Primer control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		02/11/17	Tardor 2017
NOM (en MAJÚSCULES):	**COGNOMS (en MAJÚSCULES):**	**GRUP:**	**DNI:**

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

Test (3 punts).

Preguntes de resposta múltiple (una o més respostes correctes). Valen la mitat si hi ha un error i 0 si més.

1. Sobre el protocol IP
- ✓ Qualsevol dispositiu amb dues o més interfícies pot fer de 'router' si s'activa "IP forwarding".
- ✓ La capçalera d'un datagrama IP té un camp de verificació d'errors.
- ✓ El protocol IP proporciona un servei del tipus "best effort".
- ✓ El protocol IP permet transportar paquets entre dos dispositius d'usuari ("host") però es poden perdre paquets.

2. Sobre el protocol IP
- ☐ Les adreces IPv4 tenen 32 bits i els 18 primers identifiquen la xarxa.
- ☐ La capçalera dels paquets IP es modifica a cada router posant-hi l'adreça IP del següent router.
- ☐ Els paquets IP segueixen sempre el mateix camí per arribar al destí.
- ✓ La fragmentació d'un datagrama es pot evitar amb el 'flag DO NOT FRAGMENT' a la capçalera del paquet IP.

3. El protocol ARP
- ✓ En una xarxa Ethernet s'envia un ARP-Request si l'adreça IP del següent dispositiu no està a la taula ARP.
- ☐ Permet descobrir l'adreça de nivell físic del destí final.
- ✓ Permet detectar dispositius amb adreces IP duplicades a la mateixa xarxa.
- ☐ Es basa en un servidor específic que resol les associacions entre adreça IP i adreça física (MAC).

4. Quins dels següents blocs d'adreces IP inclouen l'adreça 171.15.66.234?
- ✓ 128.0.0.0 /1
- ✓ 128.0.0.0 /2
- ☐ 171.15.0.0 /18
- ✓ 171.15.66.234 /32

5. Quines de les adreces següents poden ser l'adreça d'una subxarxa?
- ✓ 71.184.81.0 /24
- ☐ 71.184.81.0 /20
- ☐ 71.184.81.32 /26
- ✓ 71.184.81.64 /26

6. Marca les afirmacions que són correctes
- ☐ Quan un router perd un datagrama, envia un missatge de control ICMP a la destinació del datagrama perdut
- ✓ Quan un router troba el camp TTL d'una capçalera IP igual a 0, descarta el datagrama
- ☐ Quan hi ha fragmentació un datagrama que és un fragment no es pot tornar a fragmentar.
- ✓ Tots els fragments del datagrama original es reconeixen perquè tenen el mateix identificador.

7. Sobre NAT i PAT
- ✓ El mecanisme de NAT dinàmic pot assignar adreces públiques diferents als hosts de la xarxa privada.
- ☐ Els routers que fan PAT utilitzen un protocol per identificar les associacions @ privada - @ pública.
- ☐ El PAT no es pot aplicar de forma recursiva; només funciona un sol nivell de PAT.
- ☐ Dues xarxes privades remotes es poden connectar entre elles a través d'Internet utilitzant PAT o túnel IP, però sempre amb els dos mecanismes a la vegada.

8. Sobre els servidors DHCP
- ☐ El servidor ha d'estar ubicats sempre al router de la xarxa.
- ✓ El servidor DHCP pot proporcionar l'adreça IP del servidor del domini DNS
- ☐ L'única forma d'obtenir una adreça IP per un host és utilitzant el protocol DHCP.
- ✓ Si no es fan servir mecanismes especials, el servidor DHCP ha d'estar a la mateixa subxarxa que els clients.

First Midterm. Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		02/11/2017	Fall 2017
NAME (in CAPITAL LETTERS):	**FAMILY NAME (in CAPITAL LETTERS):**	**GROUP:**	**DNI/NIE:**

Time: 1hour and 30 minutes. The quiz will be collected in 25 minutes.

Test (3 points).

Multiple choice questions (any number of correct answers). Half value if there is one error and 0 if there are more.

1. About the IP protocol
- ✓ Any device with two or more interfaces may perform as a router if "IP forwarding" is activated.
- ✓ The header of an IP datagram contains a filed for error checking.
- ✓ The IP protocol provides a service known as "best effort".
- ✓ IP protocol allow to transport IP datagrams between two user's devices ("host") but some packets may get lost.

2. About the IP protocol
- ☐ IPv4 addresses have 32 bits and the first 18 bits identify the network.
- ☐ At each router, the IP header is modified to include the IP address of the next router.
- ☐ IP packets follow the same path to reach the destination always.
- ✓ The fragmentation of a datagram may be avoided using the 'DO NOT FRAGMENT' flag of the IP header.

3. About the ARP protocol
- ✓ In an Ethernet network, an ARP-Request is sent if the IP address of the next device is not found in the ARP table.
- ☐ Allows to find out the physical layer address of the remote destination device.
- ✓ Allows the detection of supplicate IP addresses in the same network.
- ☐ It is based on a server which resolves the associations between the IP address and the corresponding physical address (MAC address).

4. Which of the following blocks include the address 171.15.66.234?
- ✓ 128.0.0.0 /1
- ✓ 128.0.0.0 /2
- ☐ 171.15.0.0 /18
- ✓ 171.15.66.234 /32

5. Which of the following addresses may be a subnetwork address?
- ✓ 71.184.81.0 /24
- ☐ 71.184.81.0 /20
- ☐ 71.184.81.32 /26
- ✓ 71.184.81.64 /26

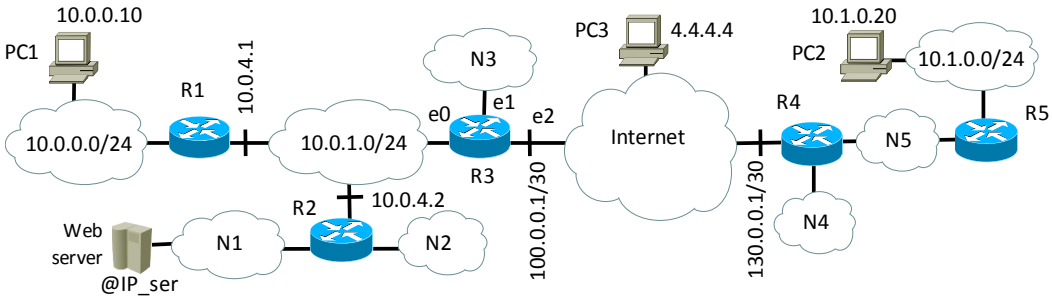
6. Check all the correct sentences
- ☐ When a router loses a datagram, it sends an ICMP control message to the destination of the lost datagram
- ✓ When a router finds the TTL field of an IP header equal to 0, it discards the datagram
- ☐ When a datagram is fragmented the new fragment cannot be fragmented again.
- ✓ All fragments of the original datagram can be recognized because all of them have the same identifier.

7. About NAT and PAT
- ✓ The dynamic PAT mechanism may allocate different IP public addresses to different hosts of the private network.
- ☐ All router implementing PAT use a protocol to identify the associations "Private Address – Public Address".
- ☐ PAT cannot be applied recursively. It only works once and a datagram cannot go through several PAT.
- ☐ Two remote private networks may connect themselves across the Internet using PAT or an IP tunnel but always with both mechanisms at the same time.

8. About the DHCP server
- ☐ The server must always be located on the router of the network.
- ✓ The DHCP server can provide the IP address of the DNS domain server
- ☐ The only way to get an IP address for a host is by using the DHCP protocol.
- ✓ If special mechanisms are not used, the DHCP server must be in the same subnet as the clients.

Solución

Problema 1 (5 puntos)
La red de la figura consiste de 2 partes: una sede central y una sucursal. Se ha configurado una VPN que mantiene un túnel entre R3 y R4 con interfaces llamadas tun0 y direcciones 192.168.0.1/30 y 192.168.0.2/30 respectivamente. Para dar salida a Internet a todos los hosts privados de la red, R3 aplica NAT dinámico con rango 100.0.0.5-100.0.0.25.



Deterninar

a) (1,75 puntos) Un direccionamiento valido para las redes N1-N5 usando el rango 160.0.0.128/25 sabiendo que los requerimientos son: N1: 10 hosts, N2: 5 hosts, N3: 20 hosts, N4: 10 hosts, N5: 20 hosts

Desarrollo

N5: 20 hosts + R4 + R5 + red + broadcast = 24 → 2^5 = 32 → 5 bits de hostID
N3: 20 hosts + R3 + red + broadcast = 23 → 2^5 = 32 → 5 bits de hostID
N4: 10 hosts + R4 + red + broadcast = 13 → 2^4 = 16 → 4 bits de hostID
N1: 10 hosts + R2 + red + broadcast = 13 → 2^4 = 16 → 4 bits de hostID
N2: 5 hosts + R2 + red + broadcast = 8 → 2^3 = 8 → 3 bits de hostID

Red	netID				hostID						
Rango inicial	160.	0.	0.	1	X	X	X	X	X	X	X
5	160.	0.	0.	1	0	0	X	X	X	X	X
3	160.	0.	0.	1	0	1	X	X	X	X	X
4	160.	0.	0.	1	1	0	0	X	X	X	X
1	160.	0.	0.	1	1	0	1	X	X	X	X
2	160.	0.	0.	1	1	1	0	0	X	X	X

Solución final

Red	Bits en hostID	Dirección de red / mascara	Dirección de broadcast
5	5	160.0.0.128/27	160.0.0.159
3	5	160.0.0.160/27	160.0.0.191
4	4	160.0.0.192/28	160.0.0.207
1	4	160.0.0.208/28	160.0.0.223
2	3	160.0.0.224/29	160.0.0.231

b) (0,5 puntos) Si es posible encontrar un direccionamiento valido si se quiere juntar las dos redes N1 y N2 en una única red con un número de hosts igual a la suma de las dos. Si es posible, determinar este direccionamiento.

N: 15 hosts + R2 + red + broadcast = 18 → 2^5 = 32 → 5 bits de hostID

Red	netID				hostID							Direccion de red
Rango inicial	160.	0.	0.	1	X	X	X	X	X	X	X	
5	160.	0.	0.	1	0	0	X	X	X	X	X	160.0.0.128/27
3	160.	0.	0.	1	0	1	X	X	X	X	X	160.0.0.160/27
4	160.	0.	0.	1	1	0	0	X	X	X	X	160.0.0.192/28
1+2	160.	0.	0.	1	1	1	X	X	X	X	X	160.0.0.224/27

c) (1,25 puntos) Se activa RIPv2 en todo el sistema (sin sumarización de rutas). Determinar la tabla de encaminamiento de R3 completando la tabla. Recordar que en la columna Adq (adquisición), hay que poner C por conectada directamente, S por estática y R por RIP.

Adq	Destino	Mascara	Gateway	Interfaz	Métrica
C	N3		-	e1	1
C	10.0.1.0	/24	-	e0	1
C	100.0.0.0	/30	-	e2	1
C	192.168.0.0	/30	-	tun0	1
R	10.0.0.0	/24	10.0.4.1	e0	2
R	N1		10.0.4.2	e0	2
R	N2		10.0.4.2	e0	2
R	N4		192.168.0.2	tun0	2
R	N5		192.168.0.2	tun0	2
R	10.1.0.0	/24	192.168.0.2	tun0	3
S	0.0.0.0	/0	100.0.0.2	e2	-

a) (1 puntos) Se quiere configurar el router R3 como firewall. En particular se quiere crear una única ACL de manera que
   i. Clientes de Internet solo puedan acceder al servidor web (puerto TCP 80) conectado a la N1 (suponer la @IP IP_serv)
   ii. Host de toda la red privada 10.0.0.0/8 puedan acceder a servicios conocidos TCP de Internet

Determinar a qué interfaz hay que asignar la ACL y en qué sentido (entrada o salida) del router R3 y completar la tabla con la configuración de esta ACL

INTERFAZ: e0 SENTIDO: salida

Permit/deny	Protocolo	Origen		Destino		Estado
		@IP/Mascara	puerto	@IP/Mascara	puerto	
Permit	TCP	0.0.0.0/0	>1023	@IP_ser	80	
Permit	TCP	0.0.0.0/0	<1024	10.0.0.0/8	>1023	respuestas
Deny	IP	0.0.0.0/0		0.0.0.0/0		

d) (0,5 puntos) Las direcciones IP origen y destino de los datagramas que entran y salen del router R3 para estos dos casos:

i. PC1 hace un ping a PC2

Entre por e0 con @IP origen 10.0.0.10 y destino 10.1.0.20 Sale con @IP origen 100.0.0.1 y destino 130.0.0.1

ii. PC1 hace un ping a PC3

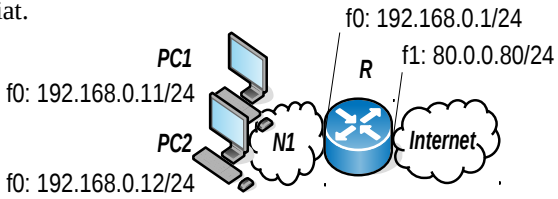
Entre por e0 con @IP origen 10.0.0.10 y destino 4.4.4.4 Sale con @IP origen 100.0.0.5 y destino 4.4.4.4

Primer Control de Xarxes de Computadors (XC), Grau en Enginyeria Informàtica		2/11/2017	Tardor 2017
Nom:	**Cognoms:**	**Grup**	**DNI**

Duració: 1h30m. El test es recollirà en 25m. Repondre en el mateix enunciat.

Problema 2 (2 punts)

En la xarxa de la figura en PC1 s'executa ping -c 1 192.168.0.255, que envia un sol missatge echo request. Totes les taules ARP estan buides i tots els dispositius de la xarxa (PCs i router) responen al ping. Respon les següents preguntes, si cal, comenta les suposicions que facis i inventa't les dades que necessitis i no doni l'enunciat.



2.1 (1 punt) Omple la taula amb el detall dels missatges que s'enviaran. En la columna «tipus de missatge» posa la informació rellevant del missatge enviat. Posa un guió «-» en les caselles que no apliquin. Fes servir només les files que necessitis.

Notació: posa pc1 per referir-te a l'adreça MAC de la interfície f0 de PC1, i PC1 per referir-te a l'adreça IP de la interfície f0 de PC1, anàlogament per PC2 i el rouer R; ff per l'adreça MAC broadcast.

Capçalera ethernet		Capçalera IP		
Font	Destinació	Font	Destinació	Tipus de missatge
pc1	ff	PC1	192.168.0.255	ICMP echo request broadcast
-	-	PC1	PC1	ICMP echo reply
pc2	ff	-	-	ARP request MAC PC1?
pc1	pc2	-	-	ARP reply amb pc1
pc2	pc2	PC2	PC1	ICMP echo reply
r	ff	-	-	ARP request MAC PC1?
pc1	r	-	-	ARP reply amb pc1
r	pc1	R	PC1	ICMP echo reply

2.2 (1 punt) Omple el contingut que tindran les taules ARP dels dispositius quan s'hagin acabat d'enviar els missatges anteriors (i no s'ha enviat cap altre missatge). Fes servir la mateix notació que abans per les adreces MAC i adreces IP.

Taula ARP de PC1		Taula ARP de PC2		Taula ARP de R	
MAC	IP	MAC	IP	MAC	IP
pc2 r	PC2 R	pc1	PC1	pc1	PC1