6. Autoconfiguración de la capa de red (DHCP)

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"

Org: 0.0.0.0 , puerto = 68
Dest: 255.255.255.255, 67
DHCPDISCOVER
SudirIP: 0.0.0.0
ID: 654

Org: 147.156.192.5, 67
Dest: 255.255.255.255, 68
DHCPOFFER
SudirIP: 147.156.192.10
ID: 654
Tiempo de vida: 3600 s

Org: 0.0.0.0, 68
Dest: 255.255.255.255, 67
DHCPREQUEST
SudirIP: 147.156.192.10
ID: 655
Tiempo de vida: 3600 s

Org: 147.156.192.5, 67
Dest: 255.255.255.255, 68
DHCPACK
SudirIP: 147.156.192.10
ID: 655
Tiempo de vida: 3600 s



Cliente DHCP
IP: ?

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz



58

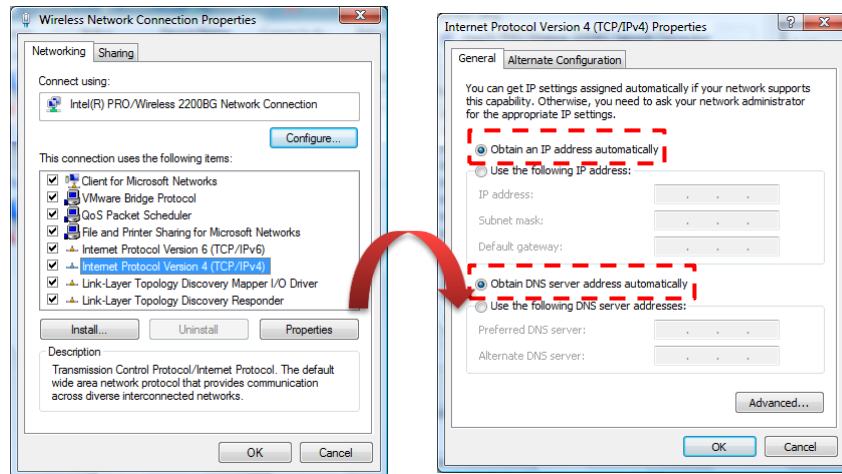


Tema 2. Capa de red

6. Autoconfiguración de la capa de red (DHCP)

DHCP

Configuración de un cliente MS Windows:



Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz



59



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;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
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;
}
```



Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2024 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

60