Primer control de Xarxes de Computadors (XC), Grado en Ingeniería Informática		20/04/2021	Primavera 2021
NOMBRE:	**APELLIDOS:**	**GRUPO**	**DNI**

Duración: 1h30m. El test se recogerá en 25 minutos. Responder los problemas en el mismo enunciado.

Test. (3,5 puntos) Las preguntas valen la mitad si hay un error y 0 si hay más de uno.

1. Marca las afirmaciones correctas sobre rangos de direcciones del protocolo IP:
- ☐ La red 14.0.0.0/8 es clase B.
- ☒ La red 14.0.0.0/8 es clase A.
- ☒ La red 192.168.0.0/24 es privada.
- ☒ La subred 1.1.1.252/30 es válida.

2. La sumarización a la clase de las direcciones IP:
- ☐ 147.83.0.0/24 y 147.83.1.0/24 es 147.83.0.0/23.
- ☒ 147.83.0.0/24 y 147.83.1.0/24 es 147.83.0.0/16.
- ☐ 147.83.0.0/24 y 147.83.1.0/24 es 147.83.0.0/8.
- ☐ 147.83.0.0/24 y 147.183.1.0/24 es 147.83.0.0/8.

3. Cuando se fragmenta un paquete IPv4 en el camino de origen a destino, al llegar a destino:
- ☒ No todos los fragmentos del mismo paquete han de tener el mismo TTL.
- ☒ Todos los fragmentos del mismo paquete tienen el mismo identificador de fragmento.
- ☐ Todos los fragmentos del mismo paquete tienen el mismo fragment offset.
- ☐ Todos los fragmentos del mismo paquete tienen los mismos flags.

4. Marca las afirmaciones correctas sobre el protocolo DHCP:
- ☒ Los clientes comienzan enviando mensajes broadcast, a la dirección IP 255.255.255.255.
- ☒ DHCP puede configurar varios parámetros de un host, no solo asignar dirección IP.
- ☒ En una red pueden haber múltiples servidores DHCP y responder todos.
- ☐ Clientes y servidores comienzan enviando mensajes a la dirección IP de broadcast de su red IP.

5. Marca las afirmaciones correctas sobre el comando ping:
- ☐ Envía paquetes IP con el flag “Don't Fragment”.
- ☐ Si no hay respuesta, indica que no pueden llegar paquetes IP a la dirección IP de destino.
- ☐ Envía paquetes IP con TTL creciente y espera como respuesta ICMP error: time exceeded.
- ☒ Envía ICMP echo request y espera como respuesta ICMP echo reply.

6. Marca las afirmaciones correctas sobre el “Gratuitous ARP”:
- ☐ Permite hacer ping a otras direcciones por ARP.
- ☒ Cuando se activa un interfaz, por ejemplo por DHCP, permite detectar conflicto por duplicidad.
- ☒ Se envía sin esperar a tener que enviar un paquete IP a otro host.
- ☐ Se envía cuando se hace un ping a una dirección IP de la misma red.

7. Marca las afirmaciones correctas sobre el protocolo RIP versión 2:
- ☒ Las actualizaciones de rutas se envían solo a los vecinos.
- ☒ Las actualizaciones de rutas también se envían periódicamente aunque no haya cambios.
- ☒ El método “split horizon” sirve para reducir el tiempo de convergencia.
- ☐ El número máximo de saltos en una red es 16.

8. Marca las afirmaciones correctas sobre el mecanismo PAT en un router al salir un paquete IP de una red privada a una pública:
- ☐ Cambia la IP origen manteniendo siempre el puerto de origen.
- ☒ Cambia la IP origen manteniendo siempre el puerto de destino.
- ☒ Cambia la IP origen pudiendo cambiar el puerto de origen.
- ☐ Cambia la IP origen pudiendo cambiar el puerto de destino.

Control de Xarxes de Computadors (XC)	Grau en Ingeniería Informàtica	20/04/2021	Primavera 2021
Nom	Cognoms	Grup	DNI

Duració: 1h30m. El test es recollirà en 25 minuts. Respondre els problemes en el mateix enunciat.

Problema 1. 4 punts. Tots els apartats valen igual. Escriu al dors si necessites més espai. Indica si necessites alguna dada que no dóna l'enunciat.

Una xarxa comunitària (per exemple guifi.net) consisteix en una infraestructura de xarxa construïda pels mateixos usuaris. En aquest context és normal fer servir el terme *node* per referir-se als routers que els usuaris afegeixen per construir la infraestructura comunitària. Suposa una xarxa comunitària on s'assignen blocs d'adreces IP de la xarxa 10.0.0.0/8 a zones geogràfiques. Els routers dels nodes es configuren perquè totes les zones de la xarxa comunitària siguin accessibles. Quan un usuari afegeix un node a una zona se li assignen adreces del bloc. Suposa que una zona *Z* té assignat el bloc 10.1.8.0/21, i als nodes d'aquesta zona s'assignen seqüencialment subxarxes /27, començant per les numèricament més petites. És a dir, al primer node que es crea en la zona *Z* s'assigna la subxarxa 10.1.8.0/27, i així successivament. Contesta les següents preguntes, justifica les respostes.

1. Quants nodes es poden crear en la zona *Z*? És a dir, quantes subxarxes /27 es poden crear en el bloc 10.1.8.0/21?

   subnetid $= 27 - 21 = 6$ bits
   Es poden crear $2^6 = 64$ subxarxes, per tant, 64 nodes.

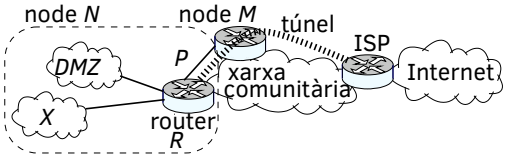
2. Quina és l'adreça que s'assignarà a l'últim node de la zona *Z*? És a dir, quina és la última subxarxa /27 del bloc 10.1.8.0/21? Dóna la resposta amb la notació amb punts.

   El subnetid de la subxarxa assignada a l'últim node serà 111.111_2, on el punt separa els bits del byte 3 i 4.
   En decimal: $111_2 = 7$ i $1110000_2 = 128 + 64 + 32 = 224$
   Per tant, la subxarxa assignada a l'ultim node serà: `10.1.(8+7).(0+224) = 10.1.15.224/27`

3. Suposa que es crea un node *N* en la zona *Z* i obté la subxarxa 10.1.11.32/27. Quants nodes hi ha en *Z* un cop creat el node *N*?

   $11 = 8 + 2 + 1 = 1011_2$ i $32 = 0010000_2$, on s'han subratllat els bits que pertanyen al subnetid.
   El subnetid és $011001_2 = 16 + 8 + 1 = 25$. Per tant, s'han creat 26 nodes (que tenen subnetid en decimal: 0, 1, $\cdots 25$).

4. Suposa que un node *N* obté la IP 10.1.8.0/27, i vol utilitzar les adreces d'aquest bloc per a les subxarxes *P*, *DMZ* i *X* que mostra la figura; on: *P* és un enllaç punt a punt amb un altre node *M* de la xarxa comunitària; *DMZ* és una xarxa on hi haurà 2 servidors, i *X* és una xarxa tan gran com sigui possible, amb les adreces de 10.1.8.0/27 que quedin disponibles. Omple la taula següent amb les adreces de les subxarxes, tenint en compte que es vol que estiguin ordenades numèricament en odre creixent (*P* les més petites, *X* les més grans).



xarxa	adreça IP/mask
P	10.1.8.0/30
DMZ	10.1.8.8/29
X	10.1.8.16/28

xarxa	subnetid (bits)
P	000xx
DMZ	01xxx
X	1xxxx

Amb /29 en la *DMZ* hi podem posar $2^3 - 2 - 1 = 5$ dispositius.

5. En la xarxa comunitària hi ha un ISP que dóna un servei d'accés a Internet (notar que hi pot haver altres ISPs). Els usuaris que contracten el servei d'aquest ISP obtenen una IP pública fixa (diferent per a cada node), i accedeixen al router de l'ISP amb un túnel IPinIP que connecta el router del node de l'usuari amb l'ISP a través de la xarxa comunitària. L'ISP encamina els datagrames de la sortida dels túnels cap a Internet. Pel node *N* de l'apartat 4, en el costat de l'ISP s'ha creat la interfície túnel `tunN` amb la IP local (entrada al túnel): 10.30.30.1; i la IP remota (sortida del túnel): 10.1.8.1. Per exemple, `tunN` es podria crear amb la comanda:
   `ISP# ip tunnel add tunN mode ipip local 10.30.30.1 remote 10.1.8.1`
   Digues quines seran les adreces IP que s'hauran de fer servir al crear la interfície túnel en el router *R* del node *N*:

IP local (entrada al túnel)	10.1.8.1
IP remota (sortida del túnel)	10.30.30.1

Es configuraran les mateixes IPs que a l'altra costat del túnel amb l'ordre canviat

6. Suposa que al node *N* de l'apartat 4 l'ISP ha assignat l'adreça IP fixa 40.0.0.35 per accedir a Internet. Justifica per què el router *R* del node *N* haurà de fer PAT (port-NAT) quan s'envien datagrames pel túnel cap a l'ISP. Explica quin és el canvi d'adreces que es farà als datagrames que surten del router *R*, tot indicant en la taula següent si el canvi es farà en la capçalera externa o interna, si el canvi es farà en l'adreça IP origen o destinació, i quina és l'adreça IP a la que es farà el canvi.

capçalera (interna/externa)	interna
adreça (origen/ destinació)	origen
adreça IP a la que es canvia	40.0.0.35

Haurà de fer PAT amb la única adreça pública que té el node *N*: 40.0.0.35. El canvi es farà en l'adreça origen de la capçalera interna, que és la capçalera que l'ISP enviarà cap a Internet a la sortida del túnel.

7. Suposa que en el node *N* de l'apartat 4 un PC de la xarxa *X* té l'adreça IP 10.1.8.18. Des d'aquest PC s'executa la comanda ping 147.83.10.10. Digues quines seran les adreces IP de la capçalera externa i interna del missatge ping que enviarà el router *R* del node *N* cap a l'ISP de la xarxa comunitària.

capçalera externa		capçalera interna	
adreça origen	adreça destinació	adreça origen	adreça destinació
10.1.8.1	10.30.30.1	40.0.0.35	147.83.10.10

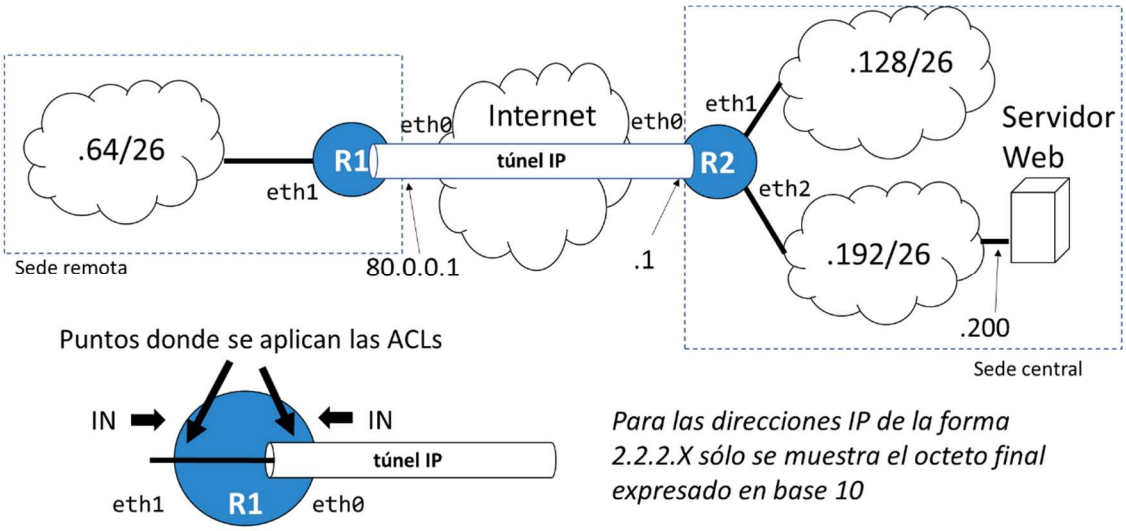
El PAT del router *R* canviarà la IP origen 10.1.8.18 per 40.0.0.35 en la capçalera interna (farà PAT a l'encaminar per la interfície del túnel, per exemple `tun0`).

Control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		20/4/2021	Primavera 2021
NOM (MAJÚSCULES):	COGNOMS (MAJÚSCULES):	GRUP:	DNI:

Duració: 1h30m total. El test es recollirà en 25 minuts.

P2 (2,5 puntos). Conectamos una red situada en una sede remota de una empresa (red de la izquierda en la figura) con la central (redes de la derecha). Dicha conexión se establece a través de un túnel IP con terminaciones en los interfaces `eth0` del router R1, en la sede remota, y `eth0` del router R2, en la sede central.

La empresa dispone del bloque de direcciones (públicas) 2.2.2.0/24, y hemos hecho el subnetting que se muestra en la figura. Los interfaces de R1 y R2 que dan acceso a Internet tienen asignadas las direcciones IP: 80.0.0.1 (`eth0`, R1) y 2.2.2.1 (`eth0`, R2).



Queremos configurar listas de acceso (ACLs) en dichos interfaces `eth0` y `eth1` de R1. Debemos tener en cuenta lo siguiente (ver figura):

- Las listas de acceso solo se aplicarán a los paquetes que entren a cada interfaz del router R1 (IN). Consideramos que para cortar la comunicación con una red es suficiente con cortar el flujo de datos en uno de los sentidos de la comunicación.
- La última entrada de la ACL es por defecto “deny all”, es decir, denegar el paso a todos los paquetes. No es necesario escribir dicha entrada.
- En el interfaz eth0 de R1, la ACL se aplica a los paquetes antes de que salgan del túnel IP.

Las restricciones que queremos imponer son las siguientes:

1. Los equipos de la red .64/26 sólo pueden comunicarse con los equipos de la sede central y esa comunicación debe establecerse por el túnel. No permitimos tráfico de entrada o salida de la red .64/26 si no va dirigido a equipos de la sede central (es decir, los equipos de dicha red no pueden tener comunicación con Internet).
2. La única comunicación permitida entre los equipos de la red .64/26 y los de la red .192/26 consiste en conexiones de clientes de la red .64/26 con el servidor web con dirección IP 2.2.2.200.
3. No hay ninguna restricción para la comunicación entre nodos de la red .64/26 y nodos de la red .128/26

Dar la configuración de las listas de acceso configuradas en los interfaces `eth0` y `eth1` del router R1. Indicar también en la columna "restricción" qué restricción de tráfico especificada en la anterior lista estamos imponiendo (es decir, escribir 1, 2 o 3 o poner un guión si no impone ninguna de las restricciones anteriores).

Nota:

- *Para simplificar la respuesta, escribir sólo el último octeto de la dirección IP expresado en base 10 para las direcciones del bloque 2.2.2.0/24, por ejemplo: escribir .64 en vez de 2.2.2.64.*
- *Expresar las máscaras (Mask) indicando el número de bits para los que queremos concordancia ("match"), por ejemplo /24 en vez de 255.255.255.0.*
- *protocolo: IP, TCP, UDP*
- *operador: <, >, ==, <> (el campo "operador puerto" puede ser también "any")*

R1, eth0, IN

Protocolo	@IP$_{source}$	Mask$_{source}$	Operador puerto$_{source}$	@IP$_{dest}$	Mask$_{dest}$	Operador puerto$_{dest}$	Permit/Deny	Restricción
IP	.1	/32	any	80.0.0.1	/32	any	Permit	1
(IP	any	any	any	any	any	any	Deny)	

R1, eth1, IN

Protocolo	@IP$_{source}$	Mask$_{source}$	Operador puerto$_{source}$	@IP$_{dest}$	Mask$_{dest}$	Operador puerto$_{dest}$	Permit/Deny	Restricción
TCP	.64	/26	> 1023	.200	/32	== 80	Permit	2
IP	.64	/26	any	.128	/26	any	Permit	3
(IP	any	any	any	any	any	any	Deny)	