Control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		8/4/2024	Primavera 2024
NOM:	**COGNOMS:**	**GRUP:**	**ID:**

Durada: 1h30m. El test es recollirà en 25 minuts. Si us plau, respondre en aquesta pàgina.

Test. (3,5 punts) Les preguntes puntuen la meitat si hi ha un error i 0 si n'hi ha més d'un error.

1. Sobre xarxes IP:
- ☒ La xarxa 10.0.0.0/8 és de classe A.
- ☐ La xarxa 100.0.0.0/16 és de classe B.
- ☒ La xarxa 192.168.255.0/24 és privada.
- ☐ La xarxa 200.0.0.0/24 és privada.

2. Quines de les adreces següents poden ser l'adreça d'una subxarxa?
- ☐ 200.2.65.0/20
- ☒ 200.2.65.0/24
- ☒ 200.2.65.32/27
- ☒ 200.2.65.64/27

3. Sobre el protocol IP:
- ☒ El missatge ICMP va al camp de dades d'un paquet IP per internet.
- ☒ La capçalera d'un paquet IP té un camp de detecció d'errors que es produeixen a la capçalera IP.
- ☐ La capçalera d'un paquet IP té un camp de detecció d'errors que es produeixen a tot el paquet IP.
- ☒ La fragmentació d'un paquet IP no es produeix si el flag DF ("DO NOT FRAGMENT") és actiu a la capçalera del paquet IP.

4. Sobre el protocol IP:
- ☒ Un dispositiu amb dues interfícies connectades a diferents xarxes pot rebre a una i reenviar paquets cap a l'altre si s'activa "IP forwarding".
- ☐ La capçalera dels paquets IP es modifica a cada router posant-hi l'adreça IP del següent router (gateway).
- ☐ Els paquets IP intercanviats entre dues adreces IP segueixen sempre el mateix camí per arribar a la destinació.
- ☒ El protocol IP permet transportar paquets entre dos dispositius terminals (hosts) però es poden perdre paquets o arribar desordenats.

5. Sobre el protocol ARP:
- ☐ Un paquet ARP amb TTL=2 permet descobrir interfícies IP a dos salts.
- ☐ Els clients envien missatges (unicast) a l'adreça IP de la que volem descobrir la seva adreça MAC d'Ethernet.
- ☒ Més d'un dispositiu pot respondre a un missatge ARP REQ, però indica IP duplicada.
- ☒ Un dispositiu connectat a una xarxa Ethernet ha de respondre a les peticions ARP referides a l'adreça IP de la interficie connectada a la xarxa.

6. Sobre el protocol DHCP:
- ☒ El client envia missatges DHCPDISCOVER i DHCPREQUEST a l'adreça IP 255.255.255.255.
- ☐ Serveix exclusivament per configurar l'adreça IP i la màscara de xarxa.
- ☒ Com a mínim un servidor DHCP ha d'estar accessible a cada xarxa.
- ☒ Per mantenir una adreça IP assignada de forma dinàmica, aquesta s'ha de renovar abans d'haver expirat.

7. Sobre el protocol ICMP:
- ☐ ARP fa servir paquets ICMP de broadcast.
- ☐ Si a una taula d'encaminament no hi ha informació per arribar a la destinació es genera un missatge d'error Destination host unreachable.
- ☒ Permet generar missatges d'error.
- ☐ Els paquets ICMP no passen per un router amb PNAT (PAT).

8. Sobre el protocol RIP versió 2:
- ☒ Cada router envia les actualitzacions de rutes a les xarxes connectades directament al router per les interfícies on s'ha activat RIP.
- ☐ Distribueix les actualitzacions (updates) a tots els routers de les xarxes, directament connectades o no.
- ☒ El mètode "split horizon" serveix per reduir l'efecte de "count to infinity".
- ☐ Els missatges RIP d'un router arriben a tots els routers de la xarxa.

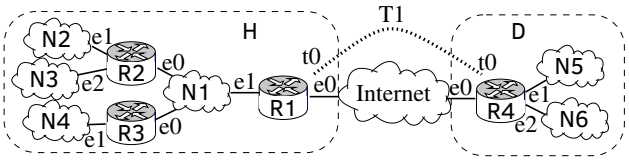
9. A una taula de rutes (com mostra la comanda: route -n):
- ☐ Els valors de la columna "Gateway" poden estar buits o tenir l'adreça IP de la interfície local per on s'ha d'enviar el paquet IP.
- ☒ Els valors de la columna "Gateway" poden estar buits o tenir l'adreça IP del proper router per on s'ha de reenviar el paquet IP (1er salt).
- ☐ Aplica la primera fila de la taula que encaixa.
- ☒ Aplica la fila de la xarxa que encaixa amb el major nombre de bits de xarxa (Longest Prefix Match, LPM).

10. Sobre traducció d'adreces NAT amb ports (Port Address Translation, PAT o PNAT). DNAT significa Destination NAT:
- ☒ PAT canvia l'adreça IP i port d'origen als paquets que surten d'una xarxa privada a la pública, mantenint l'adreça IP i port de destinació.
- ☐ PAT canvia l'adreça IP i port d'origen als paquets que entren de la xarxa pública a una privada, mantenint l'adreça IP i port de destinació.
- ☒ DNAT permet a un router redirigir connexions de xarxa entrants (iniciades per un client a la xarxa pública), traduint l'adreça IP de destinació dels paquets, per permetre l'accés a servidors dins d'una xarxa privada des de l'exterior.
- ☐ DNAT serveix per traduir les adreces IP i ports dels intercanvis de paquets que inicien clients d'una xarxa privada cap a servidors de Internet.

Control de Xarxes de Computadors (XC)	Grau en Ingeniería Informàtica	08/04/2024	Primavera 2024
Nom	Cognoms	Grup	DNI

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

Problema 1.
4.5 punts.



N1: 200.0.0.0/29
N2: 200.0.0.144/28
N3: 200.0.0.176/28
N4: 200.0.0.192/26
T1: 192.168.0.0/24

N5: 172.16.0.0/24
N6: 172.16.1.0/24
R1-e0: 80.0.0.2
R4-e0: 90.0.0.2

En la xarxa de la figura hi ha una seu H i una delegació D connectades per un túnel IPIP (T1). Totes les subxarxes d'H pertanyen al rang 200.0.0.0/24. La xarxa està configurada de forma que totes les connexions surten a Internet pel router R1 d'H. Per exemple, una connexió d'un host d'N5 anirà per T1 per poder sortir a Internet. Tots els routers d'H i D fan servir el protocol RIP versió 2 amb sumarització de rutes a la classe i split-horizon. Notar que en les preguntes 3 i 4 *hosts* no inclou els *routers*.

1. (1 punt) Completa la taula d'encaminament d'R1 i R4 un cop RIP ha convergit. Fes servir les files que necessitis. En la columna de mètriques (M) posa la mètrica RIP. Per a la columna del gateway, suposa que als routers s'ha assignat la IP numèricament més petita. Quan en una xarxa hi ha més d'un router, les IPs s'han assignat començant per el router amb el nom lexicogràficament més petit. Per exemple, la IP d'R1 en N1 és la IP numèricament més petita que es pot assignar en N1.

R1

Destinació/màsc	Gateway	If	M
80.0.0.1/32	-	e0	1
0.0.0.0/0	80.0.0.1	e0	1
N1	-	e1	1
N2	200.0.0.2	e1	2
N3	200.0.0.2	e1	2
N4	200.0.0.3	e1	2
T1	-	t0	1
172.16.0.0/16	192.168.0.2	t0	2

R4

Destinació/màsc	Gateway	If	M
90.0.0.1/32	-	e0	1
80.0.0.2/32	90.0.0.1	e0	1
N5	-	e1	1
N6	-	e2	1
T1	-	t0	1
200.0.0.0/24	192.168.0.1	t0	2
0.0.0.0/0	192.168.0.1	t0	2

2. (0.5 punts) Digues quin serà el contingut dels missatges d'update que enviarà R1 per les interfícies indicades un cop RIP ha convergit. Fes servir la notació (destinació/màscara, mètrica).

e1	(0.0.0.0/0,1) (T1,1) (172.16.0.0/16, 2)

t0	(0.0.0.0/0,1) (200.0.0.0/24,1)

3. (1 punt) Es vol ampliar H afegint una altra subxarxa que tingui el màxim nombre de hosts (agafant IPs de 200.0.0.0/24 i sense canviar les subxarxes que ja hi ha). Dóna la següent informació de la nova subxarxa. Justifica la resposta.

adreça de xarxa/màscara	adreça broadcast	max hosts
200.0.0.64/26	200.0.0.127	$2^6 - 3 = 61$

En la taula hi ha el subnetid de les subxarxes, d'on deduïm que la xarxa més gran que es pot afegir tindrà el subnetid `01xx.xxxx`, i $2^6 = 64$. Per el broadcast hem de sumar a l'últim byte $2^6 - 1 = 63$.

xarxa	subnetid
N1	0000.0xxx
N2	1001.xxxx
N3	1011.xxxx
N4	11xx.xxxx

4. (0.5 punts) Es vol dividir N4 en subxarxes més petites i que hi pugui haver al menys 4 hosts i 1 router en cada subxarxa. Digues el nombre màxim de subxarxes en que es podria dividir (n), i dona la següent informació per a la subxarxa amb valor numèricament més gran.

subxarxa numèricament més gran

n	adreça de xarxa/màscara	max hosts
8	200.0.0.248/29	$2^3 - 3 = 5$

Necessitem 3 bits de hostid, per tant, ens queden 3 bits per el subnetid, és a dir n=2^3 subxarxes. La subxarxa numèricament més gran tindrà l'últim byte=`1111.1000`$= 255 - 7 = 248$.

5. (0.75 punts) Els hosts A i B tenen la IP més gran que es pot assignar en N6 i N3, respectivament. A fa ping a B. Digues si farà falta NAT i quines seran les IPs i protocol de la capçalera IP de l'echo request quan arriba a R1 per e0 i quan surt de R1 per e1.

e0 in

capçalera externa			capçalera interna		
adreça font	**adreça destinació**	**protocol**	**adreça font**	**adreça destinació**	**protocol**
90.0.0.2	80.0.0.2	IPIP	172.16.1.254	200.0.0.190	ICMP

e1 out

adreça font	adreça destinació	protocol
172.16.1.254	200.0.0.190	ICMP

No cal NAT. El hostid de N3 té 4 bits $2^4 - 1 = 15$. Per tant, la IP de broadcast en N3 és `200.0.0.191`, i la IP de B `200.0.0.190`.

6. (0.75 punts) Ara el host A fa ping a la IP 8.8.8.8. Digues si farà falta NAT i quines seran les IPs i protocol de la capçalera IP de l'echo request quan arriba a R1 per e0 i quan surt de R1 per e0.

e0 in

capçalera externa			capçalera interna		
adreça font	**adreça destinació**	**protocol**	**adreça font**	**adreça destinació**	**protocol**
90.0.0.2	80.0.0.2	IPIP	172.16.1.254	8.8.8.8	ICMP

e0 out

adreça font	adreça destinació	protocol
80.0.0.2	8.8.8.8	ICMP

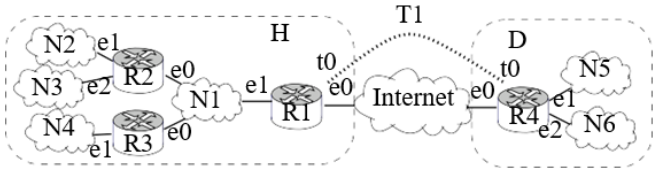
Cal NAT en R1 perquè les IPs de N5 són privades

Control de Xarxes de Computadors (XC). Grau en Enginyeria Informàtica		08/04/2024	Primavera 2024
NOM (MAJÚSCULES):	COGNOMS (MAJÚSCULES):	GRUP:	DNI/NIE:

Contestar en el mateix full.

Problema 2 (2 punts)

La figura mostra la configuració de la xarxa i l'assignació de l'adreçament. La xarxa H té adreces públiques del prefix H i la xarxa D adreces privades del prefix D. Totes les connexions a Internet passen per R1; és a dir, les xarxes N5 i N6 es comuniquen amb H i amb Internet a través del túnel T1.



Es defineixen llistes de control d'accés (ACL) en algunes interfícies dels encaminadors (*routers*).
Les interfícies on no hi ha definit cap ACL deixen passar tot el tràfic.

rule	Interface	IN/OUT	Source IP	Source port	Destination IP	Dest. port	Protocol	Action
1	R3e0	IN	ANY	>=1024	N4	<1024	TCP	Accept
1	R3e0	OUT	N4	<1024	ANY	>=1024	TCP	Accept
2	R3e0	IN	ANY	53 (dns)	200.0.0.196/32	>=1024	TCP/UDP	Accept
2	R3e0	OUT	200.0.0.196/32	>=1024	ANY	53 (dns)	TCP/UDP	Accept
3	R3e0	IN/OUT	ANY		ANY		ICMP	Accept
7	R3e0	IN/OUT	ANY	ANY	ANY	ANY	ANY	Deny
4	R1e1	IN	200.0.0.5/32	22(ssh)	ANY	>=1024	TCP	Accept
4	R1e1	OUT	ANY	>=1024	200.0.0.5/32	22 (ssh)	TCP	Accept
5	R1e1	IN	ANY	22 (ssh)	ANY	>=1024	TCP	Deny
5	R1e1	OUT	ANY	>=1024	ANY	22 (ssh)	TCP	Deny
6	R1e1	IN/OUT	ANY	ANY	ANY	ANY	TCP/UDP/ICMP	Accept
8	R1e1	IN/OUT	ANY	ANY	ANY	ANY	ANY	Deny

a) (1 punt) Contestar les següents preguntes i posar CERT o FALS on correspongui.

Qualsevol client TCP de H, D i Internet pot accedir als servidors de N4.	CERT (1)(6)
Dispositius clients TCP de N4 es poden comunicar amb tots els servidors d'Internet.	FALS (7)
Clients TCP de N4 es poden comunicar amb servidors a D.	FALS (7)
El dispositiu 200.0.0.196 és l'únic cient de la xarxa N4 amb accés a Internet.	CERT (2)(6)
Es pot establir una connexió SSH (TCP:22) amb el servidor 200.0.0.5 des de dispositius a N6.	CERT (4)
Les regles 4, 5 i 6 serveixen per bloquejar les connexions SSH entre N2 i N4.	FALS
Amb les regles 4 i 5 a N1 només hi pot haver un únic servidor SSH.	CERT (4)(5)
Amb la regla 6 es deixa passar tot el tràfic TCP, UDP i ICMP, però no altres protocols.	CERT (6)(8)
Es pot establir un túnel IPinIP entre R2 i un altre *router* extern a Internet.	FALS (8 IPinIP)
Es pot establir una VPN des d'un dispositiu a N3 amb un servidor de VPN extern a Internet.	CERT (6 TCP)

b) (1 punt) Configurar les regles de filtratge (ACL) a les interfícies corresponents per tal que: a) els dispositius a N5 siguin només clients TCP de servidors a Internet i a H, i a la vegada siguin servidors TCP només de clients a N6; b) els dispositius a N5 només contestin "*ping*" dels dispositius a N6.

rule	Interface	IN/OUT	Source IP	Source port	Destination IP	Dest. port	Protocol	Action
a	R4e1	IN	N5 (ANY)	>=1024	N6	<1024	TCP	Deny
a	R4e1	OUT	N6	<1024	N5 (ANY)	>=1024	TCP	Deny
a	R4e1	IN	N5 (ANY)	>=1024	ANY	<1024	TCP	Accept
a	R4e1	OUT	ANY	<1024	N5 (ANY)	>=1024	TCP	Accept
a	R4e1	IN	N5 (ANY)	<1024	N6	>=1024	TCP	Accept
a	R4e1	OUT	N6	>=1024	N5 (ANY)	<1024	TCP	Accept
b	R4e1	IN	N5 (ANY)		N6		ICMP	Accept
b	R4e1	OUT	N6		N5 (ANY)		ICMP	Accept
	R4e1	ANY	ANY	ANY	ANY	ANY	ANY	Deny