Primer Control Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		16/04/2018	Primavera 2018
Nom:	**Cognoms:**	**Grup:**	**DNI:**

Durada: 1h30mn. El test es recollirà en 25 mn. Respondre en el mateix enunciat.

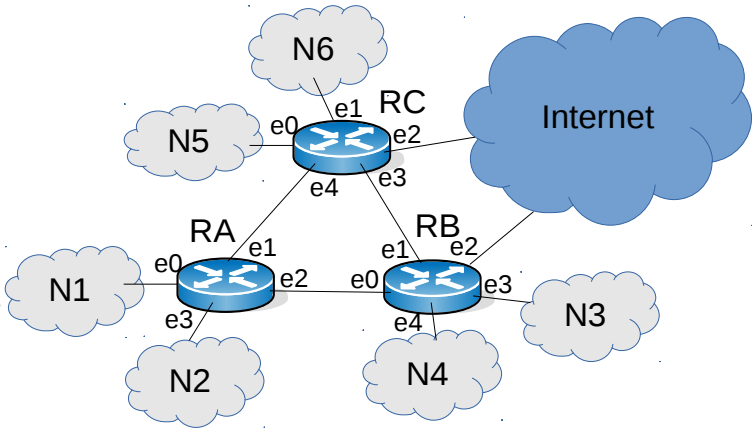
1. Respecto a los modelos TCP/IP:
   - ☐ Un datagrama IP transporta información de TCP, pero no de aplicación.
   - ☐ Sobre un protocolo de red sin conexión, sólo podemos usar protocolos de transporte sin conexión.
   - ☑ Los protocolos de DNS se sitúan en el nivel de aplicación.
   - ☑ Una entidad de nivel N debe procesar las cabeceras de nivel N.
2. Dada la subred 10.10.10.0/28:
   - ☑ Sus direcciones son privadas.
   - ☐ 10.10.10.1/28 puede ser una subred suya.
   - ☑ 10.10.10.2 puede ser la dirección de un Router de dicha subred.
   - ☐ 10.10.10.3 y 10.10.10.100 pueden ser direcciones de hosts de dicha subred.
3. Tenemos el rango de direcciones 100.0.0.0/29. Queremos direccionar en dicho rango 2 subredes de 1 host.
   - ☐ No tenemos suficientes direcciones para conseguirlo.
   - ☐ 100.0.0.0/29 y 100.0.0.4/30 pueden ser las dos subredes.
   - ☑ 100.0.0.6 puede ser un host en una de las subredes.
   - ☑ 100.0.0.3 puede ser la dirección de broadcast en una de las subredes.
4. Respecto a los protocolos de soporte a IP:
   - ☑ Los mensajes ARP son enviados para obtener la dirección física que corresponde a una dirección IP.
   - ☑ Un Router no genera mensajes ICMP como respuesta a errores de datagramas que contienen otros mensajes de error ICMP.
   - ☐ El DNS sirve para obtener la dirección del servidor de nombres local.
   - ☑ Los mensajes DNS viajan sobre UDP.
5. En la cabecera IPv4:
   - ☐ Sólo incluimos el campo Offset cuando hay fragmentación.
   - ☐ Hay un campo para indicar la longitud de la cabecera, pero no para indicar la longitud del datagrama completo.
   - ☑ El campo Protocol indica el protocolo que viaja en el payload (datos de usuario) del datagrama.
   - ☑ Si no se usan opciones, no enviamos ningún campo de opciones.
6. Sobre los Routers:
   - ☐ Analizan el payload de los datagramas para optimizar su ruta en función del protocolo de aplicación en el datagrama.
   - ☑ Un Router suele incluir un servidor DHCP y puede proporcionar servicio NAT.
   - ☐ Se comunican con otros Routers para proporcionar el servicio NAT conjuntamente.
   - ☑ No envían un datagrama a nadie hasta que no han consultado la tabla de enrutamiento para saber a quién hay que entregarlo.
7. Sobre la seguridad en IP:
   - ☐ Añadir un túnel de salida por un Router no afecta a 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 sólo se encuentra en la cabecera IP.
   - ☐ Si queremos permitir que un servidor Web que tenemos en nuestra subred sea accedido desde el exterior, es imprescindible que lo pongamos en una subred independiente de otros hosts que no queremos que sean accedidos.
   - ☑ Una forma de implementar un túnel es incluir el datagrama que queremos que atraviese el túnel como payload de otro datagrama.
8. En relación a RIP:
   - ☐ Cuando se construye un mensaje RIP Update, el valor de la métrica se incrementa en uno respecto al que tenemos en la tabla de enrutamiento.
   - ☑ Los mensajes RIP Update se pueden enviar en cuanto hay cambios en las tablas de enrutamiento aunque no hayan pasado 30 segundos desde el último update.
   - ☑ Los mensajes que intercambian los Routers en OSPF son más complejos que cuando usan RIP.
   - ☐ Al usar Split Horizon en RIP se envía más información entre Routers.

Primer control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		16/04/18	Primavera 2018
NOM (en MAJÚSCULES):	COGNOMS (en MAJÚSCULES):	GRUP:	DNI:

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

Problema 1 (4 puntos).

Un grupo de escuelas (A, B, C) dispone de una red según la figura.
Cada escuela tiene una pequeña red para gestión con 5 PCs cada una (N1, N3, N5) y otra para aulas (N2, N4, N6, las tres del mismo tamaño).
Las escuelas están interconectadas y comparten dos conexiones a Internet.
Utilizamos el rango de direcciones 192.168.0.0/24 para todas las direcciones en estas redes.



a) (1 punto) Comenzando la asignación por un extremo, o bien las direcciones más altas (192.168.0.255) o las más bajas (192.168.0.0), explica qué direcciones asignar a cada extremo de los enlaces RA-RB, RA-RC y RB-RC.

A continuación se muestran dos soluciones según comience la asignación.

Interfaz	Red/num (desde final)	IP	Red/num (desde principio)
RAe1	192.168.0.252/30	+1 = 192.168.0.253	192.168.0.0/30
RAe2	192.168.0.248/30	+1 = 192.168.0.249	192.168.0.4/30
RBe0	192.168.0.248/30	+2 = 192.168.0.250	192.168.0.4/30
RBe1	192.168.0.244/30	+1 = 192.168.0.245	192.168.0.8/30
RCe3	192.168.0.244/30	+2 = 192.168.0.246	192.168.0.8/30
RCe4	192.168.0.252/30	+2 = 192.168.0.254	192.168.0.0/30

Hasta 2 bits para 2 direcciones (dirección de red + 1 y +2, dejando libre la primera y última del rango)

b) (1.5 punto) ¿Qué rangos de direcciones asignarías a cada red para que N2, N4, N6 tengan el máximo (y el mismo) número de PCs? Explicar qué direcciones quedarían sin asignar.
Ocupadas las direcciones más altas a partir de 192.168.0.244 (1111 0100), queda espacio para asignar 3 redes de 5 PCs (3 bits host) que podrían ser N1 .232 (1110 1xxx), N3 .224 y N5 .216.
Las redes N2, N4 y N6 tendrán el mismo tamaño: Hacen falta 2 bits diferentes de las redes ya asignadas. Por tanto una red comenzará por 00 (binario), la segunda 01 (64), y la tercera 10 (128). La última combinación (11) queda con 216-192=24 direcciones sin asignar. También queda sin asignar una /30 (4 direcciones)
Las redes /26 tienen espacio para 2^6-3 = 61 PC.

A continuación se muestran dos soluciones alternativas según comience la asignación.

Red	Red/num (desde final)	Red/num (desde principio)
N1	192.168.0.232/29	192.168.0.16/29
N3	192.168.0.224/29	192.168.0.24/29
N5	192.168.0.216/29	192.168.0.32/29
N2	192.168.0.0/26	192.168.0.64/26
N4	192.168.0.64/26	192.168.0.128/26
N6	192.168.0.128/26	192.168.0.192/26
Sin asignar	192.168.0.192 – 192.168.0.215 ...	192.168.0.40 – 192.168.0.63 ...

Se activa RIPv2 con split horizon en los routers:
c) (0.75 punto) Rellenar la tabla de routing del router RB

Destino	Gateway	Interfaz	Métrica
N3	*	e3	1
N4	*	e4	1
NAB	*	e0	1
NBC	*	e1	1
NAC	RCe3 (192.168.0.246) / RAe2	e1 / e0	2
N1	RAe2 (192.168.0.249)	e0	2
N2	RAe2 (192.168.0.249)	e0	2
N5	RCe3 (192.168.0.246)	e1	2
N6	RCe3 (192.168.0.246)	e1	2
0.0.0.0/0	*	e2	1

d) (0.25 punto) Si falla el enlace RA-RB, qué métrica anunciará RA y RB cuando lo detecten?

Indicarán métrica 16 (infinito) de ese enlace y se propagará en las actualizaciones.

e) (0.5 punto) Si además del enlace RA-RB, también falla la conexión a Internet de RB, cómo quedará la tabla de routing finalmente? (Escribir sólo las modificaciones)

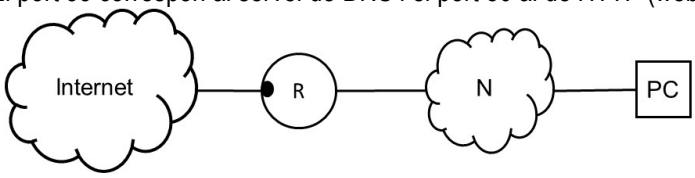
Destino	Gateway	Interfaz	Métrica
N3	*	e3	1
N4	*	e4	1
NAB	*	e0	16
NBC			
NAC	RCe3 (192.168.0.246)	e1	
N1	RCe3 (192.168.0.246)	e1	3
N2	RCe3 (192.168.0.246)	e1	3
N5			
N6			
0.0.0.0/0	RCe3 (192.168.0.246)	e1	2

Primer control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		16/04/18	Primavera 2018
NOM (en MAJÚSCULES):	COGNOMS (en MAJÚSCULES):	GRUP:	DNI:

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

Problema 2 (2 punt)

A la interfície externa del router de la figura es defineix la següent llista d'accés (ACL) o regles del tallafocs (Firewall). El port 53 correspon al servei de DNS i el port 80 al de 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	>1024	UDP/TCP	ACCEPT
3	OUT	N	>1024	D1	53	UDP/TCP	ACCEPT
4	IN	ANY	80	N	>1024	TCP	ACCEPT
5	OUT	N	>1024	ANY	80	TCP	ACCEPT
6	IN	ANY	>1024	N	80	TCP	ACCEPT
7	OUT	N	80	ANY	>1024	TCP	ACCEPT
8	ANY	ANY	ANY	ANY	ANY	ANY	DENY

Per a cada una de les transaccions indica la seqüència de paquets que entren i surten per la interfície externa del router. A la columna "Acció" indica amb X quan el tallafocs no permet el pas del datagrama. Les fletxes indiquen el sentit de transmissió: ← cap a Internet, → cap a la xarxa interna N.

Per exemple: PC es vol connectar al servidor de correu M i envia un paquet SMTP cap al servidor extern.

← / →	Aplicació	Protocol	Regla	Acció
←	Mail (SMTP)	TCP	8	X

a) Des d'un dispositiu extern es fa "ping PC"

← / →	Aplicació	Protocol	Regla	Acció
→	Ping	ICMP	1	
←	Ping	ICMP	8	X

b) Des del PC es fa una consulta al servidor extern de DNS D1

← / →	Aplicació	Protocol	Regla	Acció
←	DNS	UDP	3	
→	DNS	UDP	2	

c) Des del PC es fa una consulta al servidor extern de DNS D2

← / →	Aplicació	Protocol	Regla	Acció
←	DNS	UDP	8	X

d) Pot haver connexions de clients externs a servidors HTTP ubicats a la subxarxa N? Quines regles ho permeten o ho prohibeixen?

Les regles 6 i 7 permeten que clients externs es puguin connectar als servidors HTTP de la subxarxa N

e) Pot haver connexions a servidors HTTP externs des de la subxarxa N? Quines regles ho permeten o ho prohibeixen?

Les regles 4 i 5 permeten clients de la subxarxa N connectar-se amb servidors externs