Sistemas de Transporte de Datos

Ingeniería Informática (9186)

Ejemplos de controles de prácticas completos (sin solución)

Francisco Andrés Candelas Herías

Santiago Puente Méndez

Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

Sistemas de Transporte de Datos – I. Informática (9186)

Noviembre-Diciembre 2008 - Control de prácticas

Nombre: _____ **DNI:** _____ **Firma:**

Apellidos: _____

- Nota Final = 60% Control de Teoría + 40% Control de Prácticas.
- La entrega de este control implica el uso de una convocatoria.
- Las preguntas respondidas erróneamente no restan puntuación.
- Las preguntas se deben contestar completando los recuadros correspondientes con BOLÍGRAFO. No se evaluará lo escrito fuera de estas opciones.
- Todas las preguntas hacen referencia al esquema de interconexión de redes de la última página. Se puede separar la última página si así resulta más fácil consultar el esquema.
- El tiempo para realizar este examen es de 1 hora y 15 minutos.

Preguntas

1. Dado el esquema de interconexión de redes de la última página, se desea aplicar un control de los paquetes que se pueden enviar por la interfaz de red Frame-Relay del router R5 en base una lista de control de acceso (ACL) que garantice las siguientes condiciones:

a) Todos los equipos de la red 172.16.1.0/24 pueden enviar paquetes IP a la red 10.4.2.0/24.

b) Se permiten los paquetes dirigidos al servicio Web de la dirección 10.4.1.2 y procedentes de cualquier equipo.

c) El router R4 puede acceder a los servicios del servidor RADIUS (puertos UDP 1645 y 1646).

d) Desde el equipo PC4 se puede acceder al servicio SSH (terminal remota segura: puerto 22 de TCP) de todos los equipos de la red 10.4.1.0/24.

e) El resto de paquetes serán descartados y no se podrán enviar por la interfaz.

Considerando que la ACL se asocia al interfaz Frame-Relay de la siguiente forma, se pide especificar en el recuadro los comandos de Cisco IOS que definen la ACL (0,5 puntos).

```
interface Serial0
 ip address 10.1.0.5 255.255.255.248
 ip access-group 104 out
```

2. Completar las tablas de encaminamiento de los routers R1, R3 y R5 del esquema de la última hoja cumpliendo las siguientes condiciones (2,5 puntos).

a) Se debe asegurar la interconexión entre todos los equipos que haya en las redes Ethernet y VPN del esquema, cumpliendo los siguientes apartados.

b) Todo el tráfico destinado a una red local remota se debe encaminar a través del enlace Frame Relay o del RDSI, según corresponda, y no por Internet.

c) Los equipos de las redes locales pueden acceder a Internet por la conexión ADSL más cercana (ADSL-1 o ADSL-2), sin que para ello se envíe tráfico por la red Frame-Relay.

d) En las tablas de encaminamiento, se deben incluir también las redes y destinos conectados directamente, indicando como puerta de enlace la dirección IP de la interfaz local correspondiente junto con la letra “D”.

e) Las direcciones IP de los enlaces WAN y serie sólo deben aparecer en las tablas de los routers que necesariamente lo requieran.

f) Las tablas de encaminamiento deben ser lo más sencillas posible, teniendo en cuenta los aspectos anteriores. Para ello se pueden agrupar subredes cuando sea posible.

g) Para que una entrada se considere correcta, debe tener su destino, máscara y puerta de enlace correctos.

R1: (0,9 puntos)

Destino	Máscara	Puerta Enlace

R3: (0,7 puntos)

Destino	Máscara	Puerta Enlace

R5: (0,9 puntos)

Destino	Máscara	Puerta Enlace

3. Se desea que los servicios de los servidores WWW y VPN-NAS sean accesibles desde equipos de Internet a través del router R1, para lo que se debe configurar su NAT de la siguiente forma:

a) Entrada estática para que el servicio de VPN con protocolos L2TP (1701) se asocie al servidor VPN-NAS.

b) Entrada estática para que el servicio Web con protocolo HTTP (80) se asocie al servidor WEB.

c) También se desea conocer la entrada dinámica que se genera cuando el equipo 60.1.1.1 de Internet accede al servidor WEB usando su puerto cliente 1050.

Completar la siguiente tabla de acuerdo a los casos anteriores (0,5 puntos).

NAT de R1

	Inside global	Inside local	Outside local	Outside global
a)				
b)				
c)				

4. Por aumentar la seguridad del servidor WEB de la red Ethernet 10.5.0.0/16, y para permitir que los equipos de las redes WiFi puedan acceder a ese servidor, se establece la siguiente configuración de NAT en el router R2, usando comandos de Cisco IOS:

```
interface Eth1
 ip address 10.4.1.2 255.255.255.0
 ip nat outside
interface Eth2
 ip address 10.5.0.2 255.255.0.0
 ip nat inside

ip nat pool IPNUEVAS 10.9.0.1 10.9.0.254 netmask 255.255.255.0
ip nat inside source list 101 interface Eth1 overload
ip nat inside source static tcp 10.5.0.8 80 interface Eth1 80
ip nat inside source static tcp 10.5.0.8 443 interface Eth1 443
ip nat outside source static 10.4.2.9 10.7.0.8 extendable
ip nat outside source list 1 pool IPNUEVAS
access-list 1 permit 10.5.0.0 0.0.255.255
access-list 101 deny ip any 10.4.2.8 255.255.255.255
access-list 101 permit any any
```

Atendiendo a la configuración anterior, se debe determinar las direcciones IP que tienen los paquetes IP de los siguientes casos (1,5 puntos):

	Origen	Destino
a) Paquete IP-ICMP enviado desde el equipo PC1 al PC4 cuando pasa por la red 10.4.1.0/24.		
b) Paquete IP-UDP enviado desde el equipo PC1 al servidor RADIUS cuando pasa por la red 10.4.1.0/24.		
c) Paquete IP-TCP enviado desde el equipo PC2 al servicio Web del servidor WEB cuando pasa por la red 10.4.1.0/24.		
d) Mismo paquete del caso anterior (c) cuando pasa por la red 10.5.0.0/16.		
e) Paquete IP-TCP enviado desde el equipo PC1 al destino 10.7.0.8 cuando pasa por la red 10.5.0.0/16.		
f) Mismo paquete del caso anterior (**e**) cuando pasa por la red 10.4.1.0/24.		

5. En la interconexión del esquema, el router R3 está configurado como NAS (Network Address Server) que utiliza el servidor RADIUS con la base de datos de usuarios. La VPN emplea los protocolos L2TP, con autenticación PPP-CHAP.

a) El equipo remoto PC5 inicia una conexión VPN y está se da por válida. Se pide completar la siguiente tabla con la lista de las tramas que se envían y reciben en el router R3 relacionadas con los procesos de autenticación del usuario y de validación en la base de datos, teniendo en cuenta el orden correcto de las mismas **(1 punto)**.

Nº	IP Origen	IP Destino	Protocolo	Tipo-Significado
1				
2				
3				
4				
5				

b) Una vez que el cliente PC5 se ha conectado a la VPN, este equipo envía un paquete TCP al equipo PC4, sin utilizar la seguridad de IPSec. Se pide dibujar el formato de la trama de enlace con el paquete TCP cuando pasa por la red 10.4.1.0/24, detallando lo siguiente **(1 punto)**:

- Las cabeceras de todos los protocolos que contiene en el orden correcto.
- Las direcciones origen y destino de las cabeceras IP.
- Qué protocolos son el portador y el pasajero.

6. Considérese que los routers del esquema tienen EIGRP activado, y que el equipo remoto PC5 realiza una conexión a la VPN. El *delay* asociado a los interfaces de la VPN en el router R3 es 2,000.000µs. ¿Qué mensajes EIGRP que se envían en estos casos (0,5 puntos)?

a) Mensaje que envía R3 a los routers vecinos cuando se acepta la conexión de PC5.

b) Mensaje que envía R2 a los routers vecinos cada pocos segundos para indicar que está activo y para solicitar actualizaciones.

c) Mensaje que envía R3 a los routers vecinos cuando finaliza la conexión de PC5.

	IP Destino	Tipo de mensaje	Información
a)			
b)			
c)			

7. Considérese que en el esquema de redes se configura un túnel de nivel 3 tipo "IP sobre IP" introduciendo los siguientes comandos de Cisco IOS en el router R5:

```
interface Serial0
 ip address 10.1.0.5 255.255.255.248

interface Tunnel0
 tunnel source Serial0
 tunnel destination 10.4.1.1
 tunnel mode gre ip

! Añade una ruta para llegar a 10.4.2.0 por la interfaz del Tunnel0
ip route 10.4.2.0 255.255.255.0 Tunnel0
```

Suponiendo que en equipo PC4 se ejecuta el comando "ping 10.4.2.9 –n 1", resuelve las siguientes cuestiones (1 punto):

a) Indicar la lista completa de equipos por los que pasa el paquete IP-ICMP, en el orden correcto, e incluyendo el origen y el destino.

b) Determinar el número de saltos que contabiliza el paquete IP-ICMP al llegar al destino, y el número de reales que realiza en la red (el túnel cuenta como un salto).

Saltos contabilizados: _____ Saltos reales: _____

c) ¿Qué direcciones tienen los protocolos IP portador e IP pasajero del paquete generado por el "ping" cuando pasa por la red Frame-Relay?

Origen del pasajero: _____ Origen del portador: _____

Destino del pasajero: _____ Destino del portador: _____

8. En la estructura de redes del esquema, se configuran los routers R2 y R3 para que realicen un control de QoS de forma que se limite el ancho de banda para las descargas desde el servidor WEB. Para ello se emplean estos comandos de Cisco IOS:

Router R2:

```
interface Eth1
 ip address 10.4.1.2 255.255.0.0
 ip policy route-map QOSETH1

access-list 110 permit tcp any 10.5.0.0 0.0.255.255 eq 80
access-list 111 permit tcp any 172.16.2.0 0.0.0.255 eq 80
access-list 112 permit tcp any 172.16.1.0 0.0.0.255 eq 80

route-map QOSETH1 permit 10
 match ip address 110
 set ip precedence routine
route-map QOSETH1 permit 20
 match ip address 111
 set ip precedence priority
route-map QOSETH1 permit 30
 match ip address 112
 set ip precedence inmediate
```

Router R3:

```
interface Serial0
 ip address 10.1.0.3 255.255.255.255
 rate-limit output access-group 110 256000 conform-act transmit exceed-act drop
 rate-limit output access-group 111 512000 conform-act transmit exceed-act drop

access-list 110 permit ip host 10.4.1.2 any precedence 0
access-list 111 permit ip host 10.4.1.2 any precedence 1
```

Se pide responder a las siguientes cuestiones (1 punto):

a) ¿Qué tipo de estrategia se utiliza: *Traffic Shaping* (Cisco GTS) o *Traffic Policing* (Cisco CAR)?

b) ¿Qué router realiza una clasificación de tráfico?

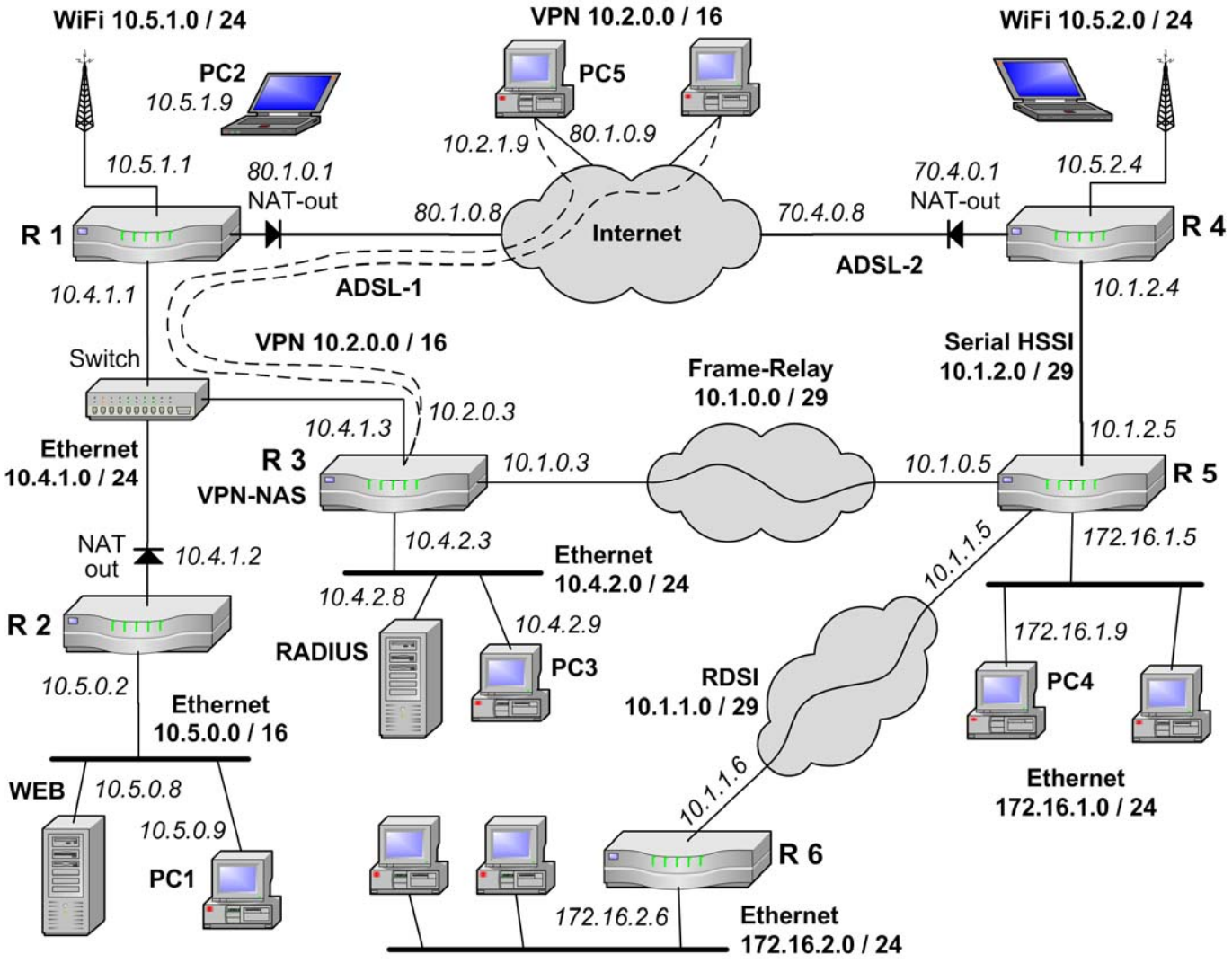
c) ¿A qué red se asigna más ancho de banda para el tráfico Web que procede del servidor WEB y va hacia la red Frame Relay: 10.5..2.0/24, 172.16.1.0/24 o 172.16.2.0/24?

d) ¿A qué velocidad se limita el envío del tráfico desde el servidor WEB hacia la red WiFi 10.5.2.0/24?

e) ¿Qué valor numérico de precedencia tienen los paquetes IP que proceden del servidor WEB y están dirigidos a la red 172.16.2.0/24 cuando pasan por la red Frame Relay?

Explica brevemente qué pasaría si, en vez de a tráfico TCP, se aplicase la configuración anterior a una aplicación de descarga de archivos basada en UDP (0,5 puntos).

Esquema de interconexión de redes para todas las preguntas



Sistemas de Transporte de Datos – I. Informática (9186)

Septiembre 2008 - Control de prácticas

Nombre: _____ **DNI:** _____ **Firma:**

Apellidos: _____

- Nota Final = 60% Control de Teoría + 40% Control de Prácticas.
- La entrega de este control implica el uso de una convocatoria.
- El control se debe completar con bolígrafo.
- Las preguntas respondidas erróneamente no restan puntuación.
- Las preguntas se deben contestar completando los recuadros correspondientes. No se evaluará lo escrito fuera de estas opciones.
- Se puede separar la última página si así resulta más fácil consultar los anexos.
- El tiempo para realizar este examen es de 1 hora y 15 minutos.

Preguntas

1. En el esquema de interconexión de redes mostrado al final del examen se necesita configurar una lista de acceso (ACL) en el router R1 (lista número 100) para bloquear determinado tráfico entre equipos internos y de Internet de forma que se cumpla que:

a) Los equipos de las redes privadas no pueden enviar paquetes a los servidores web públicos cuyos destinos son 213.215.145.96 o alguno de la red 213.248.111.0/24.

b) PC3 no puede recibir paquetes IP a la dirección 50.0.0.4.

c) Todo el tráfico que no coincida con las condiciones a) ni b) si debe ser encaminado por R1.

Especificar los comandos de Cisco IOS que definen la ACL descrita. (0,6 puntos)

2. En el esquema de interconexión de redes mostrado al final del examen se configura HSRP para los routers R7 y R8 en la red 10.1.1.0/24 como medida de seguridad ante posibles fallos en los enlaces Frame-Relay que conectan con la red 10.2.0.0/16. (0,4 puntos)

a) ¿Qué valores de prioridad se pueden configurar para R7 y R8 para que R7 esté activo y R8 esté en espera cuando los dos enlaces Frame-Relay funcionan bien?

Prioridad R7: Prioridad R8:

b) ¿Qué tiempos hay que configurar para que los routers informen de su estado cada 5 segundos, y actualicen el router activo si pasan 20 segundos de inactividad en el enlace WAN utilizado?

Hold Time: Hello Time:

3. Dado el esquema de interconexión de redes mostrado al final del examen, se pide completar las tablas de encaminamiento de los routers R1, R2 y R3 cumpliendo las siguientes condiciones:

a) Se debe asegurar la interconexión entre todos los equipos que haya en las redes Ethernet y VPN del esquema, cumpliendo los siguientes apartados.

b) Todo el tráfico destinado a una red local remota se debe encaminar a través de un enlace Frame Relay.

c) Los equipos de las redes locales pueden acceder a Internet por la conexión ADSL más cercana (ADSL-1 o ADSL-2), sin que para ello se envíe tráfico por las redes Frame-Relay.

d) En los routers R7 y R8 está configurado HSRP con la dirección de router virtual 10.1.1.1.

e) En las tablas de encaminamiento, se deben incluir también las redes y destinos conectados directamente, indicando como puerta de enlace la dirección IP del interfaz local correspondiente junto con la letra "**D**".

f) Las direcciones IP de los enlaces WAN y serie sólo deben aparecer en las tablas de los routers que necesariamente lo requieran.

g) Las tablas de encaminamiento deben ser lo más sencillas posible, teniendo en cuenta los aspectos anteriores. Para ello se pueden agrupar subredes cuando sea posible.

h) Para que una entrada se considere correcta, debe tener su destino, máscara y puerta de enlace correctos.

R1: (1 punto)

Destino	Máscara	Puerta Enlace

R2: (1 punto)

Destino	Máscara	Puerta Enlace

R3: (0,5 puntos)

Destino	Máscara	Puerta Enlace

4. En el esquema de interconexión de redes mostrado al final se desea que los servicios de los servidores S1 (FTP), S2 (WWW) y VPN/NAS sean accesibles desde equipos de Internet a través de R4, para lo que se debe configurar su NAT de la siguiente forma:

a) Entrada estática para que el servicio de VPN con protocolos L2TP (1701) se asocie al servidor VPN/NAS (supóngase que éste servidor tiene la dirección 10.1.1.30).

b) Entrada estática para que el servicio HTTP en el puerto 80 se asocie al servidor S1.

c) Entrada estática para que el servicio FTP en el puerto 21 se asocie al servidor S2.

d) También se desea conocer la entrada dinámica que se genera cuando el equipo 84.120.1.2 de Internet accede al servidor FTP.

Completar la siguiente tabla de acuerdo a los cuatro casos anteriores. (0,5 puntos)

NAT de R4

	Inside global	Inside local	Outside local	Outside global
a)				
b)				
c)				
d)				

5. En la interconexión de redes se desea que los equipos de la red 10.4.1.0/24 como PC3 tengan acceso al servidor web de S1 activo en el puerto 8080. Para ello se configura el NAT de R6 con los siguientes comandos de Cisco IOS:

```
interface Eth1
 ip address 10.1.2.6 255.255.255.0
 ip nat outside
interface Eth2
 ip address 10.4.1.1 255.255.255.0
 ip nat inside

ip nat pool IPNUEVAS 10.55.0.1 10.55.0.254 netmask 255.255.255.0
ip nat inside source list 101 interface Eth1 overload
ip nat inside source static tcp 10.4.0.28 8080 interface Eth1 80
ip nat outside source list 102 pool IPNUEVAS

access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit tcp 10.4.1.0 0.0.0.255 host 10.1.2.6 eq 80
```

Teniendo en cuenta la configuración anterior, completa la siguiente tabla indicando las direcciones IP y los puertos de los paquetes IP. (0,5 puntos)

a) Entrada estática que permite acceder al servidor web de S1 desde el exterior de R6.

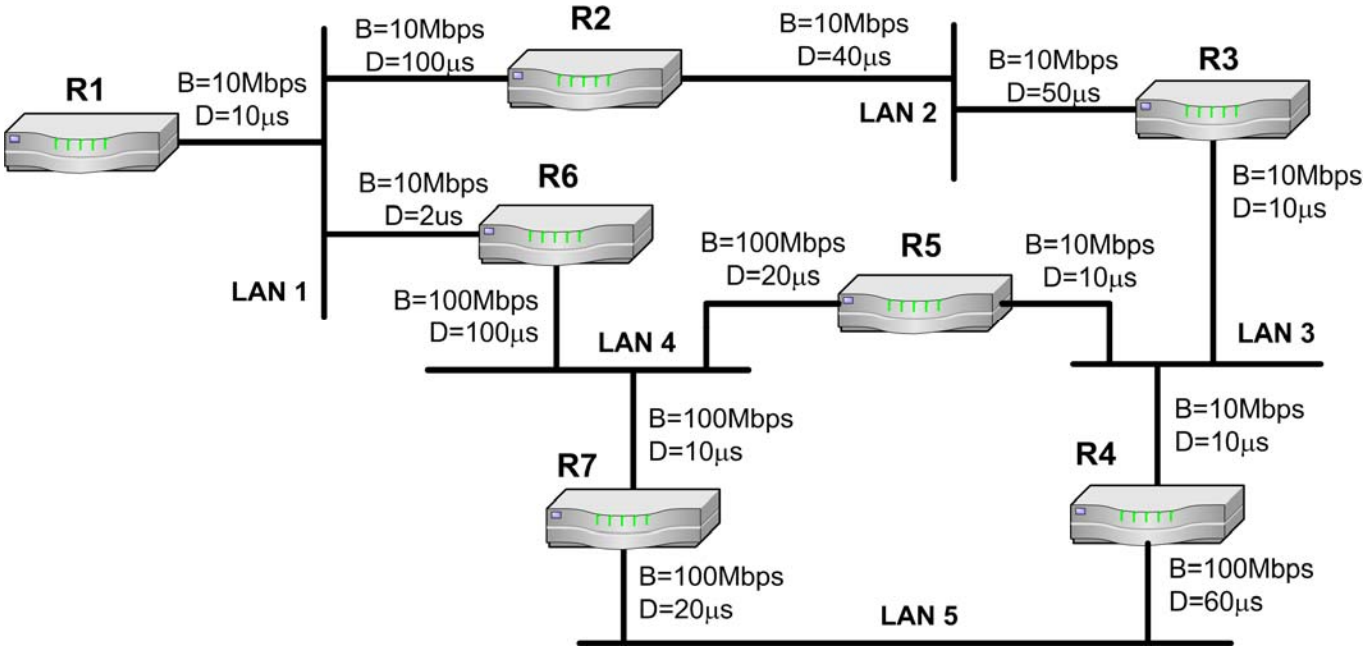
b) Entrada dinámica que se genera cuando PC4 (10.1.1.24) accede al servidor web de S1. El puerto cliente usado por PC4 es el 1040.

c) Entrada dinámica que se genera cuando PC3 (10.4.1.23) accede al servidor web de S1. El puerto cliente usado por PC3 es el 1050.

NAT de R6

	Inside global	Inside local	Outside local	Outside global
a)				
b)				
c)				

6. **En los routers del siguiente esquema está activo EIGRP. Teniendo en cuenta los parámetros de ancho de banda (B) y retardo (D) de los interfaces, se pide determinar los valores de métrica de EIGRP de los cuatro posibles caminos desde el router R1 a la red LAN 5. ¿Qué camino de los cuatro es mejor para EIGRP? (1 punto)**



Métrica del camino por R2-R3-R4:

Métrica del camino por R2-R3-R5-R7:

Métrica del camino por R6-R7:

Métrica del camino por R6-R5-R4:

Mejor camino de los cuatro:

7. **En el esquema de interconexión de redes al final del examen, se ha configurado una VPN que permite a equipos de Internet acceder a los recursos de las redes privadas. La VPN funciona con L2TP sin seguridad IPSec. Durante el proceso de conexión, trabajo y desconexión de un equipo de Internet se ha realizado una captura del tráfico en la red 10.1.1.0/16, cuyo resumen filtrado se muestra al final del examen. Atendiendo a dicha captura, se pide determinar las siguientes cuestiones. (1,5 puntos)**

Dirección IP que utiliza el servidor VPN/NAS:

Dirección IP que utiliza el servidor RADIUS:

Dirección IP original (de Internet) del cliente:

Dirección IP privada asignada al cliente para trabajar con la VPN:

Número de trama en que se asigna la dirección IP privada al cliente:

Número de trama en que el cliente envía sus datos de acceso:

Números de trama en la que el NAS envía información sobre el cliente en la BBDD de usuarios:

Número de trama del ARP con el que el NAS dice que el atenderá las tramas dirigidas al cliente de la VPN:

Nombre de usuario empleado en el equipo cliente para el acceso:

¿Se usa compresión para las tramas PPP entre el cliente y el NAS? (indicar SI o NO y el número de trama donde se establece esto).

Dibújese el formato de la trama número 44, indicando los protocolos de las diferentes cabeceras desde nivel de enlace al ICMP (incluidas éstas) en el orden correcto. Se debe indicar también las direcciones de las cabeceras IP que aparecen en la trama, y cuáles son los protocolos portador y pasajero. (1 punto)

8. Considérese que en los routers R1 y R2 del esquema de interconexión de redes se configura un control de calidad de servicio (QoS) según las configuraciones de comandos de Cisco IOS listadas al final del examen. Atendiendo a esas configuraciones de QoS, responda las siguientes cuestiones. (1,4 puntos):

¿Cuántas estrategias de suavizado de tráfico (shaping) se definen en el router R1? ¿Y cuántas de eliminación directa (policing)?

¿Cuántas estrategias de suavizado de tráfico (shaping) se definen en el router R2? ¿Y cuántas de eliminación directa (policing)?

¿Qué valor de precedencia IP tienen los paquetes con tráfico Web que llegan al equipo 10.3.2.1: **0**, **1** o **2**? ¿Quíen pone ese valor: **R1** o **R2**?

¿A qué red se asigna más ancho de banda para el tráfico Web intercambiado con Internet: **10.3.2.0**/16, **10.3.3.0**/16 o **10.3.4.0**/16?

¿A que velocidad se limita el envío de tráfico Web a Internet (por ejemplo, subir archivos con HTTP) para los equipos 10.3.X.X?

La limitación anterior, ¿Se hace mediante una estrategia de suavizado de tráfico (**shaping**) o de eliminación directa (**policing**)?

Si un equipo con dirección 10.3.X.X envía un paquete IP-HTTP a PC3, ¿Con que valor de precedencia IP (**0 a 7**) recibe PC3 el paquete?

Supóngase que también se desea limitar a 70Kbps el tráfico Web descargado desde Internet por cualquier equipo de la red 10.3.1.0 mediante "traffic shaping". Si solo se quiere modificar R1 con un nuevo comando de lista de acceso, ¿Qué comando se tendría que añadir en ese router? (0,3 puntos)

¿Y si en vez de R1 se desea modificar solamente R2 con un nuevo comando de lista de acceso? (0,3 puntos)

Anexos

Configuración de QoS en el Router R1 para la pregunta 8:

```
interface Ser1
 rate-limit output access-group 123 3000000 conform-action transmit
    exceed-action drop
interface Eth1
 ip policy route-map MIQOS1

access-list 110 permit ip any 10.3.2.0 0.0.0.255 eq 80
access-list 111 permit ip any 10.3.3.0 0.0.0.255 eq 80
access-list 112 permit ip any 10.3.4.0 0.0.0.255 eq 80
access-list 123 permit ip any any dscp af30

route-map MIQOS1 permit 10
 match ip address 110
 set ip precedence immediate
route-map MIQOS1 permit 20
 match ip address 111
 set ip precedence priority
route-map MIQOS1 permit 30
 match ip address 112
 set ip precedence routine
```

Configuración de QoS en el Router R2 para la pregunta 8:

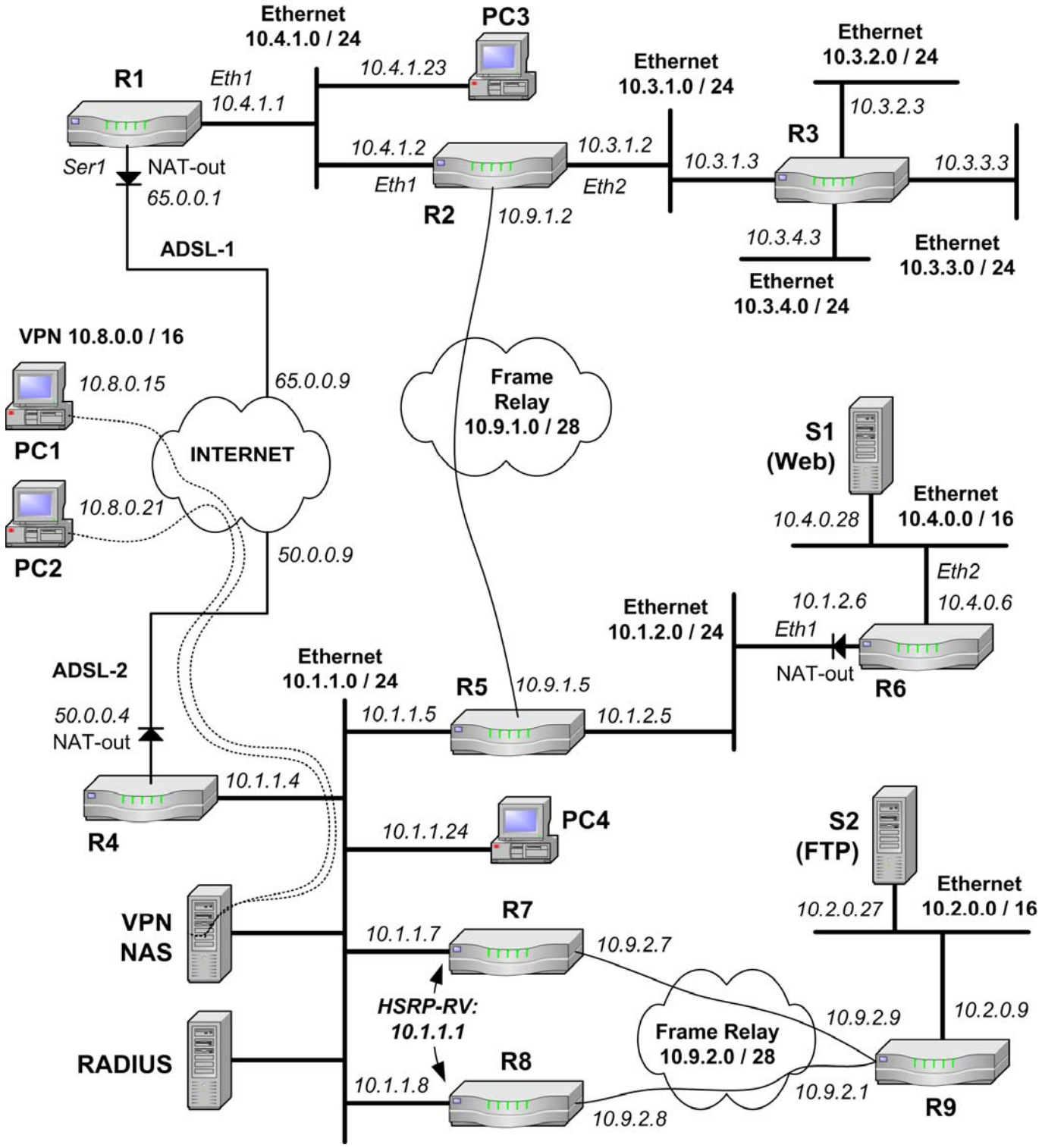
```
interface Eth1
 ip policy route-map MIQOS2
interface Eth2
 traffic-shape group 122 20000
 traffic-shape group 121 70000
 traffic-shape group 120 1000000

access-list 113 permit ip 10.3.0.0 0.0.0.255 eq 80
access-list 120 permit ip any 10.3.0.0 0.0.255.255 precedence 0
access-list 121 permit ip any 10.3.0.0 0.0.255.255 precedence 1
access-list 122 permit ip any 10.3.0.0 0.0.255.255 precedence 2

route-map MIQOS2 permit 10
 match ip address 113
 set ip dscp af30
```

Captura de la conexión VPN con L2TP utilizada en el ejercicio 7:

N.	Origen	Destino	Protocolo	Descripción
1	00:0a:5e:76:8a:2c	ff:ff:ff:ff:ff:ff	ARP	ARP request: Who has 10.1.1.25? Tell 10.1.1.4
2	00:07:0e:8c:8c:ff	00:0a:5e:76:8a:2c	ARP	ARP reply: 10.1.1.25 is at 00:07:0e:8c:8c:ff
3	80.120.2.3	10.1.1.25	L2TP	Control Message - SCCRQ (tunnel id=0, session id=0)
4	10.1.1.25	80.120.2.3	L2TP	Control Message - SCCRP (tunnel id=8, session id=0)
5	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
6	80.120.2.3	10.1.1.25	L2TP	Control Message - SCCCN (tunnel id=8, session id=0)
7	80.120.2.3	10.1.1.25	L2TP	Control Message - ICRQ (tunnel id=8, session id=0)
8	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
9	10.1.1.25	80.120.2.3	L2TP	Control Message - ICRP (tunnel id=8, session id=1)
10	80.120.2.3	10.1.1.25	L2TP	Control Message - ICCN (tunnel id=8, session id=1)
11	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
12	80.120.2.3	10.1.1.25	PPP LCP	Conf. Request (Compression negotiation=CCP)
13	10.1.1.25	80.120.2.3	PPP LCP	Conf. Request (Comp. neg.=CCP, Auth=MS-CHAP2)
14	10.1.1.25	80.120.2.3	PPP LCP	Configuration Ack
15	80.120.2.3	10.1.1.25	PPP LCP	Configuration Ack
16	80.120.2.3	10.1.1.25	PPP LCP	Identification ("MSRAS-PORTATIL-PEPE")
17	10.1.1.25	80.120.2.3	PPP CHAP	Challenge (name="PRINAS")
18	80.120.2.3	10.1.1.25	PPP CHAP	Response (name="C01")
19	00:07:0e:8c:8c:ff	ff:ff:ff:ff:ff:ff	ARP	ARP request: Who has 10.1.1.26? Tell 10.1.1.25
20	01:0a:02:03:10:11	00:07:0e:8c:8c:ff	ARP	ARP reply: 10.1.1.26 is at 01:0a:02:03:10:11
21	10.1.1.25	10.1.1.26	RADIUS	Access-Request (id=13, l=76)
22	10.1.1.26	10.1.1.25	RADIUS	Access-Accept (id=13, l=50)
23	10.1.1.25	80.120.2.3	PPP CHAP	Success
24	80.120.2.3	10.1.1.25	PPP CCP	Configuration Request (no use MPPC, no encription)
25	10.1.1.25	80.120.2.3	PPP CCP	Configuration Request (use MPPC, no encription)
26	80.120.2.3	10.1.1.25	PPP CCP	Configuration Reject (use MPPC, no encription)
27	10.1.1.25	80.120.2.3	PPP CCP	Configuration Ack (no use MPPC, no encription)
28	10.1.1.25	80.120.2.3	PPP CCP	Termination Request
29	80.120.2.3	10.1.1.25	PPP CCP	Termination Ack
30	80.120.2.3	10.1.1.25	PPP IPCP	Configuration Request (IP=0.0.0.0, DNS=0.0.0.0)
31	10.1.1.25	80.120.2.3	PPP IPCP	Configuration Request (IP=10.8.0.1)
32	80.120.2.3	10.1.1.25	PPP IPCP	Configuration Ack (IP=10.8.0.1)
33	10.1.1.25	10.1.1.26	RADIUS	Accounting-Request (User="C01", Status=start)
34	10.1.1.26	10.1.1.25	RADIUS	Accounting-Response (ok)
35	10.1.1.25	80.120.2.3	PPP IPCP	Configuration Nak (IP=10.8.0.21, DNS=10.1.1.4)
36	80.120.2.3	10.1.1.25	PPP IPCP	Configuration Request (IP=10.8.0.21, DNS=10.1.1.4)
37	10.1.1.25	80.120.2.3	PPP IPCP	Configuration Ack (IP=10.8.0.21, DNS=10.1.1.4)
38	00:07:0e:8c:8c:ff	ff:ff:ff:ff:ff:ff	ARP	ARP reply: 10.8.0.21 is at 00:07:0e:8c:8c:ff
39	10.8.0.21	10.4.1.23	ICMP	Echo (ping) request (encapsulated L2TP)
40	00:07:0e:8c:8c:ff	ff:ff:ff:ff:ff:ff	ARP	ARP request: Who has 10.1.1.5? Tell 10.8.0.21
41	00:07:0e:cd:12:3e	00:07:0e:8c:8c:ff	ARP	ARP reply: 10.1.1.5 is at 00:07:0e:cd:12:3e
42	10.8.0.21	10.4.1.23	ICMP	Echo (ping) request
43	10.4.1.23	10.8.0.21	ICMP	Echo (ping) reply
44	10.4.1.23	10.8.0.21	ICMP	Echo (ping) reply (encapsulated L2TP)
45	80.120.2.3	10.1.1.25	PPP LCP	Termination Request
46	10.1.1.25	80.120.2.3	PPP LCP	Termination Ack

N.	Origen	Destino	Protocolo	Descripción
47	10.1.1.25	80.120.2.3	L2TP	Control Message - CDN (tunnel id=8, session id=1)
48	80.120.2.3	10.1.1.25	L2TP	Control Message - StopCCN (tunnel id=8, session id=0)
49	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
50	10.1.1.25	10.1.1.26	RADIUS	Acc.-Request (User="C01", Status=stop)
51	10.1.1.26	10.1.1.25	RADIUS	Accounting-Response (ok)

Esquema de interconexión de redes para las cuestiones del examen (excepto pregunta 6):



Sistemas de Transporte de Datos – I. Informática (9186)
Noviembre/Diciembre 2009 - Control de prácticas

Nombre: _____ **DNI:** _____

Apellidos: _____

Firma:

- Nota Final = 60% Control de Teoría + 40% Control de Prácticas.
- La entrega de este control implica el uso de una convocatoria.
- El control se debe completar con bolígrafo.
- Las preguntas respondidas erróneamente no restan puntuación.
- Las preguntas se deben contestar completando los recuadros correspondientes. No se evaluará lo escrito fuera de estas opciones.
- Se puede separar la última página si así resulta más fácil consultar los anexos.
- El tiempo para realizar este examen es de 1 hora y 15 minutos.

Preguntas

1. Dado el esquema de interconexión de redes del Anexo (página 7), completa las tablas de encaminamiento de los routers R2 y R3 cumpliendo las siguientes condiciones (2,5 puntos):

a) Se debe asegurar la interconexión entre todos los equipos que haya en las LAN (Ethernet, Anillo y WiFi) y en las VPN del esquema, cumpliendo los siguientes apartados.

b) Los equipos de las redes LAN pueden acceder a Internet por la conexión a Internet más cercana.

c) Los paquetes se deben encaminar por el camino que implique un **menor número de saltos**, teniendo en cuenta el siguiente orden de prioridad para las redes en caso de igualdad de saltos: Ethernet, Anillo, ATM, WiFi, RDSI.

d) En las tablas de encaminamiento, se deben incluir también las redes y destinos conectados directamente, indicando como puerta de enlace la dirección IP del interfaz local correspondiente junto con la letra "**D**".

e) Las direcciones IP de los enlaces ADSL, ATM y RDSI sólo se deben considerar en las tablas de los routers en los que sea necesario.

f) Las tablas de encaminamiento deben ser lo más sencillas posible, teniendo en cuenta los aspectos anteriores.

g) Para simplificar las tablas, se debe agregar subredes y disminuir la máscara cuando sea posible.

h) Para que una entrada se considere correcta, debe tener su destino, máscara y puerta de enlace correctos.

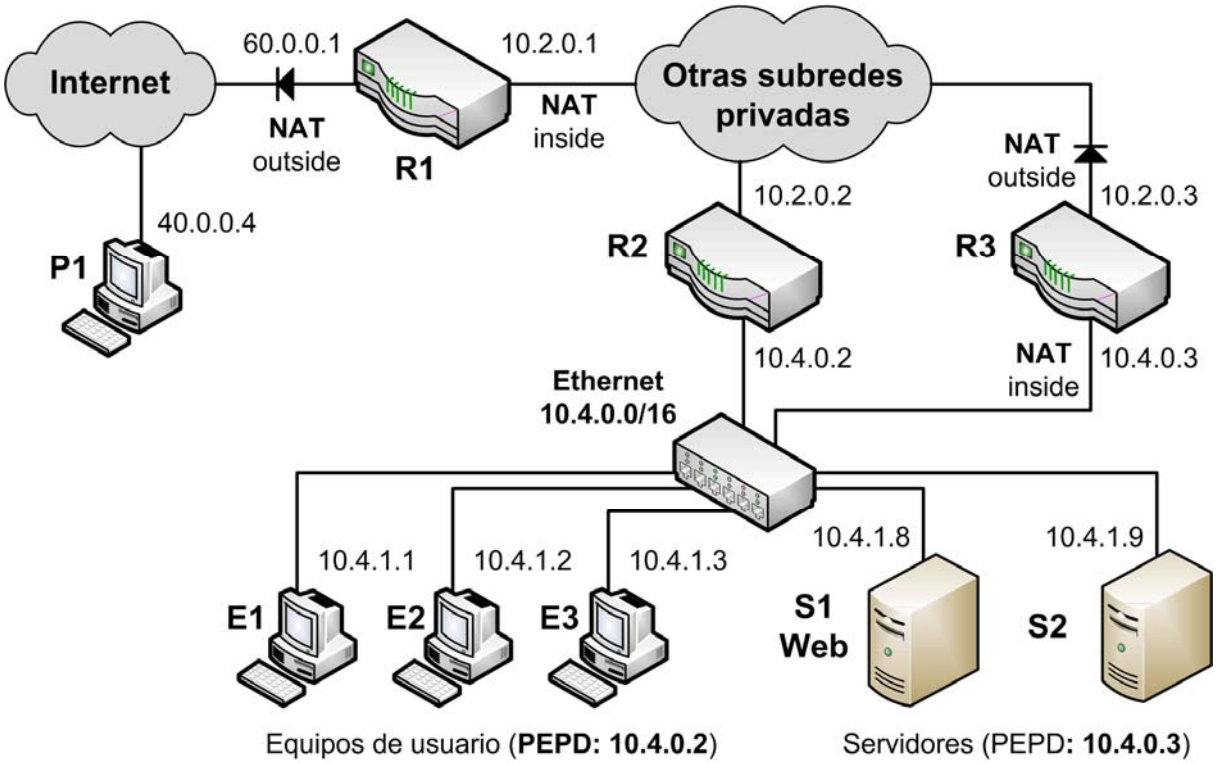
Router R5

Destino	Máscara	Puerta Enlace

Router R6

Destino	Máscara	Puerta Enlace

2. La red de una organización se estructura según el siguiente esquema. El router R1 actúa como cortafuegos para toda la red privada, el router R2 actúa como PEPD (Puerta de Enlace Por Defecto) para los equipos de usuario (E1, E2…) de la subred 10.4.0.0/16, y el router R3 actúa como un segundo cortafuegos y PEPD para los servidores (S1, S2…). (1,5 puntos).



Considérese que en R3 se ejecutan estos comandos Cisco-IOS para configurar su NAT:

```
interface Eth1
  ip address 10.2.0.3 255.255.0.0
  ip nat outside
interface Eth2
  ip address 10.4.0.3 255.255.0.0
  ip nat inside
ip nat inside source list 100 interface Eth1 overload
ip nat inside source static tcp 10.4.1.8 80 interface Eth1 8080
access-list 100 permit ip 10.4.0.0 0.0.255.255 any
```

Se pide definir las siguientes configuraciones de NAT en base a la configuración anterior del NAT de R3, indicando para ello las direcciones IP y los PUERTOS adecuados:

a) Entrada estática del NAT necesaria en R1 para que el servicio Web de S1 sea accesible desde equipos de Internet mediante la dirección pública 60.0.0.1 y el puerto 80.

b) Indicar entrada dinámica que genera el NAT de R1 cuando el equipo P1 accede al servicio Web de S1, usando como puerto cliente el número 1.025.

c) Indicar entrada dinámica que genera el NAT de R3 para el mismo caso que en b).

Pregunta	Inside global	Inside local	Outside local	Outside global
a) NAT R1				
b) NAT R1				
c) NAT R3				

Si en R3 sólo está la configuración de NAT listada antes, ¿Qué pasa si el equipo E1 accede al servicio Web de la dirección 10.2.0.3 que es redirigido a S1?

d) No hay conexión porque E1 ignora los paquetes de respuesta que recibe desde S1 debido a que la dirección origen de esos paquetes no es la correcta.

e) No hay conexión porque los paquetes de respuesta que envía S1 hacia E1 se envían a través de R3 en vez de ir directamente por la red 10.4.0.0/16, ya que R3 es la PEPD de S1.

f) Se establece una conexión TCP entre un puerto cliente de E1 y el puerto 80 de S1 directamente por la red 10.4.0.0/16 sin necesidad de routers intermedios.

g) Se establece una conexión TCP entre un puerto cliente de E1 y el puerto 8080 de S1 a través del router R3.

De las siguientes listas de comandos de Cisco IOS, ¿Cuál se podría añadir en R3 para que los equipos E1, E2… puedan acceder al servidor Web de S1 a través de la dirección 10.2.0.3?

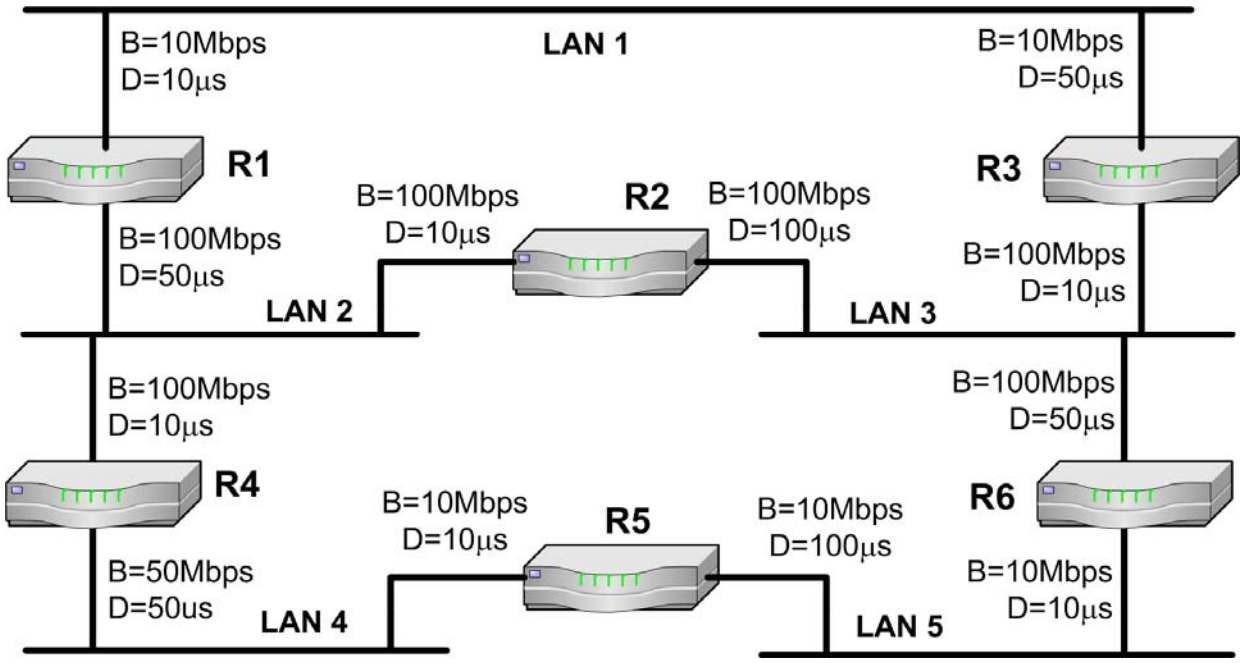
h)
```
ip nat inside source static tcp 10.4.1.8 80 interface Eth1 80
```

i)
```
ip nat pool ipsnuevas 10.2.0.4 10.2.0.254 netmask 255.255.0.0
ip nat inside source list 101 pool ipsnuevas
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
```

j)
```
ip nat pool ipsnuevas 10.40.0.1 10.40.0.254 netmask 255.255.0.0
ip nat outside source list 101 pool ipsnuevas
access-list 101 permit tcp 10.4.0.0 0.0.255.255 host 10.2.0.3 eq 8080
```

k)
```
ip nat pool ipsnuevas 10.40.0.1 10.40.0.254 netmask 255.255.0.0
ip nat outside source list 101 pool ipsnuevas
access-list 101 permit any host 10.4.1.8 eq 80
```

3. **En los routers del siguiente esquema está activo EIGRP. Teniendo en cuenta los parámetros de ancho de banda (B) y retardo (D) de los interfaces, se pide determinar los valores de métrica de EIGRP de los cuatro posibles caminos que hay desde el router R1 a la red LAN 5. Numera los caminos del mejor (1) al peor (4) según la métrica de EIGRP (1 punto).**



Camino (lista de redes)	Mín(Bi) (Kbps)	Sum(Di) (µs)	Valor de métrica EIGRP	Núm.
LAN1, LAN3, LAN5				
LAN2, LAN4, LAN5				
LAN2, LAN3, LAN5				
LAN1, LAN3, LAN2, LAN4, LAN5				

4. **En el esquema de red del Anexo (página 7) se define un túnel IP-IP con origen 10.9.9.4 y destino 10.1.2.2. Además en el router R2 se configura la siguiente entrada de encamientamiento donde "tunel0" es el interfaz del túnel (1 punto).**

Router R2

Destino	Máscara	Interfaz
10.3.8.0	*24*	*Tunel0 (Directo)*

Teniendo en cuenta las condiciones de encaminamiento de paquetes del ejercicio 1, si equipo PC1 ejecuta el comando "*ping –n 1 10.3.8.2*", ¿Qué camino seguirá el mensaje "Echo request"? Indicar el camino como la lista de routers incluyendo los equipos origen y destino.

Indica las direcciones IP de los protocolos pasajero y portador del mensaje ECHO REQUEST cuando este llega al interface 10.1.2.2 de R3.

Origen del pasajero:		Origen del portador:	
Destino del pasajero:		Destino del portador:	

Si el paquete del mensaje ECHO REQUEST parte con un valor de TTL=128 del PC1, ¿Con qué valor de TTL llega al destino 10.3.8.2? (considérese que el túnel cuenta como un único salto)

5. Una organización permite el acceso a su red local privada mediante una VPN que utiliza los protocolos L2TP, pero sin seguridad IPSec. Además, se utiliza un servidor RADIUS para gestionar los posibles usuarios de la VPN. (2 puntos)

Supóngase que un equipo de Internet se conecta como cliente de VPN al NAS (Network Access Server, o servidor de VPN) de la organización, y durante la conexión ejecuta un "ping" a un equipo de la red privada. La conexión de VPN finaliza por iniciativa del cliente.

En la siguiente tabla se listan distintas tramas desencadenadas durante la conexión del cliente a la VPN de manera desordenada. Se pide completar la tabla indicando la función que desempeña cada trama según la tabla de descripciones que hay en el Anexo (página 8), y el número de orden dentro de la conexión, desde el 1 para primera hasta el 20 para la última.

Protocolo: trama	Función	Orden
ICMP: Echo request		
ICMP: Echo reply		
PPP-CHAP: Response		
PPP-CHAP: Success		
PPP-CHAP: Challenge		
PPP-LCP: Termination Request		
PPP-LCP: Termination Ack		
PPP-LCP: Configuration Request		
PPP-LCP: Configuration Ack		
RADIUS: Accounting Request (Stop)		
RADIUS: Accounting Response		
RADIUS: Access Request		
RADIUS: Access Accept		
PPP-IPCP: Configuration Request		
PPP-IPCP: Configuration Nak		
ARP Gratuitous		

Dibújese el formato de la trama con el mensaje ICMP de "echo request" que envía el cliente por la conexión de la VPN a través de Internet, indicando claramente estos aspectos:

a) Los protocolos de las diferentes cabeceras desde nivel de enlace hasta ICMP (incluidas éstas) en el orden correcto, contando las cabeceras que incluyen los protocolos de L2TP.

b) Cuáles son los protocolos portador, de encapsulación y pasajero.

6. Dado el esquema de red del Anexo (página 7), se configura como punto de acceso para la red 10.3.9.0/24 el 10.3.9.1, y como punto de acceso para la red 10.3.8.0/24 el 10.3.8.1. También se conoce los siguientes valores para las direcciones de MAC de los equipos: (2 puntos)

IP	MAC	IP	MAC	IP	MAC	IP	MAC
10.3.9.1	A	10.3.9.2	B	10.3.9.5	C	10.3.8.1	D
10.3.8.2	E	10.2.3.2	F	10.2.3.1	G	10.2.2.1	H

Completa la siguiente tabla con las tramas que se generarán si el equipo PC2 ejecuta el comando "*ping –n 1 10.3.9.2" y a continuación el comando "ping –n 1 10.3.9.1"* (no es necesario tener en cuenta el orden de las direcciones MAC).

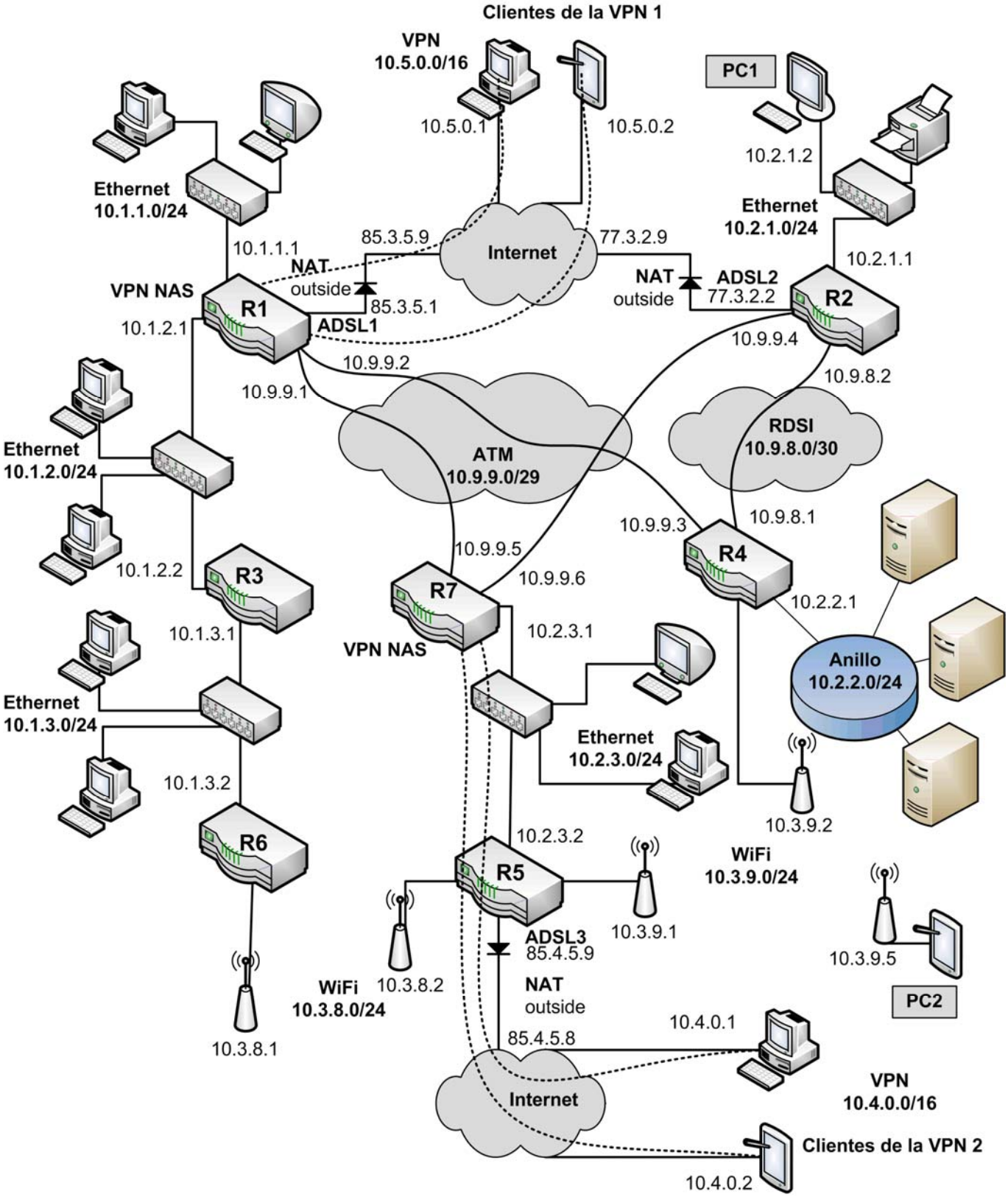
Orden	Dir. MAC 1	Dir. MAC 2	Dir. MAC 3	IP origen	IP destino	Tipo ICMP
1						
2						
3						
4						
5						
6						

Considerando que la siguiente trama representa la encapsulación IEEE 802.3 que se ha aplicado a una trama IEEE 802.11 de la red, se pide dibujar el formato de dicha trama 802.11.

MAC origen	MAC destino	Tipo	IP origen	IP destino	Datos
E	D	0x800h	10.3.8.2	10.3.8.1	ICMP

Anexo

Esquema de red para los ejercicios 1 (encaminamiento), 4 (túnel IP-IP) y 6 (WiFi):



Funciones para asignar a las tramas del ejercicio 5 (VPN):

Función	Descripción
1	El cliente informa al NAS sobre su configuración IP actual para que el NAS la valide.
2	El NAS rechaza la configuración IP del cliente y le da una válida para la VPN.
3	El cliente solicita finalizar la conexión PPP.
4	El NAS acepta la finalización de la conexión PPP.
5	El NAS envía información a la base de datos de usuarios sobre estadísticas de la conexión del cliente.
6	La base de datos de usuarios confirma que la información del cliente se ha actualizado correctamente.
7	El NAS accede a la base de datos de usuarios para comprobar la autenticidad del cliente.
8	La base de datos de usuarios informa al NAS que el cliente es válido.
9	El NAS pide al cliente que se autentifique.
10	El cliente envía su identificador de usuario y su contraseña de acceso al NAS.
11	El NAS envía al cliente la aceptación de su autentificación.
12	El NAS indica a los equipos de la red local privada de que él atiende los paquetes dirigidos al cliente de la VPN.
13	El cliente envía un ping a un equipo de la red local privada.
14	Un equipo de la red local privada contesta al ping que ha ejecutado el cliente.
15	El NAS propone opción de protocolo de autentificación al cliente (CHAP).
16	El cliente acepta el protocolo de autentificación que propone el NAS.

Sistemas de Transporte de Datos

Ingeniería Informática (9186)

Ejemplos de controles de prácticas completos (con solución)

Francisco Andrés Candelas Herías

Santiago Puente Méndez

Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

Sistemas de Transporte de Datos – I. Informática (9186)

Noviembre-Diciembre 2008 - Control de prácticas

Nombre: _____ **DNI:** _____ **Firma:**

Apellidos: _____

SOLUCIÓN

- Nota Final = 60% Control de Teoría + 40% Control de Prácticas.
- La entrega de este control implica el uso de una convocatoria.
- Las preguntas respondidas erróneamente no restan puntuación.
- Las preguntas se deben contestar completando los recuadros correspondientes con BOLÍGRAFO. No se evaluará lo escrito fuera de estas opciones.
- Todas las preguntas hacen referencia al esquema de interconexión de redes de la última página. Se puede separar la última página si así resulta más fácil consultar el esquema.
- El tiempo para realizar este examen es de 1 hora y 15 minutos.

Preguntas

1. Dado el esquema de interconexión de redes de la última página, se desea aplicar un control de los paquetes que se pueden enviar por la interfaz de red Frame-Relay del router R5 en base una lista de control de acceso (ACL) que garantice las siguientes condiciones:

a) Todos los equipos de la red 172.16.1.0/24 pueden enviar paquetes IP a la red 10.4.2.0/24.

b) Se permiten los paquetes dirigidos al servicio Web de la dirección 10.4.1.2 y procedentes de cualquier equipo.

c) El router R4 puede acceder a los servicios del servidor RADIUS (puertos UDP 1645 y 1646).

d) Desde el equipo PC4 se puede acceder al servicio SSH (terminal remota segura: puerto 22 de TCP) de todos los equipos de la red 10.4.1.0/24.

e) El resto de paquetes serán descartados y no se podrán enviar por la interfaz.

Considerando que la ACL se asocia al interfaz Frame-Relay de la siguiente forma, se pide especificar en el recuadro los comandos de Cisco IOS que definen la ACL (0,5 puntos).

```
interface Serial0
 ip address 10.1.0.5 255.255.255.248
 ip access-group 104 out
```

access-list 104 permit ip 172.16.1.0 0.0.0.255 10.4.2.0 0.0.0.255
access-list 104 permit tcp any host 10.4.1.2 eq 80
access-list 104 permit udp host 10.1.2.4 host 10.4.2.8 eq 1645
access-list 104 permit udp host 10.1.2.4 host 10.4.2.8 eq 1646
access-list 104 permit tcp host 172.16.1.9 10.4.1.0 0.0.0.255 eq 22
(el comando deny any any al final está implícito)

2. Completar las tablas de encaminamiento de los routers R1, R3 y R5 del esquema de la última hoja cumpliendo las siguientes condiciones (2,5 puntos).

a) Se debe asegurar la interconexión entre todos los equipos que haya en las redes Ethernet y VPN del esquema, cumpliendo los siguientes apartados.

b) Todo el tráfico destinado a una red local remota se debe encaminar a través del enlace Frame Relay o del RDSI, según corresponda, y no por Internet.

c) Los equipos de las redes locales pueden acceder a Internet por la conexión ADSL más cercana (ADSL-1 o ADSL-2), sin que para ello se envíe tráfico por la red Frame-Relay.

d) En las tablas de encaminamiento, se deben incluir también las redes y destinos conectados directamente, indicando como puerta de enlace la dirección IP de la interfaz local correspondiente junto con la letra “D”.

e) Las direcciones IP de los enlaces WAN y serie sólo deben aparecer en las tablas de los routers que necesariamente lo requieran.

f) Las tablas de encaminamiento deben ser lo más sencillas posible, teniendo en cuenta los aspectos anteriores. Para ello se pueden agrupar subredes cuando sea posible.

g) Para que una entrada se considere correcta, debe tener su destino, máscara y puerta de enlace correctos.

R1: (0,9 puntos)

Destino	Máscara	Puerta Enlace
80.1.0.8	*32*	*80.1.0.1 (D)*
10.5.1.0	*24*	*10.5.1.1 (D)*
10.4.1.0	*24*	*10.4.1.1 (D)*
172.16.0.0	*16*	*10.4.1.3*
10.5.2.0	*24*	*10.4.1.3*
10.4.2.0	*24*	*10.4.1.3*
10.2.0.0	*16*	*10.4.1.3*
0.0.0.0	*-*	*80.1.0.8*
~~*10.5.0.0*~~		

R3: (0,7 puntos)

Destino	Máscara	Puerta Enlace
10.1.0.5	*32*	*10.1.0.3 (D)*
10.4.2.0	*24*	*10.4.2.3 (D)*
10.4.1.0	*24*	*10.4.1.3 (D)*
10.2.0.0	*16*	*10.2.0.3 (D)*
172.16.0.0	*16*	*10.1.0.5*
10.5.2.0	*24*	*10.1.0.5*
0.0.0.0	*-*	*10.4.1.1*

R5: (0,9 puntos)

Destino	Máscara	Puerta Enlace
10.1.2.4	*32*	*10.1.2.5 (D)*
10.1.0.3	*32*	*10.1.0.5 (D)*
10.1.1.6	*32*	*10.1.1.5 (D)*
172.16.1.0	*24*	*172.16.1.5 (D)*
172.16.2.0	*24*	*10.1.1.6*
10.4.0.0	*16*	*10.1.0.3*
10.5.1.0	*24*	*10.1.0.3*
10.2.0.0	*16*	*10.1.0.3*
0.0.0.0	*-*	*10.1.2.4*
~~*10.5.0.0*~~		

3. Se desea que los servicios de los servidores WWW y VPN-NAS sean accesibles desde equipos de Internet a través del router R1, para lo que se debe configurar su NAT de la siguiente forma:

a) Entrada estática para que el servicio de VPN con protocolos L2TP (1701) se asocie al servidor VPN-NAS.

b) Entrada estática para que el servicio Web con protocolo HTTP (80) se asocie al servidor WEB.

c) También se desea conocer la entrada dinámica que se genera cuando el equipo 60.1.1.1 de Internet accede al servidor WEB usando su puerto cliente 1050.

Completar la siguiente tabla de acuerdo a los casos anteriores (0,5 puntos).

NAT de R1

	Inside global	Inside local	Outside local	Outside global
a)	*80.1.0.1:1701*	*10.4.1.3:1701*	-	-
b)	*80.1.0.1:80*	*10.4.1.2:80*	-	-
c)	*80.1.0.1:80*	*10.4.1.2:80*	*60.1.1.1:1050*	*60.1.1.1:1050*

4. Por aumentar la seguridad del servidor WEB de la red Ethernet 10.5.0.0/16, y para permitir que los equipos de las redes WiFi puedan acceder a ese servidor, se establece la siguiente configuración de NAT en el router R2, usando comandos de Cisco IOS:

```
interface Eth1
 ip address 10.4.1.2 255.255.255.0
 ip nat outside
interface Eth2
 ip address 10.5.0.2 255.255.0.0
 ip nat inside

ip nat pool IPNUEVAS 10.9.0.1 10.9.0.254 netmask 255.255.255.0
ip nat inside source list 101 interface Eth1 overload
ip nat inside source static tcp 10.5.0.8 80 interface Eth1 80
ip nat inside source static tcp 10.5.0.8 443 interface Eth1 443
ip nat outside source static 10.4.2.9 10.7.0.8 extendable
ip nat outside source list 1 pool IPNUEVAS
access-list 1 permit 10.5.0.0 0.0.255.255
access-list 101 deny ip any 10.4.2.8 255.255.255.255
access-list 101 permit any any
```

Atendiendo a la configuración anterior, se debe determinar las direcciones IP que tienen los paquetes IP de los siguientes casos (1,5 puntos):

	Origen	Destino
a) Paquete IP-ICMP enviado desde el equipo PC1 al PC4 cuando pasa por la red 10.4.1.0/24.	*10.4.1.2*	*172.16.1.9*
b) Paquete IP-UDP enviado desde el equipo PC1 al servidor RADIUS cuando pasa por la red 10.4.1.0/24.	*10.5.0.9*	*10.4.2.8*
c) Paquete IP-TCP enviado desde el equipo PC2 al servicio Web del servidor WEB cuando pasa por la red 10.4.1.0/24.	*10.5.1.9*	*10.4.1.2*
d) Mismo paquete del caso anterior (c) cuando pasa por la red 10.5.0.0/16.	*10.9.0.1*	*10.5.0.8*
e) Paquete IP-TCP enviado desde el equipo PC1 al destino 10.7.0.8 cuando pasa por la red 10.5.0.0/16.	*10.5.0.9*	*10.7.0.8*
f) Mismo paquete del caso anterior (**e**) cuando pasa por la red 10.4.1.0/24.	*10.4.1.2*	*10.4.2.9*

5. En la interconexión del esquema, el router R3 está configurado como NAS (Network Address Server) que utiliza el servidor RADIUS con la base de datos de usuarios. La VPN emplea los protocolos L2TP, con autenticación PPP-CHAP.

a) El equipo remoto PC5 inicia una conexión VPN y está se da por válida. Se pide completar la siguiente tabla con la lista de las tramas que se envían y reciben en el router R3 relacionadas con los procesos de autenticación del usuario y de validación en la base de datos, teniendo en cuenta el orden correcto de las mismas **(1 punto)**.

Nº	IP Origen	IP Destino	Protocolo	Tipo-Significado
1	*10.4.1.3*	*80.1.0.9*	*PPP-CHAP*	*Challenge (desafío)*
2	*80.1.0.9*	*10.4.1.3*	*PPP-CHAP*	*Response (respuesta)*
3	*10.4.2.3*	*10.4.2.8*	*RADIUS*	*Access-Request*
4	*10.4.2.8*	*10.4.2.3*	*RADIUS*	*Access-Accept*
5	*10.4.1.3*	*80.1.0.9*	*PPP-CHAP*	*Success (aceptado)*

b) Una vez que el cliente PC5 se ha conectado a la VPN, este equipo envía un paquete TCP al equipo PC4, sin utilizar la seguridad de IPSec. Se pide dibujar el formato de la trama de enlace con el paquete TCP cuando pasa por la red 10.4.1.0/24, detallando lo siguiente **(1 punto)**:

- Las cabeceras de todos los protocolos que contiene en el orden correcto.
- Las direcciones origen y destino de las cabeceras IP.
- Qué protocolos son el portador y el pasajero.

Ethernet	*IP*	*UDP*	*L2TP*	*PPP*	*IP*	*TCP*

Origen: 80.1.0.9
Destino: 10.4.1.3

Origen: 10.2.1.9
Destino: 172.16.1.9

Portador: UDP (trasporte)
Pasajero: PPP (enlace)

6. Considérese que los routers del esquema tienen EIGRP activado, y que el equipo remoto PC5 realiza una conexión a la VPN. El *delay* asociado a los interfaces de la VPN en el router R3 es 2,000.000µs. ¿Qué mensajes EIGRP que se envían en estos casos (0,5 puntos)?

a) Mensaje que envía R3 a los routers vecinos cuando se acepta la conexión de PC5.

b) Mensaje que envía R2 a los routers vecinos cada pocos segundos para indicar que está activo y para solicitar actualizaciones.

c) Mensaje que envía R3 a los routers vecinos cuando finaliza la conexión de PC5.

	IP Destino	Tipo de mensaje	Información
a)	*224.0.0.10*	*Update*	*Dst=10.2.1.9/32 Delay=2,000.000*
b)	*224.0.0.10*	*Hello*	*(Parámetros EIGRP)*
c)	*224.0.0.10*	*Query*	*Dst=10.1.1.20/32 Delay=Inalcanzable*

7. Considérese que en el esquema de redes se configura un túnel de nivel 3 tipo "IP sobre IP" introduciendo los siguientes comandos de Cisco IOS en el router R5:

```
interface Serial0
 ip address 10.1.0.5 255.255.255.248

interface Tunnel0
 tunnel source Serial0
 tunnel destination 10.4.1.1
 tunnel mode gre ip

! Añade una ruta para llegar a 10.4.2.0 por la interfaz del Tunnel0
ip route 10.4.2.0 255.255.255.0 Tunnel0
```

Suponiendo que en equipo PC4 se ejecuta el comando "ping 10.4.2.9 –n 1", resuelve las siguientes cuestiones (1 punto):

a) Indicar la lista completa de equipos por los que pasa el paquete IP-ICMP, en el orden correcto, e incluyendo el origen y el destino.

PC4 > R5 > R3 > R1 > R3 > PC3

b) Determinar el número de saltos que contabiliza el paquete IP-ICMP al llegar al destino, y el número de reales que realiza en la red (el túnel cuenta como un salto).

Saltos contabilizados: *3* Saltos reales: *5*

c) ¿Qué direcciones tienen los protocolos IP portador e IP pasajero del paquete generado por el "ping" cuando pasa por la red Frame-Relay?

Origen del pasajero:	*172.16.1.9*	Origen del portador:	*10.1.0.5*
Destino del pasajero:	*10.4.2.9*	Destino del portador:	*10.4.1.1*

8. En la estructura de redes del esquema, se configuran los routers R2 y R3 para que realicen un control de QoS de forma que se limite el ancho de banda para las descargas desde el servidor WEB. Para ello se emplean estos comandos de Cisco IOS:

Router R2:

```
interface Eth1
 ip address 10.4.1.2 255.255.0.0
 ip policy route-map QOSETH1

access-list 110 permit tcp any 10.5.0.0 0.0.255.255 eq 80
access-list 111 permit tcp any 172.16.2.0 0.0.0.255 eq 80
access-list 112 permit tcp any 172.16.1.0 0.0.0.255 eq 80

route-map QOSETH1 permit 10
 match ip address 110
 set ip precedence routine
route-map QOSETH1 permit 20
 match ip address 111
 set ip precedence priority
route-map QOSETH1 permit 30
 match ip address 112
 set ip precedence inmediate
```

Router R3:

```
interface Serial0
 ip address 10.1.0.3 255.255.255.255
 rate-limit output access-group 110 256000 conform-act transmit exceed-act drop
 rate-limit output access-group 111 512000 conform-act transmit exceed-act drop
access-list 110 permit ip host 10.4.1.2 any precedence 0
access-list 111 permit ip host 10.4.1.2 any precedence 1
```

Se pide responder a las siguientes cuestiones (1 punto):

a) ¿Qué tipo de estrategia se utiliza: *Traffic Shaping* (Cisco GTS) o *Traffic Policing* (Cisco CAR)? — *TP - CAR*

b) ¿Qué router realiza una clasificación de tráfico? — *R2*

c) ¿A qué red se asigna más ancho de banda para el tráfico Web que procede del servidor WEB y va hacia la red Frame Relay: 10.5..2.0/24, 172.16.1.0/24 o 172.16.2.0/24? — *172.16.1.0/24*

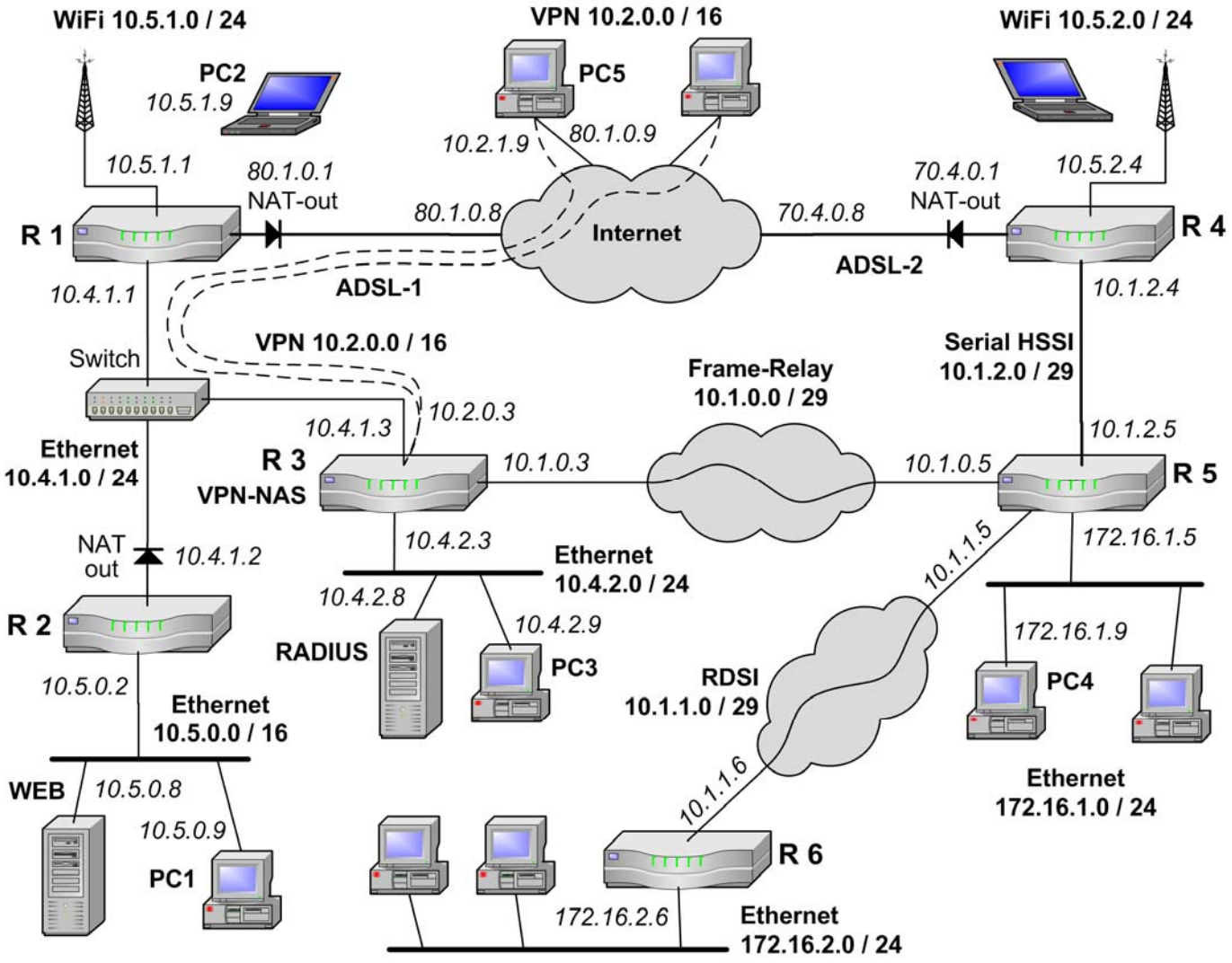
d) ¿A qué velocidad se limita el envío del tráfico desde el servidor WEB hacia la red WiFi 10.5.2.0/24? — *256Kbps*

e) ¿Qué valor numérico de precedencia tienen los paquetes IP que proceden del servidor WEB y están dirigidos a la red 172.16.2.0/24 cuando pasan por la red Frame Relay? — *1*

Explica brevemente qué pasaría si, en vez de a tráfico TCP, se aplicase la configuración anterior a una aplicación de descarga de archivos basada en UDP (0,5 puntos).

Que habría muchos problemas en la descarga porque los paquetes UDP-IP descartados no se recuperan, y no hay control de flujo, a no ser que todo eso lo resolviese la aplicación.

Esquema de interconexión de redes para todas las preguntas



Sistemas de Transporte de Datos – I. Informática (9186)

Septiembre 2008 - Control de prácticas

Nombre: _____ **DNI:** _____ **Firma:**

Apellidos: _____

SOLUCIÓN

- Nota Final = 60% Control de Teoría + 40% Control de Prácticas.
- La entrega de este control implica el uso de una convocatoria.
- El control se debe completar con bolígrafo.
- Las preguntas respondidas erróneamente no restan puntuación.
- Las preguntas se deben contestar completando los recuadros correspondientes. No se evaluará lo escrito fuera de estas opciones.
- Se puede separar la última página si así resulta más fácil consultar los anexos.
- El tiempo para realizar este examen es de 1 hora y 15 minutos.

Preguntas

1. En el esquema de interconexión de redes mostrado al final del examen se necesita configurar una lista de acceso (ACL) en el router R1 (lista número 100) para bloquear determinado tráfico entre equipos internos y de Internet de forma que se cumpla que:

a) Los equipos de las redes privadas no pueden enviar paquetes a los servidores web públicos cuyos destinos son 213.215.145.96 o alguno de la red 213.248.111.0/24.

b) PC3 no puede recibir paquetes IP a la dirección 50.0.0.4.

c) Todo el tráfico que no coincida con las condiciones a) ni b) si debe ser encaminado por R1.

Especificar los comandos de Cisco IOS que definen la ACL descrita. (0,6 puntos)

```
access-list 100 deny tcp any host 213.215.145.96 eq 80
access-list 100 deny tcp any 213.248.111.0 0.0.0.255 eq 80
access-list 100 deny ip host 10.4.1.23 host 50.0.0.4
access-list 100 permit any any
```

2. En el esquema de interconexión de redes mostrado al final del examen se configura HSRP para los routers R7 y R8 en la red 10.1.1.0/24 como medida de seguridad ante posibles fallos en los enlaces Frame-Relay que conectan con la red 10.2.0.0/16. (0,4 puntos)

a) ¿Qué valores de prioridad se pueden configurar para R7 y R8 para que R7 esté activo y R8 esté en espera cuando los dos enlaces Frame-Relay funcionan bien?

Prioridad R7: *Mayor que R8* Prioridad R8: *Menor que R7*

b) ¿Qué tiempos hay que configurar para que los routers informen de su estado cada 5 segundos, y actualicen el router activo si pasan 20 segundos de inactividad en el enlace WAN utilizado?

Hold Time: *20* Hello Time: *5*

3. Dado el esquema de interconexión de redes mostrado al final del examen, se pide completar las tablas de encaminamiento de los routers R1, R2 y R3 cumpliendo las siguientes condiciones:

a) Se debe asegurar la interconexión entre todos los equipos que haya en las redes Ethernet y VPN del esquema, cumpliendo los siguientes apartados.

b) Todo el tráfico destinado a una red local remota se debe encaminar a través de un enlace Frame Relay.

c) Los equipos de las redes locales pueden acceder a Internet por la conexión ADSL más cercana (ADSL-1 o ADSL-2), sin que para ello se envíe tráfico por las redes Frame-Relay.

d) En los routers R7 y R8 está configurado HSRP con la dirección de router virtual 10.1.1.1.

e) En las tablas de encaminamiento, se deben incluir también las redes y destinos conectados directamente, indicando como puerta de enlace la dirección IP del interfaz local correspondiente junto con la letra "**D**".

f) Las direcciones IP de los enlaces WAN y serie sólo deben aparecer en las tablas de los routers que necesariamente lo requieran.

g) Las tablas de encaminamiento deben ser lo más sencillas posible, teniendo en cuenta los aspectos anteriores. Para ello se pueden agrupar subredes cuando sea posible.

h) Para que una entrada se considere correcta, debe tener su destino, máscara y puerta de enlace correctos.

R1: (1 punto)

Destino	Máscara	Puerta Enlace
65.0.0.9	*32*	*65.0.0.1 D*
10.4.1.0	*24*	*10.4.1.1 D*
10.3.0.0	*16*	*10.4.1.2*
10.1.0.0	*16*	*10.4.1.2*
10.2.0.0	*16*	*10.4.1.2*
10.8.0.0	*16*	*10.4.1.2*
0.0.0.0	*-*	*65.0.0.9*
~~10.4.0.0~~	*16*	

R2: (1 punto)

Destino	Máscara	Puerta Enlace
10.4.1.0	*24*	*10.4.1.2 D*
10.3.1.0	*24*	*10.3.1.2 D*
10.9.1.5	*32*	*10.9.1.2 D*
10.3.2.0	*24*	*10.3.1.3*
10.3.3.0	*24*	*10.3.1.3*
10.3.4.0	*24*	*10.3.1.3*
10.1.0.0	*16*	*10.9.1.5*
10.2.0.0	*16*	*10.9.1.5*
10.8.0.0	*16*	*10.9.1.5*
0.0.0.0	*-*	*10.4.1.1*

R3: (0,5 puntos)

Destino	Máscara	Puerta Enlace
10.3.1.0	*24*	*10.3.1.3 D*
10.3.2.0	*24*	*10.3.2.3 D*
10.3.3.0	*24*	*10.3.3.3 D*
10.3.4.0	*24*	*10.3.4.3 D*
0.0.0.0	*-*	*10.3.1.2*

4. En el esquema de interconexión de redes mostrado al final se desea que los servicios de los servidores S1 (FTP), S2 (WWW) y VPN/NAS sean accesibles desde equipos de Internet a través de R4, para lo que se debe configurar su NAT de la siguiente forma:

a) Entrada estática para que el servicio de VPN con protocolos L2TP (1701) se asocie al servidor VPN/NAS (supóngase que éste servidor tiene la dirección 10.1.1.30).

b) Entrada estática para que el servicio HTTP en el puerto 80 se asocie al servidor S1.

c) Entrada estática para que el servicio FTP en el puerto 21 se asocie al servidor S2.

d) También se desea conocer la entrada dinámica que se genera cuando el equipo 84.120.1.2 de Internet accede al servidor FTP.

Completar la siguiente tabla de acuerdo a los cuatro casos anteriores. (0,5 puntos)

NAT de R4

	Inside global	Inside local	Outside local	Outside global
a)	*50.0.0.4:1701*	*10.1.1.30:1701*	-	-
b)	*50.0.0.4:80*	*10.1.2.6:80*	-	-
c)	*50.0.0.4:21*	*10.2.0.27:21*	-	-
d)	*50.0.0.4:21*	*10.2.0.27:21*	*84.120.1.2*	*84.120.1.2*

5. En la interconexión de redes se desea que los equipos de la red 10.4.1.0/24 como PC3 tengan acceso al servidor web de S1 activo en el puerto 8080. Para ello se configura el NAT de R6 con los siguientes comandos de Cisco IOS:

```
interface Eth1
 ip address 10.1.2.6 255.255.255.0
 ip nat outside
interface Eth2
 ip address 10.4.1.1 255.255.255.0
 ip nat inside

ip nat pool IPNUEVAS 10.55.0.1 10.55.0.254 netmask 255.255.255.0
ip nat inside source list 101 interface Eth1 overload
ip nat inside source static tcp 10.4.0.28 8080 interface Eth1 80
ip nat outside source list 102 pool IPNUEVAS

access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit tcp 10.4.1.0 0.0.0.255 host 10.1.2.6 eq 80
```

Teniendo en cuenta la configuración anterior, completa la siguiente tabla indicando las direcciones IP y los puertos de los paquetes IP. (0,5 puntos)

a) Entrada estática que permite acceder al servidor web de S1 desde el exterior de R6.

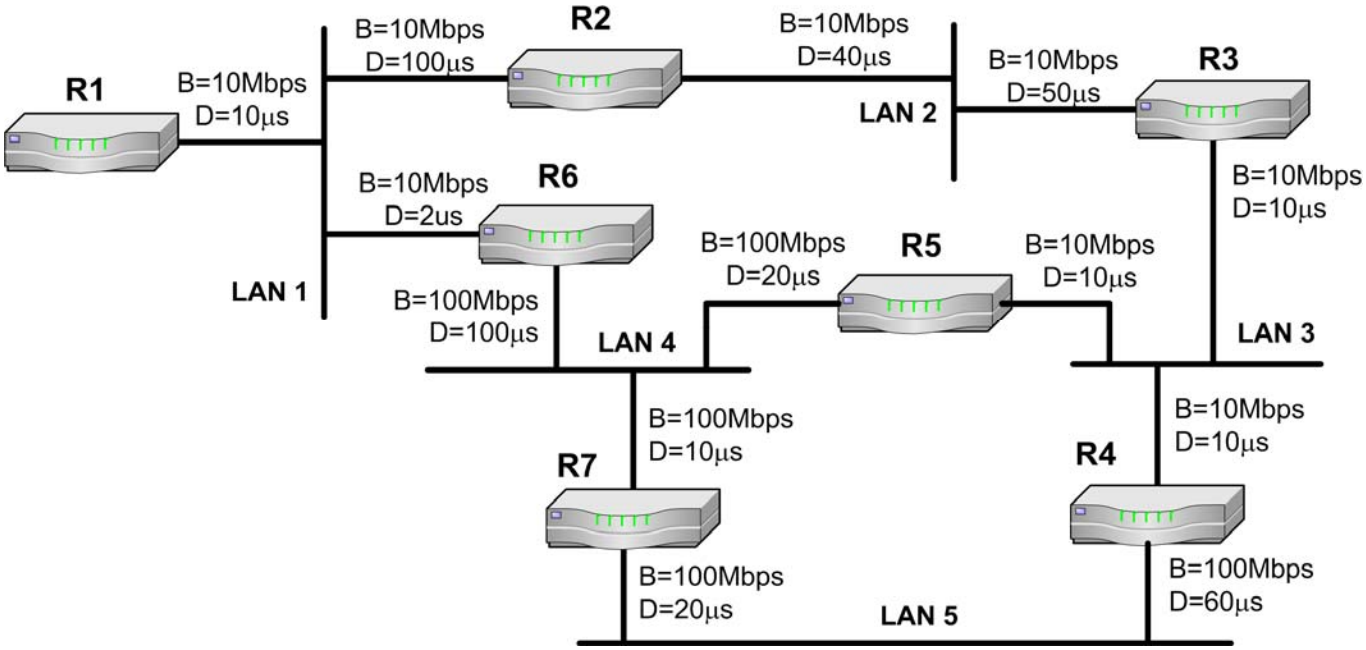
b) Entrada dinámica que se genera cuando PC4 (10.1.1.24) accede al servidor web de S1. El puerto cliente usado por PC4 es el 1040.

c) Entrada dinámica que se genera cuando PC3 (10.4.1.23) accede al servidor web de S1. El puerto cliente usado por PC3 es el 1050.

NAT de R6

	Inside global	Inside local	Outside local	Outside global
a)	*10.1.2.6:80*	*10.4.0.28:8080*	*- - -*	*- - -*
b)	*10.1.2.6:80*	*10.4.0.28:8080*	*10.1.1.24:1040*	*10.1.1.24:1040*
c)	*10.1.2.6:80*	*10.4.0.28:8080*	*10.55.0.1:1050*	*10.4.1.23:1050*

6. **En los routers del siguiente esquema está activo EIGRP. Teniendo en cuenta los parámetros de ancho de banda (B) y retardo (D) de los interfaces, se pide determinar los valores de métrica de EIGRP de los cuatro posibles caminos desde el router R1 a la red LAN 5. ¿Qué camino de los cuatro es mejor para EIGRP? (1 punto)**



Métrica del camino por R2-R3-R4:	*MinB=10Mbps; SumD=120µs; M=2563072*
Métrica del camino por R2-R3-R5-R7:	*MinB=10Mbps; SumD=100µs; M=2562560*
Métrica del camino por R6-R7:	*MinB=10Mbps; SumD=130µs; M=2563328*
Métrica del camino por R6-R5-R4:	*MinB=10Mbps; SumD=180µs; M=2564608*
Mejor camino de los cuatro:	*La métrica menor: R2-R3-R5-R7*

7. **En el esquema de interconexión de redes al final del examen, se ha configurado una VPN que permite a equipos de Internet acceder a los recursos de las redes privadas. La VPN funciona con L2TP sin seguridad IPSec. Durante el proceso de conexión, trabajo y desconexión de un equipo de Internet se ha realizado una captura del tráfico en la red 10.1.1.0/16, cuyo resumen filtrado se muestra al final del examen. Atendiendo a dicha captura, se pide determinar las siguientes cuestiones. (1,5 puntos)**

Dirección IP que utiliza el servidor VPN/NAS:	*10.1.1.25*
Dirección IP que utiliza el servidor RADIUS:	*10.1.1.26*
Dirección IP original (de Internet) del cliente:	*80.120.2.3*
Dirección IP privada asignada al cliente para trabajar con la VPN:	*10.8.0.21*
Número de trama en que se asigna la dirección IP privada al cliente:	*35*

Número de trama en que el cliente envía sus datos de acceso:	*18*
Números de trama en la que el NAS envía información sobre el cliente en la BBDD de usuarios:	*21 y 50*
Número de trama del ARP con el que el NAS dice que el atenderá las tramas dirigidas al cliente de la VPN:	*38*
Nombre de usuario empleado en el equipo cliente para el acceso:	*C01*
¿Se usa compresión para las tramas PPP entre el cliente y el NAS? (indicar SI o NO y el número de trama donde se establece esto).	*NO, 27*

Dibújese el formato de la trama número 44, indicando los protocolos de las diferentes cabeceras desde nivel de enlace al ICMP (incluidas éstas) en el orden correcto. Se debe indicar también las direcciones de las cabeceras IP que aparecen en la trama, y cuáles son los protocolos portador y pasajero. (1 punto)

Ethernet	*IP*	*UDP*	*L2TP*	*PPP*	*IP*	*ICMP*

Origen: 10.1.1.25
Destino: 80.120.2.3

Origen: 10.4.1.23
Destino: 10.8.0.21

Portador: UDP (trasporte)
Pasajero: PPP (enlace)

8. Considérese que en los routers R1 y R2 del esquema de interconexión de redes se configura un control de calidad de servicio (QoS) según las configuraciones de comandos de Cisco IOS listadas al final del examen. Atendiendo a esas configuraciones de QoS, responda las siguientes cuestiones. (1,4 puntos):

¿Cuántas estrategias de suavizado de tráfico (shaping) se definen en el router R1? ¿Y cuántas de eliminación directa (policing)?	*0*	*1*
¿Cuántas estrategias de suavizado de tráfico (shaping) se definen en el router R2? ¿Y cuántas de eliminación directa (policing)?	*3*	*0*
¿Qué valor de precedencia IP tienen los paquetes con tráfico Web que llegan al equipo 10.3.2.1: **0**, **1** o **2**? ¿Quíen pone ese valor: **R1** o **R2**?	*2*	*R1*
¿A qué red se asigna más ancho de banda para el tráfico Web intercambiado con Internet: **10.3.2.0**/16, **10.3.3.0**/16 o **10.3.4.0**/16?	*10.3.4.0/16*	
¿A que velocidad se limita el envío de tráfico Web a Internet (por ejemplo, subir archivos con HTTP) para los equipos 10.3.X.X?	*3Mbps*	
La limitación anterior, ¿Se hace mediante una estrategia de suavizado de tráfico (**shaping**) o de eliminación directa (**policing**)?	*policing*	

Si un equipo con dirección 10.3.X.X envía un paquete IP-HTTP a PC3, ¿Con que valor de precedencia IP (**0 a 7**) recibe PC3 el paquete?

af32=clase3=prec3

Supóngase que también se desea limitar a 70Kbps el tráfico Web descargado desde Internet por cualquier equipo de la red 10.3.1.0 mediante "traffic shaping". Si solo se quiere modificar R1 con un nuevo comando de lista de acceso, ¿Qué comando se tendría que añadir en ese router? (0,3 puntos)

access-list 111 permit ip any 10.3.1.0 0.0.0.255

¿Y si en vez de R1 se desea modificar solamente R2 con un nuevo comando de lista de acceso? (0,3 puntos)

access-list 121 permit ip any 10.3.1.0 0.0.0.255

Anexos

Configuració de QoS en el Router R1 para la pregunta 8:

```
interface Ser1
 rate-limit output access-group 123 3000000 conform-action transmit
    exceed-action drop
interface Eth1
 ip policy route-map MIQOS1

access-list 110 permit ip any 10.3.2.0 0.0.0.255 eq 80
access-list 111 permit ip any 10.3.3.0 0.0.0.255 eq 80
access-list 112 permit ip any 10.3.4.0 0.0.0.255 eq 80
access-list 123 permit ip any any dscp af30

route-map MIQOS1 permit 10
 match ip address 110
 set ip precedence immediate
route-map MIQOS1 permit 20
 match ip address 111
 set ip precedence priority
route-map MIQOS1 permit 30
 match ip address 112
 set ip precedence routine
```

Configuración de QoS en el Router R2 para la pregunta 8:

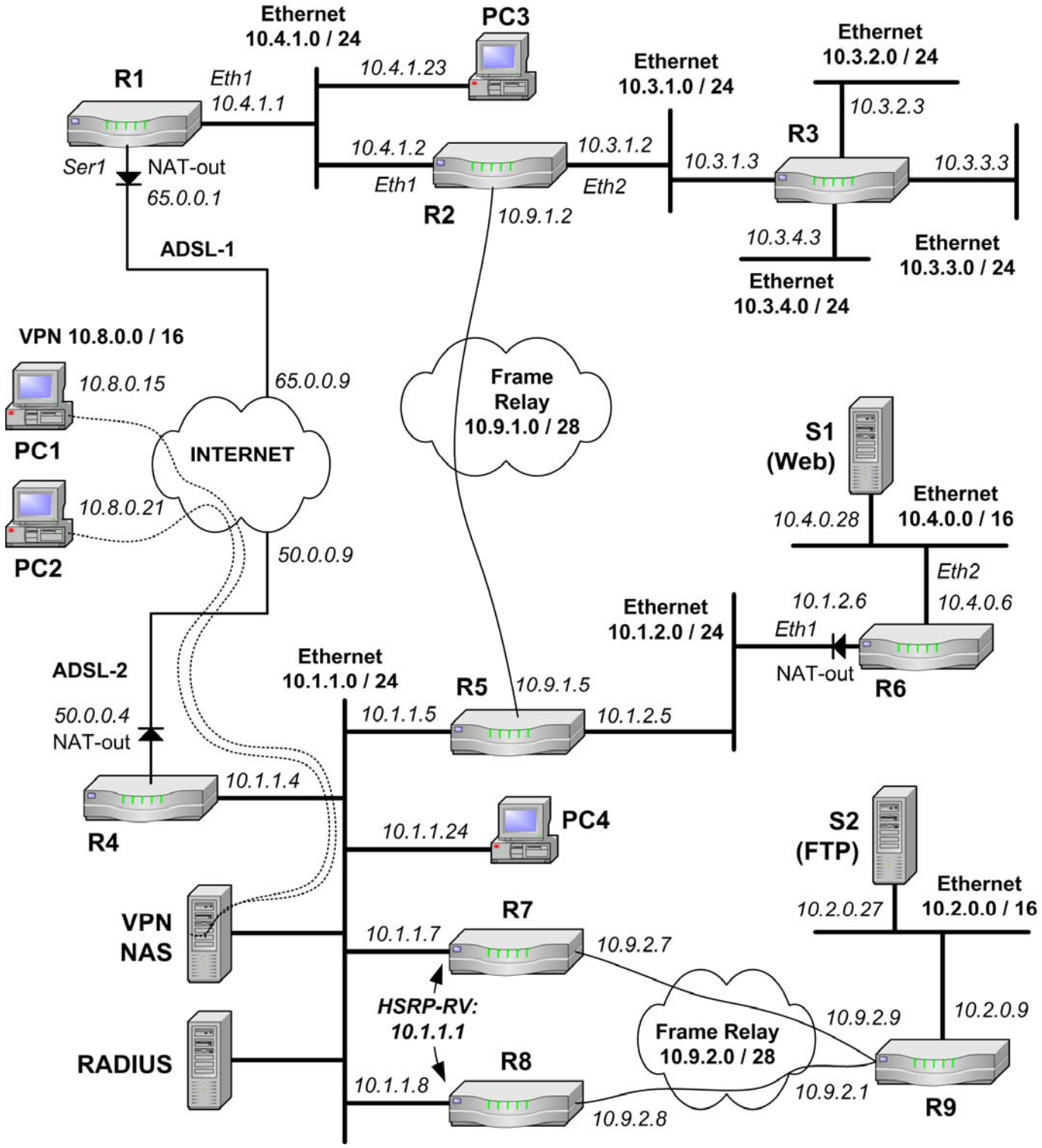
```
interface Eth1
 ip policy route-map MIQOS2
interface Eth2
 traffic-shape group 122 20000
 traffic-shape group 121 70000
 traffic-shape group 120 1000000

access-list 113 permit ip 10.3.0.0 0.0.0.255 eq 80
access-list 120 permit ip any 10.3.0.0 0.0.255.255 precedence 0
access-list 121 permit ip any 10.3.0.0 0.0.255.255 precedence 1
access-list 122 permit ip any 10.3.0.0 0.0.255.255 precedence 2

route-map MIQOS2 permit 10
 match ip address 113
 set ip dscp af30
```

Captura de la conexión VPN con L2TP utilizada en el ejercicio 7:

N.	Origen	Destino	Protocolo	Descripción
1	00:0a:5e:76:8a:2c	ff:ff:ff:ff:ff:ff	ARP	ARP request: Who has 10.1.1.25? Tell 10.1.1.4
2	00:07:0e:8c:8c:ff	00:0a:5e:76:8a:2c	ARP	ARP reply: 10.1.1.25 is at 00:07:0e:8c:8c:ff
3	80.120.2.3	10.1.1.25	L2TP	Control Message - SCCRQ (tunnel id=0, session id=0)
4	10.1.1.25	80.120.2.3	L2TP	Control Message - SCCRP (tunnel id=8, session id=0)
5	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
6	80.120.2.3	10.1.1.25	L2TP	Control Message - SCCCN (tunnel id=8, session id=0)
7	80.120.2.3	10.1.1.25	L2TP	Control Message - ICRQ (tunnel id=8, session id=0)
8	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
9	10.1.1.25	80.120.2.3	L2TP	Control Message - ICRP (tunnel id=8, session id=1)
10	80.120.2.3	10.1.1.25	L2TP	Control Message - ICCN (tunnel id=8, session id=1)
11	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
12	80.120.2.3	10.1.1.25	PPP LCP	Conf. Request (Compression negotiation=CCP)
13	10.1.1.25	80.120.2.3	PPP LCP	Conf. Request (Comp. neg.=CCP, Auth=MS-CHAP2)
14	10.1.1.25	80.120.2.3	PPP LCP	Configuration Ack
15	80.120.2.3	10.1.1.25	PPP LCP	Configuration Ack
16	80.120.2.3	10.1.1.25	PPP LCP	Identification ("MSRAS-PORTATIL-PEPE")
17	10.1.1.25	80.120.2.3	PPP CHAP	Challenge (name="PRINAS")
18	80.120.2.3	10.1.1.25	PPP CHAP	Response (name="C01")
19	00:07:0e:8c:8c:ff	ff:ff:ff:ff:ff:ff	ARP	ARP request: Who has 10.1.1.26? Tell 10.1.1.25
20	01:0a:02:03:10:11	00:07:0e:8c:8c:ff	ARP	ARP reply: 10.1.1.26 is at 01:0a:02:03:10:11
21	10.1.1.25	10.1.1.26	RADIUS	Access-Request (id=13, l=76)
22	10.1.1.26	10.1.1.25	RADIUS	Access-Accept (id=13, l=50)
23	10.1.1.25	80.120.2.3	PPP CHAP	Success
24	80.120.2.3	10.1.1.25	PPP CCP	Configuration Request (no use MPPC, no encription)
25	10.1.1.25	80.120.2.3	PPP CCP	Configuration Request (use MPPC, no encription)
26	80.120.2.3	10.1.1.25	PPP CCP	Configuration Reject (use MPPC, no encription)
27	10.1.1.25	80.120.2.3	PPP CCP	Configuration Ack (no use MPPC, no encription)
28	10.1.1.25	80.120.2.3	PPP CCP	Termination Request
29	80.120.2.3	10.1.1.25	PPP CCP	Termination Ack
30	80.120.2.3	10.1.1.25	PPP IPCP	Configuration Request (IP=0.0.0.0, DNS=0.0.0.0)
31	10.1.1.25	80.120.2.3	PPP IPCP	Configuration Request (IP=10.8.0.1)
32	80.120.2.3	10.1.1.25	PPP IPCP	Configuration Ack (IP=10.8.0.1)
33	10.1.1.25	10.1.1.26	RADIUS	Accounting-Request (User="C01", Status=start)
34	10.1.1.26	10.1.1.25	RADIUS	Accounting-Response (ok)
35	10.1.1.25	80.120.2.3	PPP IPCP	Configuration Nak (IP=10.8.0.21, DNS=10.1.1.4)
36	80.120.2.3	10.1.1.25	PPP IPCP	Configuration Request (IP=10.8.0.21, DNS=10.1.1.4)
37	10.1.1.25	80.120.2.3	PPP IPCP	Configuration Ack (IP=10.8.0.21, DNS=10.1.1.4)
38	00:07:0e:8c:8c:ff	ff:ff:ff:ff:ff:ff	ARP	ARP reply: 10.8.0.21 is at 00:07:0e:8c:8c:ff
39	10.8.0.21	10.4.1.23	ICMP	Echo (ping) request (encapsulated L2TP)
40	00:07:0e:8c:8c:ff	ff:ff:ff:ff:ff:ff	ARP	ARP request: Who has 10.1.1.5? Tell 10.8.0.21
41	00:07:0e:cd:12:3e	00:07:0e:8c:8c:ff	ARP	ARP reply: 10.1.1.5 is at 00:07:0e:cd:12:3e
42	10.8.0.21	10.4.1.23	ICMP	Echo (ping) request
43	10.4.1.23	10.8.0.21	ICMP	Echo (ping) reply
44	10.4.1.23	10.8.0.21	ICMP	Echo (ping) reply (encapsulated L2TP)
45	80.120.2.3	10.1.1.25	PPP LCP	Termination Request
46	10.1.1.25	80.120.2.3	PPP LCP	Termination Ack

N.	Origen	Destino	Protocolo	Descripción
47	10.1.1.25	80.120.2.3	L2TP	Control Message - CDN (tunnel id=8, session id=1)
48	80.120.2.3	10.1.1.25	L2TP	Control Message - StopCCN (tunnel id=8, session id=0)
49	10.1.1.25	80.120.2.3	L2TP	Control Message - ZLB (tunnel id=8, session id=0)
50	10.1.1.25	10.1.1.26	RADIUS	Acc.-Request (User="C01", Status=stop)
51	10.1.1.26	10.1.1.25	RADIUS	Accounting-Response (ok)

Esquema de interconexión de redes para las cuestiones del examen (excepto pregunta 6):



Sistemas de Transporte de Datos – I. Informática (9186)
Noviembre/Diciembre 2009 - Control de prácticas

Nombre: _____ **DNI:** _____

Apellidos: _____

Firma:

SOLUCIÓN

- Nota Final = 60% Control de Teoría + 40% Control de Prácticas.
- La entrega de este control implica el uso de una convocatoria.
- El control se debe completar con bolígrafo.
- Las preguntas respondidas erróneamente no restan puntuación.
- Las preguntas se deben contestar completando los recuadros correspondientes. No se evaluará lo escrito fuera de estas opciones.
- Se puede separar la última página si así resulta más fácil consultar los anexos.
- El tiempo para realizar este examen es de 1 hora y 15 minutos.

Preguntas

1. Dado el esquema de interconexión de redes del Anexo (página 7), completa las tablas de encaminamiento de los routers R2 y R3 cumpliendo las siguientes condiciones (2,5 puntos):

a) Se debe asegurar la interconexión entre todos los equipos que haya en las LAN (Ethernet, Anillo y WiFi) y en las VPN del esquema, cumpliendo los siguientes apartados.

b) Los equipos de las redes LAN pueden acceder a Internet por la conexión a Internet más cercana.

c) Los paquetes se deben encaminar por el camino que implique un **menor número de saltos**, teniendo en cuenta el siguiente orden de prioridad para las redes en caso de igualdad de saltos: Ethernet, Anillo, ATM, WiFi, RDSI.

d) En las tablas de encaminamiento, se deben incluir también las redes y destinos conectados directamente, indicando como puerta de enlace la dirección IP del interfaz local correspondiente junto con la letra "**D**".

e) Las direcciones IP de los enlaces ADSL, ATM y RDSI sólo se deben considerar en las tablas de los routers en los que sea necesario.

f) Las tablas de encaminamiento deben ser lo más sencillas posible, teniendo en cuenta los aspectos anteriores.

g) Para simplificar las tablas, se debe agregar subredes y disminuir la máscara cuando sea posible.

h) Para que una entrada se considere correcta, debe tener su destino, máscara y puerta de enlace correctos.

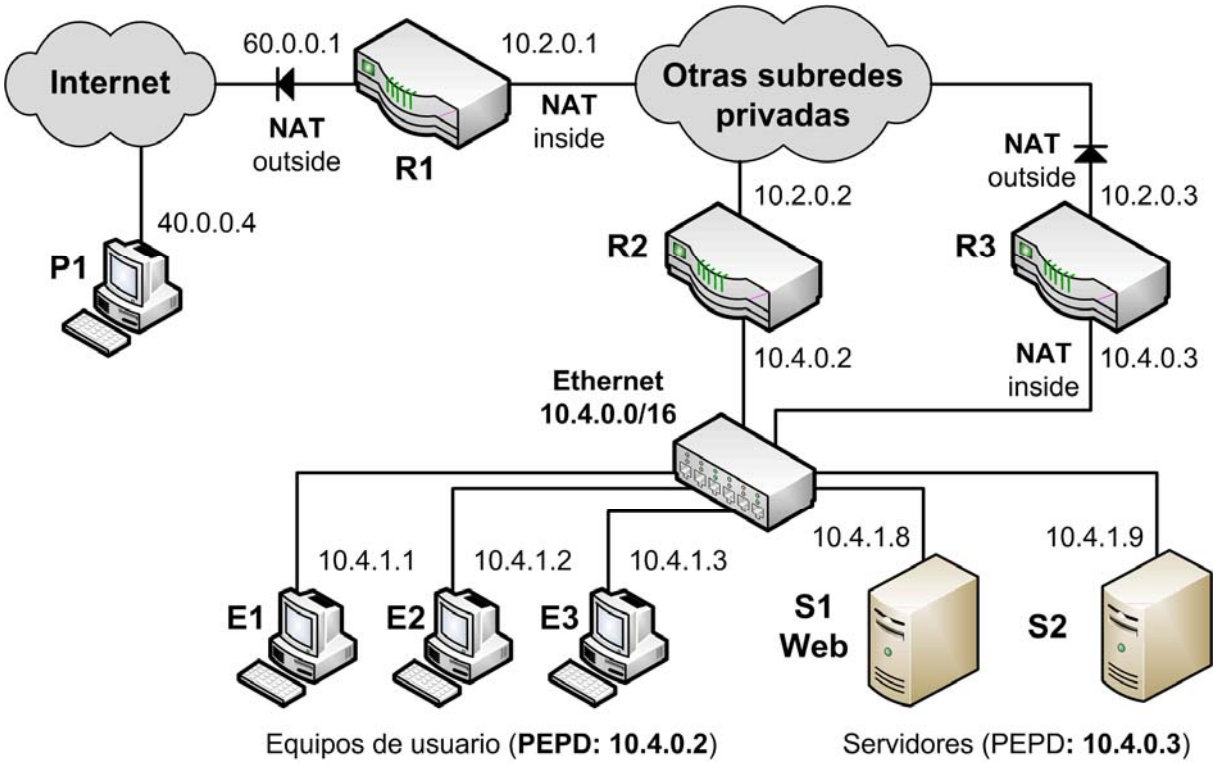
Router R5

Destino	Máscara	Puerta Enlace
85.4.5.8	*32*	*85.4.5.9 D*
10.3.8.0	*24*	*10.3.8.2 D*
10.3.9.0	*24*	*10.3.9.1 D*
10.2.3.0	*24*	*10.2.3.2 D*
10.2.1.0	*24*	*10.2.3.1*
10.1.1.0	*24*	*10.2.3.1*
10.1.2.0	*24*	*10.2.3.1*
10.5.0.0	*16*	*10.2.3.1*
10.4.0.0	*16*	*10.2.3.1*
10.1.3.0	*24*	*10.1.3.8*
10.2.2.0	*24*	*10.3.9.2*
0.0.0.0	*-*	*85.4.5.8*

Router R6

Destino	Máscara	Puerta Enlace
10.3.8.0	*24*	*10.3.8.1 D*
10.1.3.0	*24*	*10.1.3.2 D*
10.1.2.0	*24*	*10.1.3.1*
10.1.1.0	*24*	*10.1.3.1*
10.5.0.0	*16*	*10.1.3.1*
0.0.0.0	*-*	*10.3.8.2*

2. La red de una organización se estructura según el siguiente esquema. El router R1 actúa como cortafuegos para toda la red privada, el router R2 actúa como PEPD (Puerta de Enlace Por Defecto) para los equipos de usuario (E1, E2…) de la subred 10.4.0.0/16, y el router R3 actúa como un segundo cortafuegos y PEPD para los servidores (S1, S2…). (1,5 puntos).



Considérese que en R3 se ejecutan estos comandos Cisco-IOS para configurar su NAT:

```
interface Eth1
  ip address 10.2.0.3 255.255.0.0
  ip nat outside
interface Eth2
  ip address 10.4.0.3 255.255.0.0
  ip nat inside
ip nat inside source list 100 interface Eth1 overload
ip nat inside source static tcp 10.4.1.8 80 interface Eth1 8080
access-list 100 permit ip 10.4.0.0 0.0.255.255 any
```

Se pide definir las siguientes configuraciones de NAT en base a la configuración anterior del NAT de R3, indicando para ello las direcciones IP y los PUERTOS adecuados:

a) Entrada estática del NAT necesaria en R1 para que el servicio Web de S1 sea accesible desde equipos de Internet mediante la dirección pública 60.0.0.1 y el puerto 80.

b) Indicar entrada dinámica que genera el NAT de R1 cuando el equipo P1 accede al servicio Web de S1, usando como puerto cliente el número 1.025.

c) Indicar entrada dinámica que genera el NAT de R3 para el mismo caso que en b).

Pregunta	Inside global	Inside local	Outside local	Outside global
a) NAT R1	*60.0.0.1:80*	*10.2.0.3:8080*	-	-
b) NAT R1	*60.0.0.1:80*	*10.2.0.3:8080*	*40.0.0.4:1025*	*40.0.0.4:1025*
c) NAT R3	*10.2.0.3:6060*	*10.4.1.8:80*	*40.0.0.4:1025*	*40.0.0.4:1025*

Si en R3 sólo está la configuración de NAT listada antes, ¿Qué pasa si el equipo E1 accede al servicio Web de la dirección 10.2.0.3 que es redirigido a S1?

d) No hay conexión porque E1 ignora los paquetes de respuesta que recibe desde S1 debido a que la dirección origen de esos paquetes no es la correcta.

e) No hay conexión porque los paquetes de respuesta que envía S1 hacia E1 se envían a través de R3 en vez de ir directamente por la red 10.4.0.0/16, ya que R3 es la PEPD de S1.

f) Se establece una conexión TCP entre un puerto cliente de E1 y el puerto 80 de S1 directamente por la red 10.4.0.0/16 sin necesidad de routers intermedios.

g) Se establece una conexión TCP entre un puerto cliente de E1 y el puerto 8080 de S1 a través del router R3.

De las siguientes listas de comandos de Cisco IOS, ¿Cuál se podría añadir en R3 para que los equipos E1, E2… puedan acceder al servidor Web de S1 a través de la dirección 10.2.0.3?

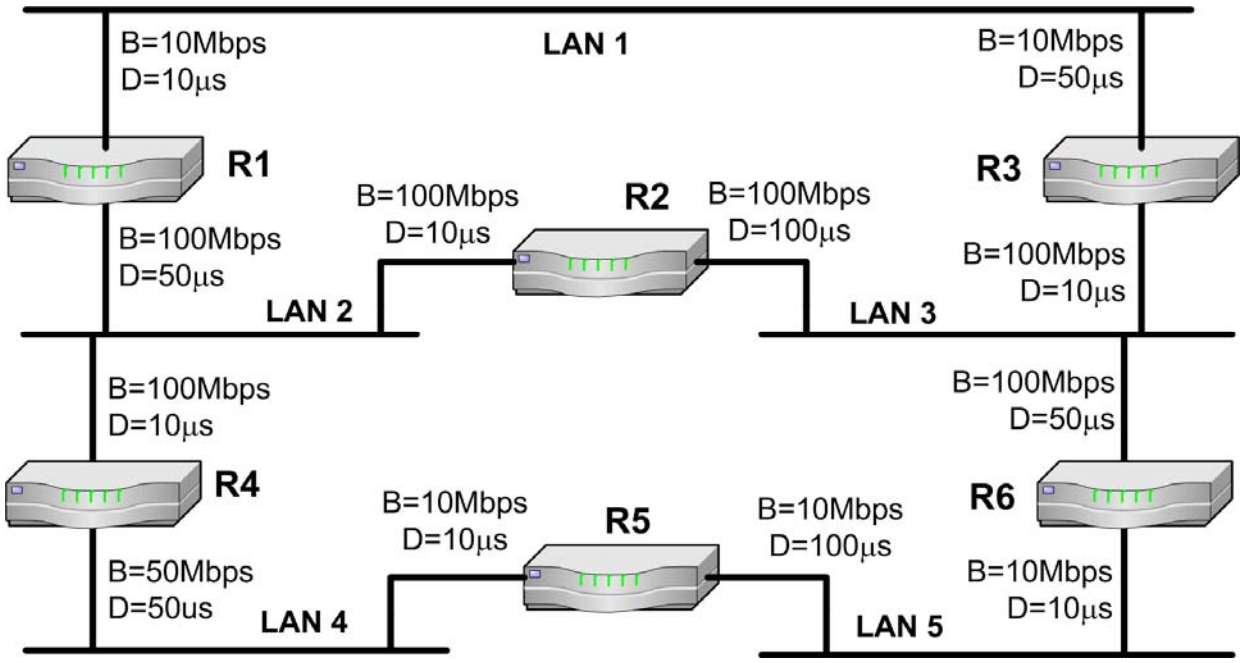
h)
```
ip nat inside source static tcp 10.4.1.8 80 interface Eth1 80
```

i)
```
ip nat pool ipsnuevas 10.2.0.4 10.2.0.254 netmask 255.255.0.0
ip nat inside source list 101 pool ipsnuevas
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
```

j)
```
ip nat pool ipsnuevas 10.40.0.1 10.40.0.254 netmask 255.255.0.0
ip nat outside source list 101 pool ipsnuevas
access-list 101 permit tcp 10.4.0.0 0.0.255.255 host 10.2.0.3 eq 8080
```

k)
```
ip nat pool ipsnuevas 10.40.0.1 10.40.0.254 netmask 255.255.0.0
ip nat outside source list 101 pool ipsnuevas
access-list 101 permit any host 10.4.1.8 eq 80
```

3. **En los routers del siguiente esquema está activo EIGRP. Teniendo en cuenta los parámetros de ancho de banda (B) y retardo (D) de los interfaces, se pide determinar los valores de métrica de EIGRP de los cuatro posibles caminos que hay desde el router R1 a la red LAN 5. Numera los caminos del mejor (1) al peor (4) según la métrica de EIGRP (1 punto).**



Camino (lista de redes)	Mín(Bi) (Kbps)	Sum(Di) (µs)	Valor de métrica EIGRP	Núm.
LAN1, LAN3, LAN5	*10.000*	*30*	*$256\cdot(10^7/10.000 + 30/10) = 256.768$*	*1*
LAN2, LAN4, LAN5	*10.000*	*200*	*$256\cdot(10^7/10.000 + 200/10) = 261.120$*	*4*
LAN2, LAN3, LAN5	*10.000*	*160*	*$256\cdot(10^7/10.000 + 160/10) = 260.096$*	*2*
LAN1, LAN3, LAN2, LAN4, LAN5	*10.000*	*180*	*$256\cdot(10^7/10.000 + 180/10) = 260.608$*	*3*

4. **En el esquema de red del Anexo (página 7) se define un túnel IP-IP con origen 10.9.9.4 y destino 10.1.2.2. Además en el router R2 se configura la siguiente entrada de encamientamiento donde "tunel0" es el interfaz del túnel (1 punto).**

Router R2

Destino	Máscara	Interfaz
10.3.8.0	*24*	*Tunel0 (Directo)*

Teniendo en cuenta las condiciones de encaminamiento de paquetes del ejercicio 1, si equipo PC1 ejecuta el comando "*ping –n 1 10.3.8.2*", ¿Qué camino seguirá el mensaje "Echo request"? Indicar el camino como la lista de routers incluyendo los equipos origen y destino.

PC1 -> [R2 -> R7 -> R1 -> R3] -> R6 –>R5

Indica las direcciones IP de los protocolos pasajero y portador del mensaje ECHO REQUEST cuando este llega al interface 10.1.2.2 de R3.

Origen del pasajero:	*10.2.1.2*	Origen del portador:	*10.9.9.4*
Destino del pasajero:	*10.3.8.2*	Destino del portador:	*10.1.2.2*

Si el paquete del mensaje ECHO REQUEST parte con un valor de TTL=128 del PC1, ¿Con qué valor de TTL llega al destino 10.3.8.2? (considérese que el túnel cuenta como un único salto) *126*

5. Una organización permite el acceso a su red local privada mediante una VPN que utiliza los protocolos L2TP, pero sin seguridad IPSec. Además, se utiliza un servidor RADIUS para gestionar los posibles usuarios de la VPN. (2 puntos)

Supóngase que un equipo de Internet se conecta como cliente de VPN al NAS (Network Access Server, o servidor de VPN) de la organización, y durante la conexión ejecuta un "ping" a un equipo de la red privada. La conexión de VPN finaliza por iniciativa del cliente.

En la siguiente tabla se listan distintas tramas desencadenadas durante la conexión del cliente a la VPN de manera desordenada. Se pide completar la tabla indicando la función que desempeña cada trama según la tabla de descripciones que hay en el Anexo (página 8), y el número de orden dentro de la conexión, desde el 1 para primera hasta el 20 para la última.

Protocolo: trama	Función	Orden
ICMP: Echo request	*13*	*11*
ICMP: Echo reply	*14*	*12*
PPP-CHAP: Response	*10*	*4*
PPP-CHAP: Success	*11*	*7*
PPP-CHAP: Challenge	*9*	*3*
PPP-LCP: Termination Request	*3*	*13*
PPP-LCP: Termination Ack	*4*	*14*
PPP-LCP: Configuration Request	*15*	*1*
PPP-LCP: Configuration Ack	*16*	*2*
RADIUS: Accounting Request (Stop)	*5*	*15*
RADIUS: Accounting Response	*6*	*16*
RADIUS: Access Request	*7*	*5*
RADIUS: Access Accept	*8*	*6*
PPP-IPCP: Configuration Request	*1*	*8*
PPP-IPCP: Configuration Nak	*2*	*9*
ARP Gratuitous	*12*	*10*

Dibújese el formato de la trama con el mensaje ICMP de "echo request" que envía el cliente por la conexión de la VPN a través de Internet, indicando claramente estos aspectos:

a) Los protocolos de las diferentes cabeceras desde nivel de enlace hasta ICMP (incluidas éstas) en el orden correcto, contando las cabeceras que incluyen los protocolos de L2TP.

b) Cuáles son los protocolos portador, de encapsulación y pasajero.

Ethernet	*IP*	*UDP*	*L2TP*	*PPP*	*IP*	*ICMP*

Portador: UDP (trasporte)
Encapsulación: L2TP
Pasajero: PPP (enlace)

6. Dado el esquema de red del Anexo (página 7), se configura como punto de acceso para la red 10.3.9.0/24 el 10.3.9.1, y como punto de acceso para la red 10.3.8.0/24 el 10.3.8.1. También se conoce los siguientes valores para las direcciones de MAC de los equipos: (2 puntos)

IP	MAC	IP	MAC	IP	MAC	IP	MAC
10.3.9.1	A	10.3.9.2	B	10.3.9.5	C	10.3.8.1	D
10.3.8.2	E	10.2.3.2	F	10.2.3.1	G	10.2.2.1	H

Completa la siguiente tabla con las tramas que se generarán si el equipo PC2 ejecuta el comando "*ping –n 1 10.3.9.2*" y a continuación el comando "*ping –n 1 10.3.9.1*" (no es necesario tener en cuenta el orden de las direcciones MAC).

Orden	Dir. MAC 1	Dir. MAC 2	Dir. MAC 3	IP origen	IP destino	Tipo ICMP
1	*C*	*B*	*A*	*10.3.9.5*	*10.3.9.2*	*Echo request*
2	*B*	*C*	*A*	*10.3.9.2*	*10.3.9.5*	*Echo reply*
3	*C*	*A*	*A*	*10.3.9.5*	*10.3.9.1*	*Echo request*
4	*A*	*C*	*A*	*10.3.9.1*	*10.3.9.5*	*Echo reply*
5						
6						

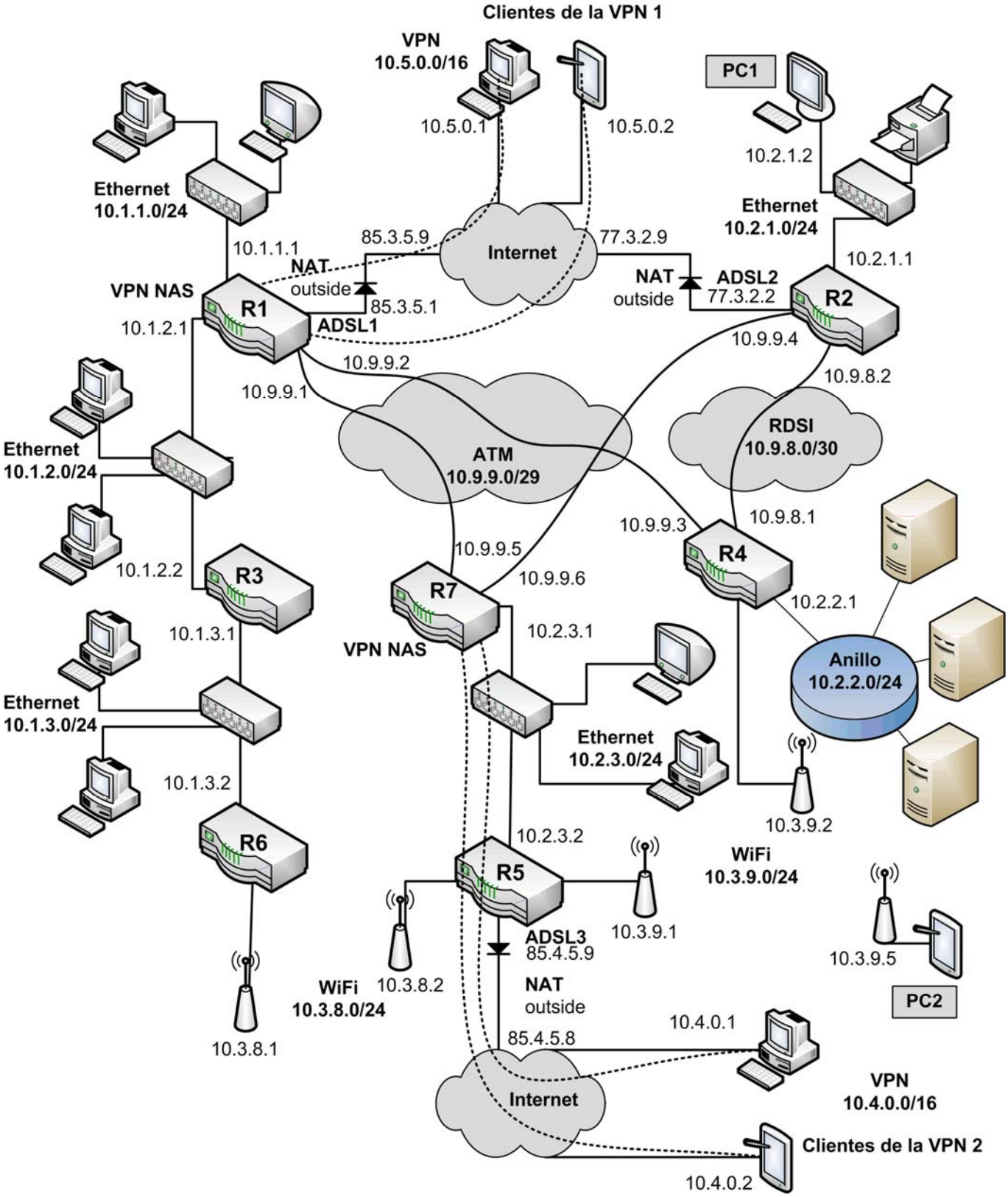
Considerando que la siguiente trama representa la encapsulación IEEE 802.3 que se ha aplicado a una trama IEEE 802.11 de la red, se pide dibujar el formato de dicha trama 802.11.

MAC origen	MAC destino	Tipo	IP origen	IP destino	Datos
E	D	0x800h	10.3.8.2	10.3.8.1	ICMP

Control	*MAC1:E*	*MAC2: D*	*MAC3: D*	*Secuencia*	*LLC*	*IP*	*ICMP*

Anexo

Esquema de red para los ejercicios 1 (encaminamiento), 4 (túnel IP-IP) y 6 (WiFi):



Funciones para asignar a las tramas del ejercicio 5 (VPN):

Función	Descripción
1	El cliente informa al NAS sobre su configuración IP actual para que el NAS la valide.
2	El NAS rechaza la configuración IP del cliente y le da una válida para la VPN.
3	El cliente solicita finalizar la conexión PPP.
4	El NAS acepta la finalización de la conexión PPP.
5	El NAS envía información a la base de datos de usuarios sobre estadísticas de la conexión del cliente.
6	La base de datos de usuarios confirma que la información del cliente se ha actualizado correctamente.
7	El NAS accede a la base de datos de usuarios para comprobar la autenticidad del cliente.
8	La base de datos de usuarios informa al NAS que el cliente es válido.
9	El NAS pide al cliente que se autentifique.
10	El cliente envía su identificador de usuario y su contraseña de acceso al NAS.
11	El NAS envía al cliente la aceptación de su autentificación.
12	El NAS indica a los equipos de la red local privada de que él atiende los paquetes dirigidos al cliente de la VPN.
13	El cliente envía un ping a un equipo de la red local privada.
14	Un equipo de la red local privada contesta al ping que ha ejecutado el cliente.
15	El NAS propone opción de protocolo de autentificación al cliente (CHAP).
16	El cliente acepta el protocolo de autentificación que propone el NAS.