Primer Control Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		3/04/2017	Primavera 2017
Nom:	**Cognoms:**	**Grup:**	**DNI:**

Durada: 1h15mn. El test es recollirà en 25 mn. Respondre en el mateix enunciat.

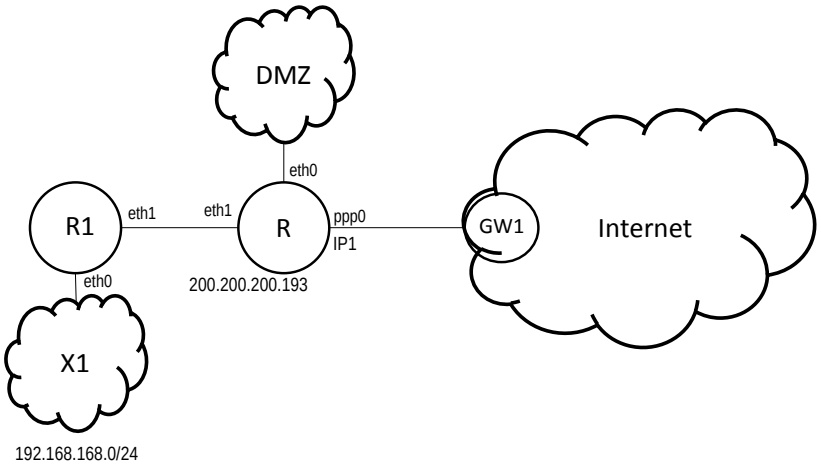
Test. (4 punts). Totes les preguntes poden ser multiresposta. Valen la meitat si hi ha un error, 0 si més. Marqueu la resposta correcta.

1. Respecto a los modelos TCP/IP y OSI de ISO:
   - ☐ Cuando una aplicación envía unos pocos bytes, el segmento TCP correspondiente es más grande que el datagrama IP.
   - ☑ Sobre un protocolo de red sin conexión, podemos usar protocolos de transporte con y sin conexión.
   - ☐ Los protocolos de DNS se sitúan en el nivel de red.
   - ☐ Un Router recibe segmentos TCP, los convierte a IP y los vuelve a re-enviar.
2. Respecto a direcciones IPv4:
   - ☐ 192.170.100.0/28 es una dirección privada.
   - ☑ 192.170.100.0/28 es una dirección de subred.
   - ☑ 192.170.100.14/28 puede ser un host.
   - ☑ 192.170.100.0/30 y 192.170.100.4/30 podrían ser subredes del rango 192.170.100.0/28.
3. Tenemos el rango de direcciones 10.0.3.0/27. Queremos direccionar en dicho rango 2 redes de 1 host, 1 de 5 hosts y otra de 7 hosts.
   - ☐ No tenemos suficientes direcciones para conseguirlo.
   - ☐ 10.0.3.8/29 y 10.0.3.8/30 pueden ser las dos subredes de 1 host.
   - ☑ 10.0.3.8/29 puede ser una de las subredes.
   - ☐ 10.0.3.0/26 podría ser la subred de 7 hosts.
4. Respecto a los protocolos de soporte a IP:
   - ☐ Los mensajes ARP van encapsulados en un paquete IP.
   - ☑ Los mensajes ICMP van encapsulados en un paquete IP.
   - ☑ El DNS sirve para obtener una dirección IP a partir de un nombre.
   - ☐ Los mensajes ARP viajan sobre UDP.
5. En la cabecera IPv4:
   - ☑ Las dos direcciones ocupan más de un tercio de la cabecera.
   - ☑ La longitud de la cabecera se mide en bloques de 32 bits.
   - ☐ El campo Protocol indica el protocolo sobre el que viaja el datagrama.
   - ☐ Para solicitar una Calidad de Servicio determinada disponemos de hasta dos bytes.
6. Sobre los Routers:
   - ☐ Cada vez que reciben un datagrama generan un mensaje informativo de control ICMP.
   - ☑ Un Router puede implementar varios protocolos de nivel de enlace.
   - ☐ Utilizan el protocolo DHCP para poder fragmentar el datagrama cuando va a ser entregado al host.
   - ☑ Utilizan la tabla de enrutamiento para saber a quién hay que entregar el datagrama.
7. Sobre la seguridad en IP:
   - ☑ Si añadimos un túnel de salida por un Router, debemos cambiar los valores de la tabla de enrutamiento.
   - ☑ Una ACL sirve para filtrar datagramas para evitar que salgan de, o entren a, un Router en función de información que no sólo se encuentra en la cabecera IP.
   - ☐ Si queremos evitar que un servidor Web que tenemos en nuestra subred sea atacado, es imprescindible que use DNAT y que esté en una subred separada del resto por otro Router.
   - ☐ Una forma de implementar un túnel es incluir el datagrama que queremos que atraviese el túnel en la cabecera de un datagrama de salida.
8. En relación a RIP:
   - ☐ Si tenemos una tabla de Routing con dos entradas con métricas de 100 y 200, los mensajes RIP Update que se envíen para esas dos entradas serán distintos.
   - ☐ Los mensajes RIP Update sólo se envían cuando hay cambios en las tablas de Routing.
   - ☐ El protocolo OSPF es igual al RIP cuando usa Split Horizon y Poisoned Reverse a la vez.
   - ☑ El Split Horizon permite evitar que un Router envíe a otro información que ya había obtenido de él.

Control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		03/04/2017	Primavera 2017
NOM (en MAJÚSCULES):	**COGNOMS (en MAJÚSCULES):**	**GRUP:**	**DNI:**

Duració: 1h 15 minuts. El test es recollirà en 25 minuts.

Problema (4 punts).
La figura mostra una part de la xarxa d'una empresa amb la seva configuració. S'utilitza el rang d'adreces privades 192.168.168.0/24 per a la xarxa X1 i el rang d'adreces públiques disponible és 200.200.200.192/28. L'adreça del router R assignada per l'ISP és IP1 i la del router de l'ISP és GW1.



a) (0'5 punts) Del rang d'adreces públiques disponible s'assigna l'adreça 200.200.200.193 a la interfície interna del router R amb R1. Determinar quina serà la subxarxa més gran que es pot assignar a la DMZ (adreces públiques) i quants servidors s'hi poden allotjar.

Enllaç R-R1: subxarxa 200.200.200.192/30.
Si R té l'adreça 200.200.200.193, R1 tindrà 200.200.200.194/30.
El rang 200.200.200.196/30 no es pot assignar. DMZ: 200.200.200.200/29
Host id: 3 bits. Màxim 5 servidors públics (2^3 menys xarxa, broadcast i router).

b) (0'5 punts) Completa les taules d'encaminament de R1 i R.

R1			
Network	Mask	Gateway	Iface
(X1) 192.168.168.0	/24		eth0
200.200.200.192	/30		eth1
0.0.0.0	/0	200.200.200.193	eth1

R			
Network	Mask	Gateway	Iface
(DMZ) 200.200.200.200	/29		eth0
200.200.200.192	/30		eth1
(X1) 192.168.168.0	/24	(R1.eth1) 200.200.200.194	eth1
GW1	/32		ppp0
0.0.0.0	/0	GW1	ppp0

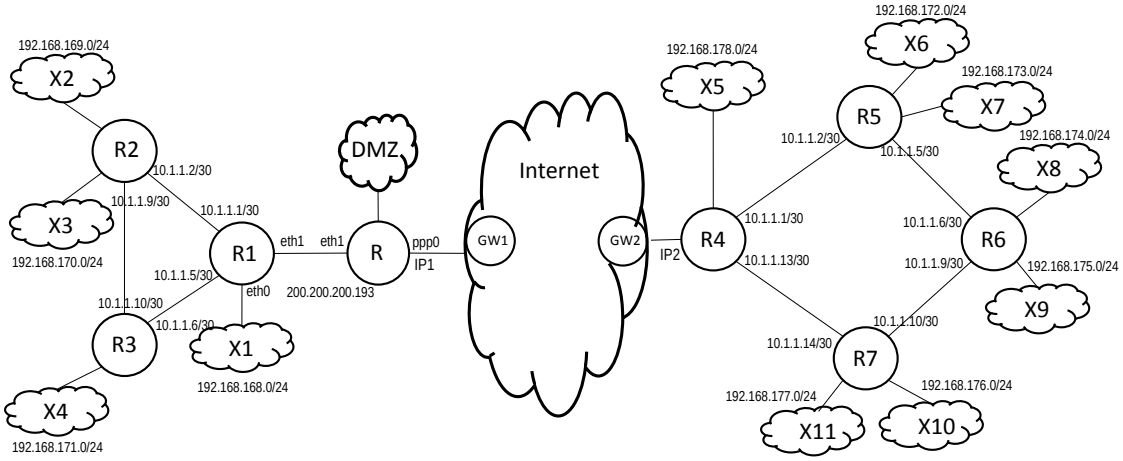
c) (0'75 punts) Un dispositiu connectat a X1 fa "ping 200.200.200.193". Completar la seqüència de trames Ethernet i datagrames que passen per X1 fins que arriba la primera resposta suposant que el dispositiu està ja configurat i que les taules ARP són buides. L'adreça IP del dispositiu és "A", l'adreça Mac és "a"; l'adreça IP de la interfície del router és "R1" i la seva MAC és "r1".

Ethernet header		ARP message		IP header			data
src	destination	type	contents	source	destination	protocol	message
a	FF:FF:FF:FF:FF:FF	RQ	R1 ?				
r1	a	RESP	R1 is r1				
a	r1			A	200.200.200.193	ICMP	Echo RQ
r1	a			200.200.200.193	A	ICMP	Echo RE

d) (0'5 punts) El router R1 fa NAT (PAT o PNAT) de manera que R no gestiona adreces privades. Completa la informació dels datagrames IP que passaran per l'enllaç entre R i R1 en el cas anterior (des de X1 es fa un "ping 200.200.200.193").

IP header			data
source	destination	protocol	message
(R1) 200.200.200.194	(R) 200.200.200.193	ICMP	Echo RQ
(R) 200.200.200.193	(R1) 200.200.200.194	ICMP	Echo RE

La figura mostra la xarxa completa de l'empresa amb dues seus amb adreçament privat connectades a través d'Internet.



Les subxarxes Xn tenen adreces privades del tipus 192.168.x.0/24. Els enllaços entre routers interns tenen adreces privades del tipus 10.1.1.x/30. Es defineix un túnel entre R1 i R4 per connectar les dues xarxes privades; el túnel es configura amb l'adreçament 192.168.0.0/30. Les subxarxes X5 ... X11 es connecten a Internet passant sempre pel túnel cap a R1.

e) (0'75 punts) Completar la taula d'encaminament de R1 incloent el túnel i amb el mínim nombre d'entrades (agregant les subxarxes quan sigui possible).

Network	Mask	Gateway	Iface
(R1-R2) 10.1.1.0	/30		eth2
(R1-R3) 10.1.1.4	/30		eth3
(R1-R) 200.200.200.192	/30		eth1
(X1) 192.168.168.0	/24		eth0
(túnel) 192.168.0.0	/30		tun0
(X2) 192.168.169.0	/24	10.1.1.2	eth2
(X3) 192.168.170.0	/24	10.1.1.2	eth2
(X4) 192.168.171.0	/24	10.1.1.6	eth3
192.168.172.0	/22	192.168.0.2	tun0
192.168.176.0	/22	192.168.0.2	tun0
0.0.0.0	/0	200.200.200.193	eth1

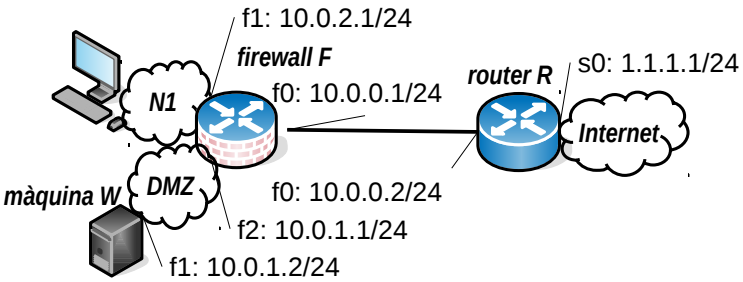
X2 no es por agregar amb X3
X3 no es pot agregar amb X4
X4 no es pot agregar
Agregació X6, X7, X8, X9
Agregació X10, X11, X5

f) (0'5 punts) Des d'un dispositiu de la xarxa X11 s'executa la comanda "traceroute 200.200.200.202". Aquesta adreça correspon a un servidor públic situat a la DMZ. Determinar la seqüència d'adreces IP que ens retornarà l'execució del "traceroute".
192.168.177.1 (R7) – 10.1.1.13 (R4) – 200.200.200.192 (R1) – 200.200.200.193 (R) – 200.200.200.202

g) (0'5 punts) Si la MTU de totes les xarxes és 1500 octets, hi haurà fragmentació en algun cas? Si és així, quina és la mida dels fragments resultants?
Si la MTU és 1500 la mida màxima dels datagrames és de 1500 octets (20 capçalera + 1480 dades). Quan passen pel túnel seran de 1520 i caldrà fragmentar. Com 1480 és múltiple de 8 octets hi haurà un fragment de 1500 (20+1480) i un segon de 40 octets (20+20).

Control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		3/4/2017	Primavera 2017
NOM:	**COGNOMS:**	**DNI**	

Duració: 1h15m. El test es recollirà en 25 min. Respondre en el mateix enunciat.



La figura mostra el nom de les interfícies i la adreça IP que tenen assignada.

Problema 2 (2 punts)

La xarxa de la figura té una única adreça pública que fa servir el **router R** per fer PAT/DNAT. No hi ha més xarxes que les indicades. Suposa que R ja està correctament configurat, d'acord amb les adreces que mostra la figura. També hi ha el **firewall F** que es desitja configurar per aconseguir els següents **objectius** entre N1/DMZ i Internet:

1. Es pot connectar des de la **xarxa N1** cap a qualsevol servidor estàndard (***well known port***) d'Internet.
2. Es poden rebre/enviar missatges **ICMP** des de N1/DMZ i Internet.
3. Es pot connectar des de **DMZ** als servidors de noms (port **53**), que hi ha en Internet.
4. Des d'Internet es pot accedir al servidor web (port **80**) que hi ha en la **màquina W**.

Es desitja configurar el **firewall F** per assolir els objectius anteriors seguint les següents **condicions** (per ordre de preferència):

1. No es permeten connexions entre N1/DMZ i Internet que no correspongui als objectius anteriors.
2. Nombre mínim de regles.
3. Regles el més restrictives possible.

Es demana omplir la taula següent tenint en compte que les columnes protocol/IP/port són els camps de les capçaleres IP i transport (quan són aplicables). La regla s'aplica als **paquets que entren (in)** per la **interfície f0** del **firewall F**. No es poden fer servir més regles que les files indicades per a cada objectiu, tot i que és possible fer-ne servir menys. En qualsevol casella «**any**» vol dir qualsevol valor i «-» vol dir que no és aplicable. La llista acaba amb la regla «descarta tot». Posar les adreces IP amb notació en punts/màscara. Per els ports es poden fer servir els operadors <, >, =.

Objectiu	**protocol**	**@IP-origen/masc.**	**port-origen**	**@IP-dest./masc.**	**port-dest**	**Acceptar: A, Denegar: D**
1	TCP	any	<=1023	10.0.2.0/24	>1023	A
1	UDP	any	<=1023	10.0.2.0/24	>1023	A
2	ICMP	any	-	any	-	A
2						
3	UDP	any	=53	10.0.1.0/24	>1023	A
3						
4	TCP	any	>1023	10.0.1.2/32	=80	A
4						
	any	any	-	any	-	D