

Primer control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		29/10/18	Tardor 2018
NOM (en MAJÚSCULES):	COGNOMS (en MAJÚSCULES):	GRUP:	DNI:

Duració: 1h 30 minuts. El test es recollirà en 25 minuts.

Test. 4 punts. Las preguntas pueden ser

- Respuesta única (RU). Una respuesta RU correcta cuenta 0.4 puntos.
- Multirespuesta (MR). Una respuesta MR correcta cuenta 0.4 puntos, la mitad si hay un solo error, 0 en los otros casos. En las MR puede haber desde una hasta todas respuestas correctas.

1. **RU.** En el modelo TCP/IP, el orden de capas a partir de abajo es

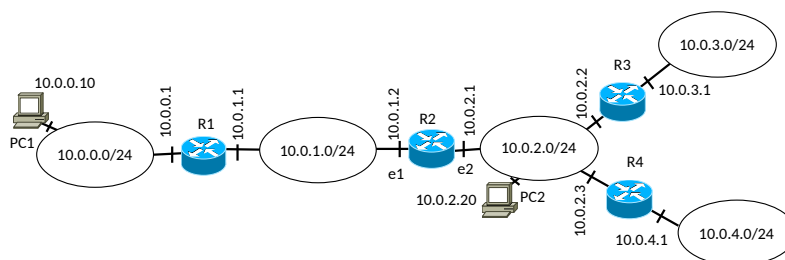
- ☐ Físico, Enlace, Red, Transporte, Sesión, Presentación, Aplicación
- ☐ Tarjeta de red, Red, Internet, Aplicación
- ☐ Interfaz de red, Enlace, Red, Transporte, Aplicación
- ☐ Físico, Red, Transporte, Aplicación
- ☒ Interfaz con la red física, Red, Transporte, Aplicación de red

2. **MR.** A partir del rango 128.0.0.128/25 se pueden crear

- ☒ 4 redes con 25 hosts cada una
- ☒ 6 redes, 2 con 20 hosts, 3 con 10 hosts y 1 con 5 hosts
- ☐ 8 redes con 16 hosts cada una
- ☐ 2 redes, una de 64 hosts y otra de 40 hosts
- ☒ 16 redes de 4 hosts cada una

3. **RU.** Considerando la red de la figura y suponiendo que todas las tablas ARP están vacías y que todo está bien configurado, determinar en número de mensajes **ARP request** que se envían en total si se quiere enviar un datagrama de PC1 a PC2 y una respuesta de PC2 a PC1.

- ☐ 1
- ☐ 2
- ☒ 3
- ☐ 4
- ☐ 5
- ☐ 6
- ☐ 7



4. **RU.** Suponer que se activa RIPv2 en la red de la figura de la pregunta 3. Determinar el mensaje RIPv2 que R1 envía a R2 cada 30 segundos

- ☐ 10.0.0.0/24 métrica 1, 10.0.1.0/24 métrica 1, 10.0.2.0/24 métrica 2, 10.0.3.0/24 métrica 3, 10.0.4.0/24 métrica 3
- ☐ 10.0.2.0/24 métrica 2, 10.0.3.0/24 métrica 3, 10.0.4.0/24 métrica 3
- ☒ 10.0.0.0/24 métrica 1
- ☐ 10.0.0.0/24 métrica 1, 10.0.1.0/24 métrica 1

5. **RU.** Si la interfaz e1 del router R2 de la pregunta 3 cae, determinar el mensaje RIP que R2 envía por la red 10.0.2.0/24

- ☐ a R3: 10.0.1.0/24 métrica 16, 10.0.1.0/24 métrica 16 y 10.0.4.0/24 métrica 2
- ☐ a R4: 10.0.1.0/24 métrica 16, 10.0.1.0/24 métrica 16 y 10.0.3.0/24 métrica 2
- ☐ 10.0.1.0/24 métrica 16 y 10.0.0.0/24 métrica 2
- ☐ 10.0.1.0/24 métrica 16
- ☒ 10.0.0.0/24 métrica 16 y 10.0.1.0/24 métrica 16

6. **MR.** Marca la o las afirmaciones correctas.

- ☐ Un ARP gratuito se usa para verificar que hay conectividad entre dos hosts
- ☒ Si un router descarta un datagrama y envía un mensaje ICMP, el ICMP lo envía a la @IP origen del datagrama
- ☐ El campo TTL en la cabecera IP se usa para fragmentar datagramas demasiado largos para ser encapsulados en tramas
- ☒ Si no se usa NAT, dos hosts conectados a Internet no pueden tener la misma @IP pública

7. **RU.** La dirección IP 225.5.5.5 es

- ☐ De clase A
- ☐ De clase B
- ☐ De clase C
- ☐ Privada
- ☒ De clase D
- ☐ De clase E

8. **MR.** Si a un router con la tabla de encaminamiento de la derecha le llega un datagrama con destino:

- ☒ 10.0.0.200, el datagrama se envía por la interfaz e0
- ☒ 200.0.2.10, el datagrama se envía por la interfaz e2
- ☒ 10.10.3.1, el datagrama se envía por la interfaz e0
- ☒ 10.0.3.10, el datagrama se envía por la interfaz e1
- ☐ 10.0.1.130, el datagrama se envía por la interfaz e1

Red	Mascara	Gateway	Interfaz
10.0.0.0	24	-	e0
10.0.1.0	25	-	e1
10.0.2.0	24	-	e2
10.0.0.0	8	10.0.0.1	e0
0.0.0.0	0	10.0.2.1	e2
10.0.3.10	32	10.0.1.1	e1

9. **RU.** El NAT por puertos (PAT o NAT overload) se usa

- ☐ Para traducir un puerto privado a uno público
- ☐ Para permitir que un cliente público pueda acceder a un servidor privado
- ☒ Para permitir que un grupo de clientes privados pueda comunicarse con un servidor público
- ☐ Para que un grupo de host privados pueda tener cada uno su propia IP pública única y diferente en Internet

10. **RU.** Cuál de estos protocolos puede asignar una ruta por defecto a un host

- ☐ DNS
- ☐ TCP
- ☒ DHCP
- ☐ RIP
- ☐ NAT
- ☐ ACL

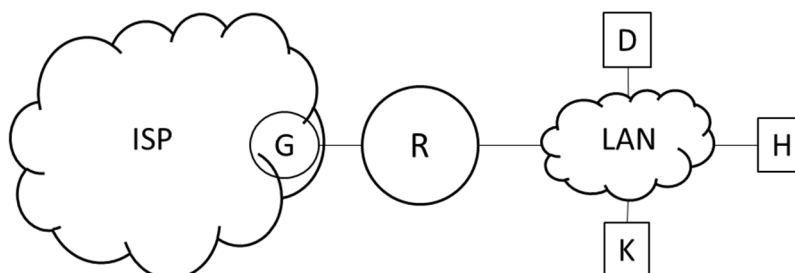
Primer control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		29/10/2018	Tardor 2018
NOM (en MAJÚSCULES):	COGNOMS (en MAJÚSCULES):	GRUP:	DNI:

Duració: 1 hora i 30 minuts. El test es recollirà en 25 minuts.

Problema 1 (4 punts)

La xarxa local de la figura té adreçament públic amb capacitat per allotjar 220 dispositius. D és el servidor local de DNS, el router R fa de servidor de DHCP, H i K són dos dels dispositius de la xarxa. El domini de la xarxa és *domini.tld* (per exemple, el dispositiu H té el nom *h.domini.tld*) Tots els dispositius estan correctament configurats i en marxa, a excepció de H que està apagat inicialment.

La notació que utilitzem és lletra majúscula per a l'adreça IP i minúscula per a l'adreça MAC (Ethernet).



a) (0'75 punts) Completar la seqüència de trames Ethernet i paquets IP que es transmetran per la xarxa local al posar en marxa H per obtenir la seva configuració.

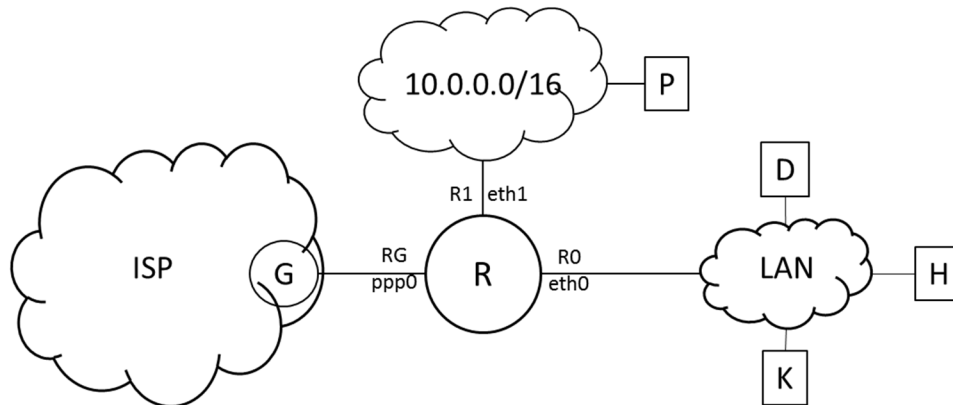
Ethernet		IP		
src	dst	src	dst	payload
h	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	DHCP Discover
r	FF:FF:FF:FF:FF:FF	R	255.255.255.255	DHCP Offer
h	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	DHCP Request
r	h	R	H	DHCP ACK

Un cop completada la configuració, el dispositiu H coneix la seva adreça IP (H), la del servidor de DNS (D) i la del router per defecte (R).

b) (1'25 punts) Completar la seqüència de trames i paquets quan des de H s'executa la comanda "ping k.domini.tld"

Ethernet		ARP		IP		
src	dst	Q/R	message	src	dst	Payload
h	bcast	Q	ARP D?			
d	h	R	ARP D is d			
h	d			H	D	DNS Q k.domini.tld
d	h			D	H	DNS R k.domini.tld = K
h	bcast	Q	ARP K?			
k	h	R	ARP K is k			
h	k			H	K	ICMP echo request
k	h			K	H	ICMP echo response

A la configuració inicial s'afegeix una xarxa privada tal com es mostra a la figura. La figura indica les interfícies del router R i les seves adreces IP.



La taula d'encaminament del router R és la següent:

Destination	Gateway	interface
LAN	----	eth0
10.0.0.0/16	----	eth1
G/32 (ISP)	----	ppp0
0.0.0.0/0	G	ppp0

c) (1 punt) Des del dispositiu P (xarxa privada) s'executa la comanda "ping www.upc.edu" (l'adreça IP del servidor web és U). Completar la seqüència de datagrames que passen per R indicant les interfícies d'entrada i sortida corresponents. Cal tenir en compte que el router fa NAT.

Interface	In/Out	Src IP address	Dst IP address	payload
eth1	in	P	D	DNS request
eth0	out	R0	D	DNS request
eth0	in	D	R0	DNS response U
eth1	out	D	P	DNS response U
eth1	in	P	U	ICMP echo request
ppp0	out	RG	U	ICMP echo request
ppp0	in	U	RG	ICMP echo reply
eth1	out	U	P	ICMP echo reply

d) (1 punt) Per tal de poder accedir des de casa es configura un túnel des del router de casa (HR) fins al router R (interfície RG). La xarxa privada definida a casa és 10.10.10.0/24.

Completar les entrades que s'afegeixen a la taula d'encaminament del router R:

Destination	Gateway	interface
192.168.0.0/30		tun0
10.10.10.0/24	192.168.0.2	tun0

Quan el dispositiu H executa la comanda "ping 10.10.10.10" completar la seqüència de datagrames que passen pel router R.

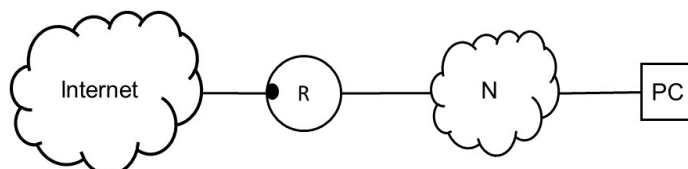
Interface	In/Out	Src IP address	Dst IP address	payload
eth0	in	H	10.10.10.10	ICMP echo request
ppp0	out	RG	HR	Datagrama H, 10.10.10.10

Primer control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		29/10/18	Tardor 2018
NOM (en MAJÚSCULES):	COGNOMS (en MAJÚSCULES):	GRUP:	DNI:

Duració: 1h 30 minuts. El test es recollirà en 25 minuts.

Problema 2 (2 punts)

El Router R de la figura dispone de un Firewall en su interfaz en el lado de Internet. Suponer el subconjunto de Access Control List (ACL) de la tabla siguiente. Tener en cuenta que el port 53 corresponde al servicio DNS y el port 80 al HTTP (web).



	IN/OUT	IP src	port src	IP dst	port dst	Protocol	Action
1	IN	ANY		N		ICMP	ACCEPT
2	IN	D1	53	N	>1023	UDP/TCP	ACCEPT
3	OUT	N	>1023	D1	53	UDP/TCP	ACCEPT
4	IN	ANY	>1023	N	80	TCP	ACCEPT
5	OUT	N	80	ANY	>1023	TCP	ACCEPT
6	ANY	ANY	ANY	ANY	ANY	ANY	DENY

a) (0,5 punts) Indicar (en la tabla proporcionada) la secuencia de paquetes que entran y salen a través del Firewall cuando un cliente HTTP externo a N se conecta a un servidor HTTP en N (pide una página web que le es retornada). Las flechas indican el sentido de la transmisión: ← hacia Internet, → hacia la red interna N.

← / →	Aplicación	Núm. regla ACL que se usa	Acción
→	HTTP	4	Aceptar
←	HTTP	5	Aceptar

b) (0,5 punts) Indicar (igual que en la pregunta a) la secuencia de paquetes que entran y salen a través del Firewall cuando se hace una consulta (de la que hay respuesta) desde PC hacia un servidor DNS D2 externo a N.

← / →	Aplicación	Núm. regla ACL que se usa	Acción
←	DNS	6	Denegar

c) (0,5 punts) Si queremos que se intercambien mensajes de ICMP entre PC y alguna máquina en Internet, ¿hay que añadir alguna regla a la ACL? **SI** **NO**

Si fuese así, indicar cuál o cuáles. En caso contrario, indicar qué reglas ya lo permiten.

Reglas	IN/OUT	IP src	port src	IP dst	port dst	Protocol	Action
-	OUT	N		ANY		ICMP	ACCEPT

d) (0,5 punts) Si queremos que PC acceda a un servidor HTTP externo a N, ¿hay que añadir alguna regla a la ACL? **SI** **NO**

Si fuese así, indicar cuál o cuáles. En caso contrario, indicar qué reglas ya lo permiten.

Reglas	IN/OUT	IP src	port src	IP dst	port dst	Protocol	Action
-	IN	ANY	80	N	>1023	TCP	ACCEPT
	OUT	N	>1023	ANY	80	TCP	ACCEPT