

Práctica 3

5. Cuestiones a realizar

5.1 PROTOCOLO TCP

5.1.1 Utiliza el programa Rexec para ejecutar comandos UNIX en la máquina Linux 2 172.20.43.232.

Con el monitor de red, analiza y estudia la secuencia de paquetes TCP que se desencadenan. Comprueba que las secuencias de conexión y desconexión TCP que aparecen son las comentadas en el apartado 2.2 del documento de la práctica.

Determina cuál es el valor de MSS que se negocia en los paquetes TCP SYN

Rexec (Ejecución Remota de Comandos) Vr.1.1

Dpto. Ingeniería de Sistemas y Comunicaciones
Sistemas de Transporte de Datos

Variables TCP/IP

Dirección IP local: 192.168.222.1 Puerto local: 56536
Estado: Predeterminado. Cerrado Puerto del Servidor: 512

Parámetros

Usuario: pc02 Contraseña: #####
Servidor: 172.20.43.232 Comando: pwd

Ejecutar Salir

Servidor REXEC en TCP port 512
/home/pc02

ip.addr == 172.20.43.232

No.	Time	Source	Destination	Protocol	Length	Info
13	1.100581	172.20.43.199	172.20.43.232	TCP	66	56563 → 512 [SYN] Seq=2351928862 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	1.102002	172.20.43.232	172.20.43.199	TCP	66	512 → 56563 [SYN, ACK] Seq=42842340 Ack=2351928863 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=4
15	1.102070	172.20.43.199	172.20.43.232	TCP	54	56563 → 512 [ACK] Seq=2351928863 Ack=42842341 Win=131328 Len=0
16	1.103338	172.20.43.199	172.20.43.232	EXEC	70	Session Establishment
17	1.104521	172.20.43.232	172.20.43.199	TCP	60	512 → 56563 [ACK] Seq=42842341 Ack=2351928879 Win=14600 Len=0
18	1.105807	172.20.43.232	172.20.43.199	EXEC	85	Username:pc02 Server -> Client Data
20	1.160368	172.20.43.199	172.20.43.232	TCP	54	56563 → 512 [ACK] Seq=2351928879 Ack=42842372 Win=131328 Len=0
21	1.231795	172.20.43.232	172.20.43.199	EXEC	65	Username:pc02 Server -> Client Data
22	1.232554	172.20.43.232	172.20.43.199	TCP	60	512 → 56563 [FIN, ACK] Seq=42842383 Ack=2351928879 Win=14600 Len=0
23	1.232586	172.20.43.199	172.20.43.232	TCP	54	56563 → 512 [ACK] Seq=2351928879 Ack=42842384 Win=131328 Len=0
24	1.233135	172.20.43.199	172.20.43.232	TCP	54	56563 → 512 [FIN, ACK] Seq=2351928879 Ack=42842384 Win=131328 Len=0
25	1.234160	172.20.43.232	172.20.43.199	TCP	60	512 → 56563 [ACK] Seq=42842384 Ack=2351928880 Win=14600 Len=0

Proceso de conexión:

```
199 (56563) -> 232 (512) | SYN [Seq=2351928862]
232 (512)    -> 199 (56563) | SYN/ACK [Seq=42842340; ACK= Seq(-1) + 1]
199 (56563) -> 232 (512) | ACK [Seq=ACK(-1); ACK= Seq(-1) + 1]
```

Proceso de desconexión:

```
232 (512)    -> 199 (56563) | FIN/ACK [Seq=42842382; ACK= Seq(-1) + Data]
```

/* Mismo origen, distinto, seq y ack

```
199 (56563) -> 232 (512) | ACK [Seq=ACK(-1); ACK= Seq(-1) + 1]
199 (56563) -> 232 (512) | FIN/ACK [Seq=ACK(-1); ACK= Seq(-1) + 1]
*/
```

```
232 (512)    -> 199 (56563) | ACK [Seq=ACK(-1); ACK= Seq(-1) + 1]
```

El MSS es de 1460 bytes, en este caso ambas máquinas tenían el mismo MTU (1500).

```
▼ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Nc
  > TCP Option - Maximum segment size: 1460 bytes
```

Comprueba también los valores de puertos utilizados (número asignado de puerto cliente y número de puerto utilizado por el servidor), como varían los números de secuencia de byte y de ACK, y los flags activados en las cabeceras TCP.

Los cambios de valor de secuencia y ACK ya están en el apartado anterior.

El servidor utiliza el puerto especificado para el protocolo UTC en la herramienta rexec (512), la máquina origen utiliza el puerto 56563.

Los flags varían dependiendo del propósito del paquete enviado:

En los paquetes con propósito de sincronización tienen el bit Syn a 1.

```
▼ Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...0 = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
```

Los paquetes TCP de confirmación aparecen con el flag Acknowledgment a 1 y poseen un Acknowledgment Number.

```

Acknowledgment Number: 42842341
0101 .... = Header Length: 20 bytes (5)
▼ Flags: 0x010 (ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set

```

Aquellos destinados a cerrar las conexiones tienen el bit Fin a 1, en la misma captura se puede ver que más de una flag puede ser activada (siempre que tenga un sentido lógico en la comunicación).

```

▼ Flags: 0x011 (FIN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  > .... .... ...1 = Fin: Set

```

Analiza los valores de las ventanas de receptor anunciadas. ¿Son iguales en el cliente y en el servidor? ¿Cuál es más grande y por qué piensas que son diferentes?

La ventana de mi equipo es 64240, mientras la del equipo con el que intercambio paquetes es de 14600. Para recibir correctamente los paquetes mi ventana debe ser mayor a la del servidor para, en caso de error, poder almacenar en mi buffer los paquetes que sigo recibiendo hasta recibir de nuevo el paquete que causó error en un primer lugar. Por norma general, cuanto mayor es la ventana del emisor más es desaprovechado el medio físico en estos casos.

```

Window: 64240
[Calculated window size: 64240]
Checksum: 0xaffe [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0

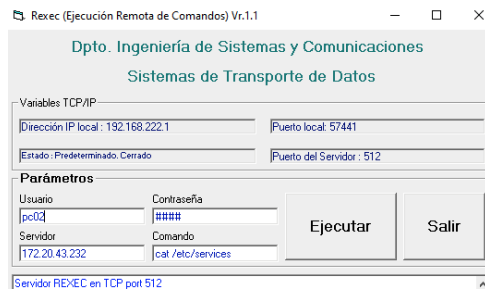
```

```

Window: 14600
[Calculated window size: 14600]
Checksum: 0xc971 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0

```

5.1.2 Utiliza el programa Rexec para ejecutar el comando 'cat /etc/services' en la máquina Linux 2 172.20.43.232.



La información recibida es de varios miles de bytes y se enviará en paquetes TCP de gran tamaño. ¿ Fragmenta el protocolo IP estos paquetes TCP grandes ? ¿ Por qué no ?

El protocolo Ip no se encarga de la fragmentación de paquete TCP, es más, los paquetes TCP colocan el bit DF a 1 en su cabecera Ip. La “fragmentación” de estos paquetes depende del MSS. El MSS es calculado restando al segmento físico con menos MTU el peso de la cabecera IP y TCP. En el proceso de sincronización ambas máquinas comparten su MTU para poder utilizar la menor de ellas para el MSS de la comunicación. En el caso de que la necesidad de una fragmentación ocurra en un segmento físico intermedio, como la cabecera Ip de estos paquetes indica que no deben ser fragmentados se devuelve a la máquina origen un error ICMP fragmentation is needed y es la máquina origen la que fragmenta todos los paquetes que se enviarán a partir de ese momento para que sus paquetes puedan ser enrutados sin necesidad de ser fragmentados en segmentos intermedios, lo que ralentizará el intercambio de información.

5.1.3 Norma RFC 1191

Descarga de los materiales de la práctica 3 en MoodleUA el archivo ‘rfc1191.txt’ en el escritorio de tu PC (C:\Users\EPS\Desktop).

En una ventana de comandos en línea (con permisos de administrador) y dentro del directorio C:\Users\EPS\Desktop emplea el programa ftp para enviar el fichero rfc1191.txt al servidor Linux 3 172.20.41.243. Previamente, inicia el monitor de red para capturar toda la secuencia de paquetes intercambiados con el PC del alumno.

Para realizar la transferencia del archivo se empleará la siguiente secuencia de comandos:

C:\Users\EPS\route delete 0.0.0.0

C:\ Users\EPS\ipconfig /release

C:\ Users\EPS\ipconfig /renew

C:\pracredes

C:\Users\EPS\ftp 172.20.41.243

```
PS C:\Users\EPS\Desktop> ftp 172.20.41.243
Conectado a 172.20.41.243.
220 bftpd 4.2 at 172.20.41.243 ready.
503 USER expected.
Usuario (172.20.41.243:(none)): pc01
331 Password please.
Contraseña:
PS C:\Users\EPS\Desktop> ftp 172.20.41.243
Conectado a 172.20.41.243.
220 bftpd 4.2 at 172.20.41.243 ready.
503 USER expected.
Usuario (172.20.41.243:(none)): pc02
331 Password please.
Contraseña:
230 User logged in.
ftp> rename rfc1191.txt old.txt
350 File exists, ready for destination name
250 OK
ftp> put rfc1191.txt
200 PORT 172.20.43.199:49251 OK
150 BINARY data connection established.
226 File transmission successful.
ftp: 11453 bytes enviados en 21.38segundos 0.54a KB/s.
ftp> quit
221 See you later...
```

Determina con el monitor de red qué valor de MSS se ha negociado en la conexión TCP

```
Options: (12 bytes), Maximum segment size, No-Options
> TCP Option - Maximum segment size: 1460 bytes
> TCP Option - No-Operation (NOP)
> TCP Option - Window scale: 0 (multiply by 1)
> TCP Option - No-Operation (NOP)
> TCP Option - No-Operation (NOP)
> TCP Option - SACK permitted
```

El MSS acordado ha sido de 1460 bytes.

¿Aparecen paquetes ICMP fragmentation needed and the bit don't fragment was set? ¿Quién envía el mensaje ICMP de error?

El Router 1 (10.4.2.5) envía varios errores ICMP Fragmentation needed. El MTU de R1 será menor que el MTU de las máquinas que establecen la conexión.

¿Cómo afecta este mensaje ICMP al tamaño de los paquetes TCP intercambiados entre tu PC y el equipo Linux 3 (172.20.41.243)?

Desde ese momento los paquetes TCP tienen un MSS de (MTU - Cab. TCP - Cab. Ip)
 $600 - 20 - 20 = 560$

```
MTU of next hop: 600
> Internet Protocol Version 4, Src: 172.20.43.199,
  Transmission Control Protocol, Src Port: 49251, I
```

¿Reenvía tu PC algún paquete TCP al equipo Linux 3?


Después de conocer el nuevo MSS, mi PC reenvía los paquetes al equipo Linux 3. En este caso intenta enviar cada paquete con su MSS inicial y luego, al recibir el error ICMP, lo reenvía con el mismo valor de secuencia con el MSS adecuado. La fragmentación no puede ser realizada por el protocolo Ip pues los paquetes del protocolo TCP tienen el bit DF activado.

```
1174 49251 → 33017 [ACK] Seq=4062643428 Ack=2918825536 Win=131328 Len=1120
  70 Destination unreachable (Fragmentation needed)
614 49251 → 33017 [ACK] Seq=4062643428 Ack=2918825536 Win=131328 Len=560
60 33017 → 49251 [ACK] Seq=2918825536 Ack=4062643988 Win=33640 Len=0
1174 49251 → 33017 [ACK] Seq=4062643988 Ack=2918825536 Win=131328 Len=1120
  70 Destination unreachable (Fragmentation needed)
614 49251 → 33017 [ACK] Seq=4062643988 Ack=2918825536 Win=131328 Len=560
```

¿Fragmenta IP algún paquete TCP?

En ningún caso (explicado en la práctica) el protocolo Ip fragmenta paquetes TCP, esto sería ineficiente (congestión en los routers que deben fragmentar y encaminar los paquetes) y es por eso que se utilizan los paquetes ICMP de error. Además, los paquetes enviados tienen el bit DF a 1 por norma del protocolo.

5.1.4 Intentar acceder al servidor Web de la máquina 172.20.43.232 empleando un navegador web (Firefox, Internet Explorer, etc.) con la dirección http://172.20.43.232/. Determinar qué secuencia de paquetes se intercambian en la conexión TCP y por qué.

 https://172.20.43.232

Se producen una serie de intentos por parte de mi máquina para conectar con 172.20.43.232 en el puerto 80 (el puerto http por defecto) pero esta devuelve paquetes TCP con el bit RST a 1, lo que indica un rechazo en la conexión. El equipo Linux 2 puede tener este puerto cerrado.

```
66 54538 → 80 [SYN] Seq=3354746016 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
60 80 → 54538 [RST, ACK] Seq=0 Ack=3354746017 Win=0 Len=0
```

5.2 PROTOCOLO UDP

5.2.1 Utiliza el programa Udp para realizar un envío de datos al puerto 7 (eco) del equipo Linux 2 (172.20.43.232). Para ello basta especificar la dirección IP y el puerto del servidor, colocar algún texto en el panel inferior de la aplicación y pulsar el botón "Envía UDP".

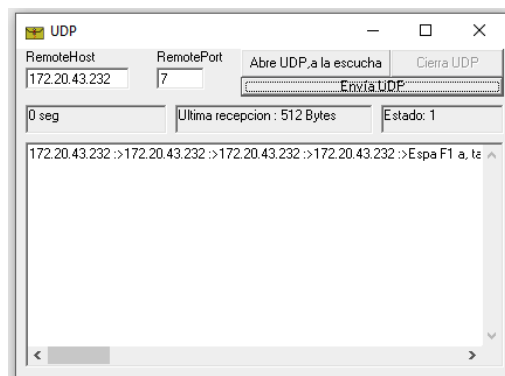
Con el monitor de red analizar la secuencia de paquetes UDP que se desencadenan cuando se envía como datos un texto de menos de 100 caracteres.

En el protocolo UDP no se utilizan paquetes de sincronización a diferencia de en el protocolo TCP. Filtrando por los paquetes eco (puerto utilizado) únicamente se ve un Request desde mi máquina y el correspondiente response de la máquina destino.

Comparar los valores de los campos de tamaño de las cabeceras IP y UDP.

La cabecera Ip ocupa 20 bytes mientras que la cabecera UDP tan solo 8 bytes. Estos están formados por el puerto fuente, el puerto destino, la longitud en bytes del paquete y el SVT(sumo de verificación).

5.2.2 Realizar el mismo procedimiento que en el apartado anterior pero enviando un texto mucho más grande (sobre 2000 bytes) al puerto UDP 7. Para ello puede copiarse parte de algún fichero de texto en el panel inferior de la aplicación Udp



Protocol	Length	Info
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=2960, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=4440, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=5920, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=7400, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=8880, ID=7104) [Reassembled in #88]
IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=10360, ID=7104) [Reassembled in #88]
ECHO	1150	Request
ECHO	554	Response

A diferencia del protocolo TCP, el protocolo UDP no se encarga de la fragmentación de los paquetes que superen el MTU, en este caso es el protocolo Ip el que fragmenta dichos paquetes.

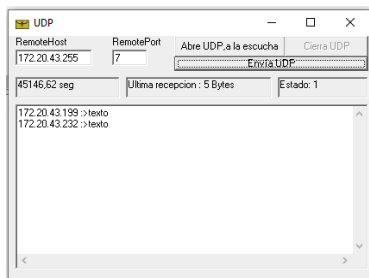
Analiza el valor del campo longitud de la cabecera UDP y del campo longitud total de la cabecera IP en los paquetes enviados y recibidos.

En los paquetes Ip fraccionados no hay cabecera UDP, y el Total Length de la cabecera Ip es de 1500.

En el paquete UDP Echo Request el campo longitud de la cabecera UDP indica el tamaño del paquete UDP completo, en este caso 12956. La longitud total de la cabecera Ip es 1136, donde está incluido los datos del protocolo UDP enviados y ambas cabeceras.

El paquete UDP Echo Response tiene el mismo tamaño indicado en la cabecera UDP y cabecera Ip que en el Echo Request como ocurría en el protocolo ICMP.

5.2.3 Realizar un nuevo envío de un texto corto al puerto UDP 7, pero dirigido a la dirección de broadcast de la red local.



El protocolo UDP es capaz de enviar paquetes a la dirección broadcast y que todos los equipos de la red lo reciban pero para evitar ataques que puedan utilizar esto como una vulnerabilidad el protocolo UDP establece que los equipos no responderán a los mensajes UDP dirigidos a la dirección de difusión. Únicamente contesta un equipo.

5.2.4 Intenta enviar un texto al puerto 80 de la máquina Linux 2 (172.20.43.232) empleando el programa Udp. Determina la secuencia de paquetes que se intercambian entre tu equipo y el equipo 172.20.43.232

172.20.43.199	172.20.43.232	UDP	47 58540 → 80 Len=5
172.20.43.232	172.20.43.199	ICMP	75 Destination unreachable (Port unreachable)

El equipo 172.20.43.232 contesta con un mensaje ICMP de error Port Unreachable, pues se está intentado enviar un paquete UDP al puerto http de la máquina Linux 2 y

este no es accesible. A diferencia de en el protocolo TCP no se recibe un mensaje de error del mismo protocolo, en cambio se apoya en el protocolo ICMP.

5.3 VELOCIDAD DE TRANSMISIÓN

Determina de forma experimental la velocidad de transmisión en la red Ethernet del aula L24 mediante el envío de tramas de un tamaño determinado con la aplicación ping. Para ello emplea el comando:

ping -n 1 -l 1472 direccion_IP_PC_AulaL24

Donde dirección_IP_PC_AulaL24 es la dirección IP de algún PC del aula del laboratorio. La red Ethernet del aula L24 emplea Ethernet 100BaseTX (no así los routers del laboratorio que emplean Ethernet 10BaseT).

```
Haciendo ping a 172.20.43.198 con 1472 bytes de datos:
Respuesta desde 172.20.43.198: bytes=1472 tiempo<1m TTL=128

Estadísticas de ping para 172.20.43.198:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

15	0.847581	172.20.43.199	172.20.43.198	ICMP	1514 Echo (ping) request
16	0.848315	172.20.43.198	172.20.43.199	ICMP	1514 Echo (ping) reply

$V_t = \text{Bits} / \text{TiempoTransmisión (bps)}$

Para conocer cuántos bits se han enviado es necesario saber cuántos bytes ocupa el mensaje ICMP Echo Request enviado, en este caso se sabe gracias a WireShark que las cabeceras y datos ocupan 1514 bytes, a los que hay que sumar los 8 de preámbulo y los 4 de CRC. Esto deja un total de 1526 bytes multiplicado por 2 ya que se necesita el tamaño de petición y respuesta: 3052 bytes. Como se pide en bits 24416 bits.

En cuanto al tiempo de transmisión como se sabe cuando se empezó a transmitir el Echo Request y cuando se recibió el último bit del Echo Reply, se conoce el tiempo total de transmisión de ambos paquetes.

$0.848315 - 0.847581 = 0.000734$ segundos

Sustituyendo en la ecuación original:

$V_t = 24416 \text{ bits} / 0.000734 \text{ s} = 33,264 \text{ Mbps}$

Práctica 4

5.1 NAT

1. Visualización de traducción de paquetes

Inicia el monitor de red en el PC del alumno para capturar el tráfico sin traducir generado por el alumno. Emplea un filtrado por la dirección IP 150.150.150.64+x. Una vez iniciada la captura del tráfico se enviarán paquetes SYN al servicio web del destino 150.150.150.64+x con la aplicación nc.exe.

C:\sw\Netcat\nc -nvw 1 150.150.150.64+x 80

Espera la finalización de la aplicación nc que envía paquetes TCP SYN.
En la conexión SSH al servidor Linux2, ejecuta el comando 'NAT-R1'.

a) Determina cómo se realiza la traducción del paquete SYN en el router R1.

El R1 transforma el puerto origen a el valor más pequeño después de 4096 que no esté en uso, en este caso los puertos 4183, 4104 y 4198.

```
pc01@box:~$ NAT-R1 | grep 150.150.150.65
tcp 172.25.40.31:4183 172.20.43.198:2065 150.150.150.65:80 150.150.150.65:80
```

```
pc01@box:~$ NAT-R1 | grep 150.150.150.65
tcp 172.25.40.31:4104 172.20.43.198:3065 150.150.150.65:80 150.150.150.65:80
```

```
pc01@box:~$ NAT-R1 | grep 150.150.150.65
tcp 172.25.40.31:4198 172.20.43.198:4065 150.150.150.65:80 150.150.150.65:80
```

b) ¿ Cómo se emplea el puerto origen a la hora de realizar la traducción ?

2. Empleo de la misma dirección Outside Global por varios usuarios.

Trabaja en colaboración con un compañero para determinar cómo funciona NAT cuando varios PCs distintos envían paquetes a la misma dirección IP de Internet. Para ello debéis emplear el mismo número de puerto origen a un mismo destino.

Un alumno ejecuta el comando:

C:\sw\Netcat\nc -p 2064+x -nv 150.150.150.64+x 80

Y el otro ejecuta:

C:\sw\Netcat\nc -p 2064+x -nv 150.150.150.64+x 80

Donde x es el mismo valor para ambos alumnos.

a) Determina qué puertos origen emplea el router R1 en la traducción visualizando la información de la tabla de traducciones.

Ambos equipos han utilizado el puerto 2065 para establecer la conexión y ambas les ha sido asignado otro distinto a partir del valor 4096.

```
pc01@box:~$ NAT-R1 | grep 150.150.150.65
tcp 172.25.40.31:4134 172.20.43.198:2065 150.150.150.65:80 150.150.150.65:80
tcp 172.25.40.31:4177 172.20.43.199:2065 150.150.150.65:80 150.150.150.65:80
```

b) ¿ Qué ocurre si el acceso se produce a números de puerto destino diferentes y la misma dirección IP de Internet ? ¿ Cómo se realiza la traducción ?

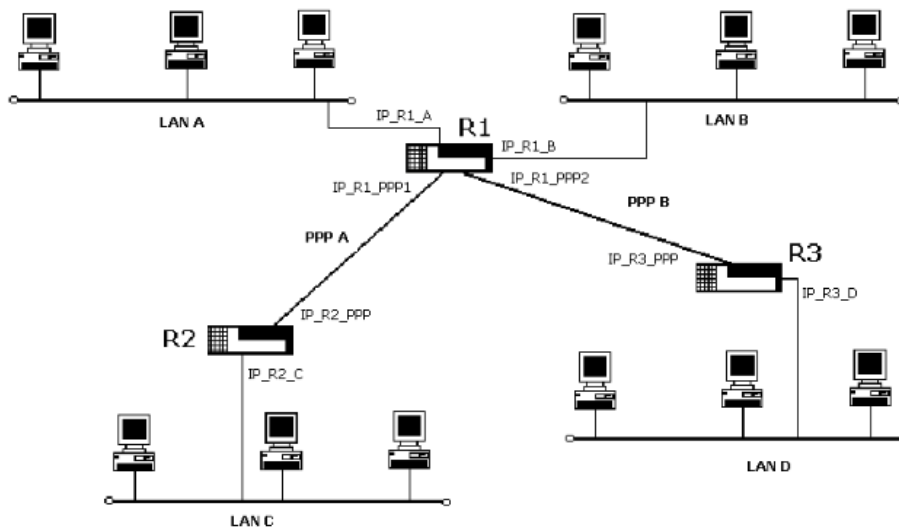
```
pc01@box:~$ NAT-R1 | grep 150.150.150
tcp 172.25.40.31:4140 172.20.43.198:2065 150.150.150.65:80 150.150.150.65:80
tcp 172.25.40.31:4138 172.20.43.199:2065 150.150.150.65:81 150.150.150.65:81
4128 172.20.43.221:2088 150.150.150.88:80 150.150.150.88:80
```

c) ¿ Y si el acceso se produce a números de puerto destino diferentes y diferentes direcciones IP de Internet ? ¿ Cómo se realiza la traducción ?

```
pc01@box:~$ NAT-R1 | grep 150.150.150
tcp 172.25.40.31:4157 172.20.43.198:2065 150.150.150.65:80 150.150.150.65:80
tcp 172.25.40.31:4138 172.20.43.199:2065 150.150.150.66:81 150.150.150.66:81
```

5.2. Construcción de tablas de encaminamiento

Dado el siguiente esquema de red, considera que todo el conjunto es la red 10.1.0.0/16. Establece las subredes necesarias de manera que las redes de difusión (LAN A, B, C y D) tengan una máscara de 24 bits y en las redes punto a punto se emplee la máscara adecuada. Indica así mismo la tabla de encaminamiento de los routers R1, R2 y R3 para que exista conectividad entre todas las redes de difusión y además, que los routers R2 y R3 sólo tengan 4 entradas en sus tablas de encaminamiento.



Para ello completa las siguientes tablas:

DIRECCIONAMIENTO IP			
Red	Dirección/Máscara	Red	Dirección/Máscara
LAN A	10.1.0.0/24	LAN D	10.1.3.0/24
LAN B	10.1.1.0/24	PPP A	10.1.4.0/30
LAN C	10.1.2.0/24	PPP B	10.1.4.4/30
Dirección IP	Valor	Dirección IP	Valor
IP_R1_A	10.1.0.1	IP_R2_C	10.1.2.1
IP_R1_B	10.1.1.1	IP_R2_PPP	10.1.4.2
IP_R1_PPP1	10.1.4.1	IP_R3_D	10.1.3.1

IP_R1_PPP2	10.1.4.5	IP_R3_PPP	10.1.4.6
------------	----------	-----------	----------

TABLA DE ENCAMINAMIENTO DEL ROUTER R1	
Destino/Máscara	Puerta de enlace
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.4.0/30	10.1.4.1
10.1.4.4/30	10.1.4.5
10.1.2.0/24	10.1.4.2
10.1.3.0/24	10.1.4.6

TABLA DE ENCAMINAMIENTO DEL ROUTER R2	
Destino/Máscara	Puerta de enlace
10.1.2.0/24	10.1.2.1
10.1.4.0/30	10.1.4.2
10.1.3.0/24	10.1.4.1
10.1.0.0/23	10.1.4.1

TABLA DE ENCAMINAMIENTO DEL ROUTER R3	
Destino/Máscara	Puerta de enlace
10.1.3.0/24	10.1.3.1
10.1.4.4/30	10.1.4.6
10.1.2.0/24	10.1.4.5
10.1.0.0/23	10.1.4.5

5.3 Protocolo DHCP

1. Liberación de dirección IP

Identifica el paquete DHCP Release que ha transmitido tu PC y analiza el contenido del mensaje con el monitor de red.

a) ¿Cuál es la dirección IP del Servidor DHCP indicado en el contenido del mensaje DHCP (DHCP Server Identifier)?

▼ Option: (54) DHCP Server Identifier (172.25.2.42)

El Servidor DHCP se encuentra en la Ip 172.25.2.42.

b) ¿Coincide la dirección IP del servidor DHCP con la dirección IP a la que se envía el paquete?

Source	Destination	Protocol	Length	Info
172.20.43.198	172.25.2.42	DHCP	342	DHCP Release

Sí, ambas son la misma dirección Ip.

2. Asignación de dirección IP

Identifica el paquete DHCP Discover que ha transmitido tu PC y analiza el contenido del mensaje con el monitor de red.

a) ¿ Se indica a qué servidor DHCP se envía el mensaje ?

No, el mensaje se envía a todos los equipos de la red.

b) ¿ A qué dirección IP y MAC va dirigido el paquete con el mensaje DHCP Discover ?

El mensaje DHCP Discover va dirigido a la dirección Broadcast en ambos casos (255.255.255.255 - ff:ff:ff:ff:ff:ff).

c) ¿ Se solicita en el mensaje DHCP una dirección IP en concreto para el cliente (Requested IP Address)?

▼ Option: (50) Requested IP Address (172.20.43.198)
Length: 4
Requested IP Address: 172.20.43.198

Sí, la 172.20.43.198, que es la Ip estática que recibe el PC01 del aula del laboratorio.

Identifica los paquetes DHCP Offer capturados y analiza el contenido de los mensajes con el monitor de red.

a) ¿ Cuántos mensajes DHCP Offer se capturan ? ¿ Proceden todos de la misma dirección IP ?

En mi experimento solo he capturado un paquete DHCP Offer procedente del Relay Agent (172.20.43.195) conectado al servidor DHCP.

b) ¿ En qué se diferencia el contenido de los mensajes DHCP Offer capturados ?

Solo he capturado un paquete DHCP Offer.

c) ¿ Crees que existe un Relay Agent en la red del laboratorio ? ¿Cuál es su dirección IP?

```
Relay agent IP address: 172.20.43.195
```

Para poder conectar los servidores DHCP de la universidad con el aula se precisa de un Relay Agent.

Identifica los paquetes DHCP Request y DHCP ACK en la captura y analiza el contenido de los mensajes con el monitor de red.

a) ¿ A qué servidor DHCP envía la petición de configuración (DHCP Request) tu PC ?

Al servidor DHCP alojado en 172.25.2.42 mediante el Relay Agent.

Selecciona el paquete DHCP ACK procedente del servidor DHCP indicado en el mensaje DHCP Request. Emplea para ello el dato de la opción DHCP Server Identifier en el mensaje DHCP Request..

b) ¿ Qué dirección IP y máscara de red se asignará a tu PC ?

```
Option: (50) Requested IP Address (172.20.43.198)
```

```
Option: (1) Subnet Mask (255.255.255.192)
```

Los ordenadores del aula de laboratorio tienen una Ip y Máscara de red fija, en este caso, 172.20.43.198 / 255.255.255.192.

c) Indica la dirección IP de la puerta de enlace por defecto que se asignará.

```
▼ Option: (3) Router
  Length: 4
  Router: 172.20.43.195
```

La dirección de la puerta de enlace por defecto será 172.20.43.195, el Relay Agent. ¿?

d) ¿ Por cuánto tiempo será válida la asignación de la dirección IP a tu PC (Lease time) ?

```
IP Address Lease Time: (691200s) 8 days
```

Será válida durante 8 días, cuando acabe este tiempo, el cliente deberá enviar de nuevo un paquete DHCP Request y recibir otro DHCP ACK con un nuevo Lease Time.