



*Este examen consta de 7 ejercicios con un total de 65 puntos. Utilice letra clara y escriba únicamente en el espacio reservado. Cada 10 errores ortográficos restan 5 puntos a la nota total. No está permitido el uso de calculadora.*

Apellidos: \_\_\_\_\_ Nombre: \_\_\_\_\_ Grupo: \_\_\_\_\_

1. (8p) Enumere y explique la utilidad de los 6 flags que aparecen en la cabecera TCP.

- URG: Activa el puntero urgente.
- ACK: El segmento contiene información de reconocimiento.
- PSH: Los datos deben entregarse inmediatamente
- RST: Rechaza un intento de conexión o resetea una conexión activa
- SYN: Se utiliza durante el proceso de conexión
- FIN: Se utiliza durante el proceso de desconexión

2. (7p) Explique, con ayuda de esquemas y diagramas, qué es, qué problema resuelve y cómo funciona el mecanismo NAT (*Network Address Translation*).

NAT es una técnica que permite a un conjunto de hosts con direcciones privadas acceder a una red pública empleando unas pocas direcciones públicas (normalmente una).

Al recibir un paquete procedente de un host de la red interna, el enrutador NAT traduce la dirección origen (privada) por una pública disponible y apunta ambas en su tabla NAT. Al recibir la respuesta del servidor público, realiza la traducción inversa (esta vez en la dirección destino), y entrega el paquete al host correspondiente en la red interna.

3. (8p) Explique en qué consiste el *síndrome de la ventana tonta*.

Cuando los acuses de recibo indican ventanas receptoras pequeñas, el emisor crea y envía segmentos pequeños. Eso provoca un importante desperdicio en los recursos de la red y del host.

4. (7p) Explica cuales serían los inconvenientes de utilizar un sistema de direccionamiento de red basado en MAC.

Las direcciones MAC son planas, no sería sencillo asignar direcciones a las redes ni establecer correspondencias con los hosts que hay en ellas; eso también complicaría el enrutamiento.

Al estar ligada la dirección MAC al NIC es complicado cambiar dichas direcciones e interoperar con dispositivos de red que tengan direcciones de enlace con formatos distintos.



5. (7p) La figura muestra la topología de red de una empresa compuesta por 5 redes Ethernet interconectadas mediante enrutadores. Se muestran las direcciones IP y el último octeto de la dirección MAC de cada interfaz de red. La máscara de red de todas las redes es 255.255.255.0.

Indique las rutas que seguirán los datagramas entre cada pareja de hosts. Se muestran algunos resultados como ejemplo:

- **A hacia A:** A ->A
- **A hacia B:** A ->R2 ->R4 ->B
- **A hacia C:** A ->R2 ->R4 ->R3 ->R6 ->C
- **A hacia D:** A ->R2 ->D
- **A hacia E:** A ->R2 ->E
- **B hacia A:** B ->R1 ->A
- **B hacia B:** B ->B
- **B hacia C:** B ->R1
- **B hacia D:** B ->R4 ->D
- **B hacia E:** B ->R4 ->E
- **C hacia A:** C ->R6 ->R5 ->R4 ->R3 ->R6...
- **C hacia B:** C ->R6 ->R5 ->B
- **C hacia C:** C ->C
- **C hacia D:** C ->R6 ->R5 ->R4 ->D
- **C hacia E:** C ->R6 ->R5 ->R4 ->E
- **D hacia A:** D ->R4 ->R3 ->R6 ->R5 ->R4...
- **D hacia B:** D ->R4 ->B
- **D hacia C:** D ->R4 ->R3 ->R6 ->C
- **D hacia D:** D ->D
- **D hacia E:** D ->E
- **E hacia A:** (depende de la tabla de E)
- **E hacia B:** (depende de la tabla de E)
- **E hacia C:** (depende de la tabla de E)
- **E hacia D:** E ->D
- **E hacia E:** E ->E



6. (8p) Teniendo en cuenta las tablas de enrutamiento mostradas en la figura, explica si las siguientes tramas Ethernet son posibles. Indica en qué redes pueden aparecer y en cuales no.

- Una trama con origen :c3 y destino :c1 cuya carga es un paquete IP.

Sí, en la red 212.1.1.0/24 si D (:c3) envía un paquete IP a R2 (:c1)

- Una trama con origen :e1 y destino :e2 cuya carga es un paquete IP con origen 212.1.3.3 y destino 212.1.0.1

Sí, en la red 212.1.3.0/24 cuando C (212.1.3.3) envía paquetes IP a A (212.1.0.1).

- Una trama con origen :e2 y destino :e1 cuya carga es una petición ARP preguntando por la dirección 212.1.3.3

No, el destino de una petición ARP debería ser siempre broadcast.

- Una trama con origen :e2 y destino ff:ff:ff:ff:ff:ff cuya carga es una petición ARP preguntando por la dirección 212.1.1.5

No tiene sentido que la interfaz :e2 de R5 pregunte por la MAC de interfaz 212.1.1.5 de R4 ya que no es un vecino de la red 212.1.3.2.

- Una trama con origen :c3 y destino :c4 cuya carga es una respuesta ARP con dirección origen 212.1.1.2

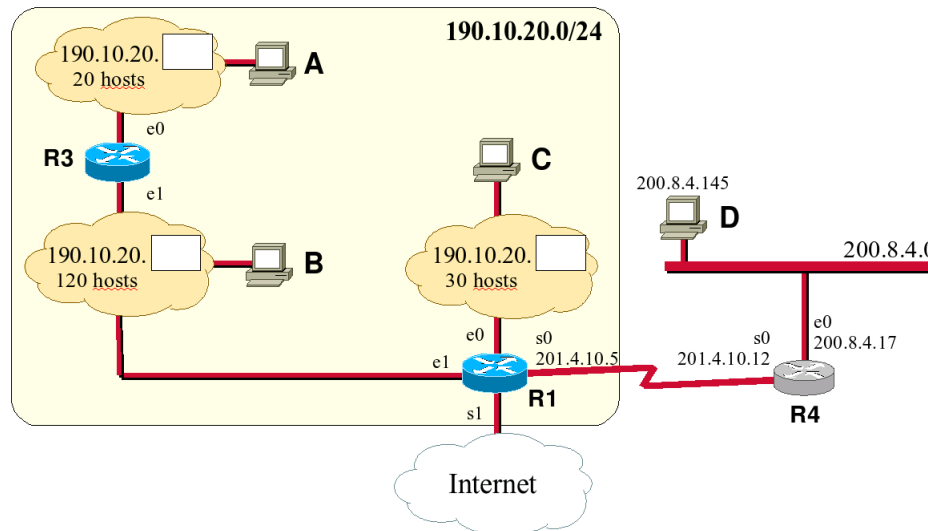
No, si es una respuesta ARP de D (212.1.1.9) con destino a E, la dirección origen debe ser 212.1.1.9 (D).

Ha llegado al host B un segmento UDP procedente de A, destinado al puerto 8000 de B. Indique el valor de todos los campos que conozca de las cabeceras Ethernet e IP que transportan el segmento, y de la cabecera del propio segmento UDP. Suponga que el TTL de los paquetes enviados por A es 64.

- Ethernet: origen(:b3), destino(:b2), tipo(IP), payload(paquete IP)
- IP: origen(212.1.0.1), destino(212.1.4.4), TTL(62), tipo(UDP), payload(segmento UDP)
- UDP: destino(8000)



7. (20p) Una empresa ha abierto otra sucursal. En la siguiente figura aparece la topología propuesta para dicha sucursal (enmarcada), un enlace serie con otra sucursal distante y un acceso a Internet a través del enrutador R1. La nueva sucursal tiene asignada la red 190.10.20.0/24.



Aplicando *subnetting*, indica para cada una de las tres subredes: dirección de red, máscara, dirección de broadcast y nº de direcciones que quedan libres, teniendo en cuenta las necesidades de cada una. Sobre la figura, asigna direcciones a todos los interfaces de los enrutadores y a los hosts.

**Red B:** 190.10.20.0/25, broadcast: 190.10.20.127 (6 direc. sin usar)  
**Red A:** 190.10.20.128/26, broadcast: 190.10.20.191 (42 direc. sin usar)  
**Red C:** 190.10.10.192/26, broadcast: 190.10.10.255 (32 direc. sin usar)

Indica qué paquetes aparecen en la red de la figura (tanto de hosts como de enrutadores) como consecuencia de que el host A envíe un paquete IP al host D. Se supone que todas las cachés ARP están vacías.

A contruye un paquete IP con origen=IP de A y destino=IP de D  
A envía ARP Request a su red preguntando por la MAC de R3.  
R3 envía ARP Reply a A indicando la MAC de su iface e0.  
A encapsula el paquete IP en una trama Ethernet y la envía a R3.  
R3 envía ARP Request a la red 190.10.20.0/25 preguntando por la MAC de R1.  
R1 envía ARP Reply a R3 indicando la MAC de su iface e1.  
R3 envía a R1 el paquete IP original encapsulado en una trama Ethernet.  
R1 empaqueta el paquete IP en una trama PPP y lo envía por su iface s0 a R4.  
R4 envía ARP Request a la red 200.8.4.0/24 preguntado por la MAC de D.  
D envía ARP Reply a R4 indicando su MAC.  
R4 envía a D el paquete IP original encapsulado en una trama Ethernet.

Escribe la tabla de enrutamiento de R1.

destino/mask - next hop - iface  
190.10.20.0/25 - ED - e1  
190.10.20.128/26 - R3 - e1  
190.10.10.192/26 - ED - e0  
200.8.4.0/24 - R4 - s0  
default - ? - s1