Computer Networks - *Xarxes de Computadors*

Outline

- Course Syllabus
- Unit 1: Introduction
- **Unit 2. IP Networks**
  - **Resolució examen 2021t-c - test**
- Unit 3. LANs
- Unit 4. TCP
- Unit 5. Network applications

Duració: 1h 30 minuts. El test es recollirà en 20 minuts.

Test (3 punts). Les preguntes valen la mitat si hi ha un error i 0 si hi ha més d'un error a la resposta.

1. En una xarxa de commutació de paquets en mode datagrama (xarxa IP)

- ☐ Cada paquet d'una comunicació extrem a extrem va identificat amb el mateix identificador de fragment.
- ☐ Els paquets d'una mateixa comunicació extrem a extrem segueixen el mateix camí dins la xarxa.
- ☒ Els paquets d'una mateixa comunicació extrem a extrem són processats en tots els routers per on passen.
- ☐ Alguns paquets es poden perdre però arriben al destinatari sempre ordenats.

4. Si la MTU ("*Maximum Transmission Unit*") és 1448, i es vol transmetre un datagrama amb un camp de dades de:

- ☒ 1400 octets (bytes) no caldrà fer fragmentació.
- ☐ 1440 octets (bytes) no caldrà fer fragmentació.
- ☒ 4912 octets (bytes) hi haurà fragmentació i es transmetran 4 datagrames (fragments).
- ☐ 4912 octets (bytes) hi haurà fragmentació i es transmetran 5 datagrames (fragments).

Atenció: capçalera IP > 40 bytes → 2 paquets => resposta 1 no correcta

// == divisió entera; % == mòdul

IP 20bytes:
1400 // (1448 – (20)) = 0
1400 % (1448 – (20)) = 20

IP 20bytes, UDP 8bytes:
1400 // (1448 – (20 + 8)) = 0
1400 % (1448 – (20 + 8)) = 20

IP 20bytes:
1400 // (1448 – (60)) = 1
1400 % (1448 – (60)) = 12

IP 20bytes, UDP 8bytes:
1400 // (1448 – (60 + 8)) = 1
1400 % (1448 – (60 + 8)) = 20

7. Sobre el protocol IP.

- ☐ És un protocol orientat a la connexió.
- ☐ És un protocol d'aplicació entre el client i el servidor.
- ☒ És un protocol que no proporciona una comunicació fiable.
- ☐ És un protocol amb adreces de longitud variable.

IP 20bytes:
4912 // (1448 – 20) = 3
4912 % (1448 – 20) = 628

IP 20bytes, UDP 8bytes:
4912 // (1448 – (20 + 8)) = 3
4912 % (1448 – 20) = 652

IP 60bytes, UDP 8bytes:
4912 // (1448 – (60 + 8)) = 3
4912 % (1448 – (60 + 8)) = 772

8. Sobre el protocol ARP (*Address Resolution Protocol*).

- ☐ El protocol utilitza datagrames de *broadcast* per resoldre l'adreça de destinació.
- ☒ Els missatges *ARP Request* utilitzen trames Ethernet de *broadcast*.
- ☒ S'utilitza per trobar l'adreça MAC (física) associada a una adreça IP de la mateixa xarxa.
- ☒ La taula ARP conté l'associació adreça MAC – adreça IP si la comunicació està activa (amb intercanvi de trames).

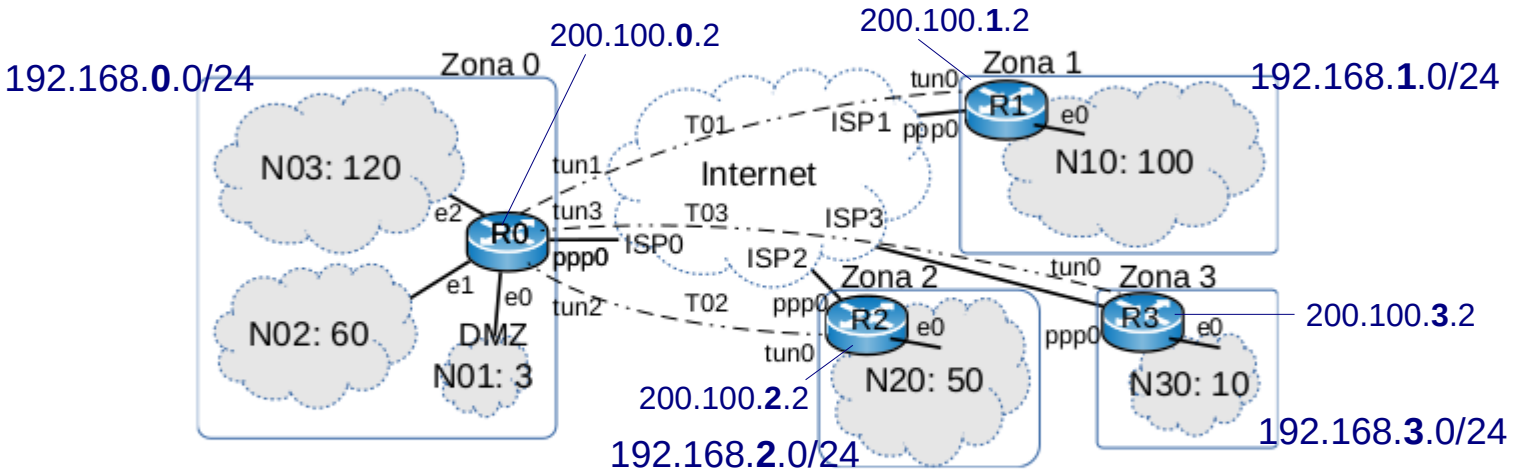
Computer Networks - *Xarxes de Computadors*

Outline

- Course Syllabus
- Unit 1: Introduction
- **Unit 2. IP Networks**
  - **Resolució examen 2021t-c – Problema 1**
- Unit 3. LANs
- Unit 4. TCP
- Unit 5. Network applications

Problema 1 (5 punts)

Una empresa de serveis internet té 4 zones Z={*0..3*}: una seu (zona 0) amb el personal de gestió i sistemes, prepara una nova xarxa global amb servidors a 3 països (zones 1, 2, 3) segons la figura.



Per cada xarxa la figura indica el nombre de hosts màxim que s'esperen connectar (per ex. N10: 100).
L'adreçament de cada xarxa es fa amb adreces privades classe C de rangs que comencen per 192.168.
Cada zona té assignada una xarxa: zona **Z** 192.168.**Z**.0/24. Per exemple 192.68.0.0/24 a la zona 0.
Cada ISP**Z** assigna la IP pública 200.100.**Z**.2 a R**Z**. Per exemple ISP0 assigna 200.100.0.2 a R0.
Cada zona esta interconnectada amb la seu central per internet amb un túnel IPinIP.

Typo: 168

Atenció: info rellevant

a) (1 punt) Assigna rangs d'adreces privades a cada subxarxa de forma compacta (sense forats a cada zona i mínim forat entre zones) per permetre l'agregació per zones als routers.

Rangs IP	#H	Xarxa	Adreça/màscara
192.168.**0**.0/24	120	N03	192.168.0.0/25
	60	N02	192.168.0.128/26
	3	N01	192.168.0.192/29
192.168.**1**.0/24	100	N10	192.168.1.0/25
192.168.**2**.0/24	50	N20	192.168.2.0/26
192.168.**3**.0/24	10	N30	192.168.3.0/28
	2	T01	192.168.4.0/30
	2	T02	192.168.5.0/30
	2	T03	192.168.6.0/30

Altres tb ok

Netmask	# IPs	# hosts	IP min (netid)	IP max (broadcast)
/24	$2^8 = 256$	256-2 = 254	Netid + 0	Netid + 255
/25	$2^7 = 128$	128-2 = 126	Netid + 0	Netid + 127
/26	$2^6 = 64$	64-2 = 62	Netid + 0	Netid + 63
/27	$2^5 = 32$	32-2 = 30	Netid + 0	Netid + 31
/28	$2^4 = 16$	16-2 = 14	Netid + 0	Netid + 15
/29	$2^3 = 8$	8-2 = 6	Netid + 0	Netid + 7
/30	$2^2 = 4$	4-2 = 2	Netid + 0	Netid + 3
~~/31~~	~~$2^1 = 2$~~	~~2-2 = 0~~		
/32	$2^0 = 1$	1	IP	

b) (0.25 punts) Quin és el rang agregat d'adreces per la zona 0 i perquè?

Z0: 192.168.0.0/24. Només pot ser una /24 perquè N03 ja és una /25 (la primera) i N02 ja ocupa espai de la segona i, per tant, com a mínim ha de ser una /24. Amb /24 n'hi ha prou, perquè N01 i N02 estan dins de la segona /25.

Observació: info redundant (ja ens han dit que era RIPv2), però que ens ajuda a evitar errors

c) (0.5 punts) Si es fa servir RIPv2 amb split horizon per anunciar totes les xarxes, també les estàtiques, tenint en compte l'agregació a la classe de RIP. Quin serà el contingut dels missatges que s'enviaran al túnel entre les zones 0 i 1? Dona la resposta en forma *(Xzn, m)*, 0/0 és ruta per defecte, i *m* és la mètrica.

Atenció: info rellevant pq RIPv2 també pot fer VLSM

R0 envia: (Z0, 1), (192.168.5.0, 1), (192.168.6.0,1), (0/0,1), (Z2,2), (Z3,2)

R1 envia: (Z1,1), (0/0,1)

L'enunciat diu que s'anuncien "totes" les rutes, per tant, estrictament parlant també caldria anunciar les dels ISPs, és a dir, R0: (200.100.0.0,1), (200.100.2.0,2) i (200.100.3.0,2) i R1 (200.100.1.0,1), tot i que a la pràctica aquests auncis no són habituals perquè aquestes rutes només són d'interés local. Per aquesta mateixa raó, té poc sentit anunciar l'accés a internet, quan aquest accés és necessari per fer l'anunci.

Orientació 1: cal identificar exactament a quines xarxes pertany cada router; cal parar atenció especial al router R1
Orientació 2: cal identificar quines rutes ha après cada router i de quin altre router les ha après per fer be l'"split horizon"

Atenció: ara ens demanen sobre R1; cal llegir bé els anunciats

d) (1 punt) Completar la taula d'encaminament de R1 una vegada la xarxa ha arribat al equilibri:

Xarxa	Gateway	Interface	Mètrica
N10	–	e0	1
N20	192.168.4.1	tun0	3
N30	192.168.4.1	tun0	3
Z0	192.168.4.1	tun0	2
T01	–	tun0	1
T02	192.168.4.1	tun0	2
T03	192.168.4.1	tun0	2
ISP1	–	ppp0	1
0/0	ISP1-gw	ppp0	1

Orientació: és un cas relativament senzill perquè i) aquest router només té 3 NICs i ii) ens donen totes les xarxes. Només cal parar una mica d'atenció amb les mètriques.

Atenció: aquesta entrada ens orienta sobre la nomenclatura I format

e) (0.75 punts) Es fa servir PAT a cada router connectat a internet. Indica el valor de la capçalera IP externa dels datagrames que entren i surten de R0 si un client de la xarxa N03 fa:

Atenció: info rellevant

Cas 1: una connexió TCP cap a un servidor a internet (1.2.3.4:80)

Cas 2: una connexión a un servidor a N3.

Atenció: a l'enunciat hi manca dir que la conneixó és TCP i N3 hauria de ser N30 (typo)

Cas1

Interface	IP origen	IP destí	Protocol
e2	192.168.0.2	1.2.3.4	TCP
ppp0	200.100.0.2	1.2.3.4	TCP

Cas 2:

Interface	IP origen	IP destí	Protocol
e2	192.168.0.2	192.168.3.2	TCP
ppp0	200.100.0.2	200.100.3.2	IPIP

Orientació: el primer cas es tracta d'un cas de PAT amb sortida a internet estàndard, per tant, només es fa la substitució de l'IP d'origen i només hi ha una capçalera IP. En el segon cas, però, no es fa PAT sinó un encapusalment IPIP i, per tant, hi haurà dues capçaleres IP i el protocol de l'externa serà IPIP (i el de l'interna TCP).

f) (0.25 punts) Si volem permetre connexions des d'internet només a servidors de la DMZ (N01) a la Zona 0, quin mecanisme cal activar al router?

Destination network address translation (DNAT)

Atenció: tràfic sortint

g) (0.75 punts) Indicar les regles per filtrar correctament el tràfic de servidors que surt per R0 (ACLin per e0) cap a Internet, abans d'aplicar NAT:
web: HTTP ports 80 i 443 per TCP, noms: DNS, port 53 per UDP, correu: SMTP, port 25 per TCP.

IP origen	Port origen	IP destí	Port destí	Protocol	Acció (allow/deny)
N01	80	any	> 1023	TCP	allow
N01	443	any	> 1023	TCP	allow
N01	53	any	> 1023	UDP	allow
N01	25	any	> 1023	TCP	allow
any	any	any	any	any	deny

Observació: fixem-nos que la darrera regla és una regla per defecte de “deny”. Per tant, les regles anteiors han de ser d’“allow” i n’hi ha d’haver una per cada port I protocol que volguem permetre. Cal que totes aquestes regles precedeixin a la per-defecte perquè sinó, no s’aplicarien mai.

g) (0.5 punts) Per millorar el rendiment hem afegit un túnel T12 entre la zona 1 i la zona 2. Quines entrades canvien a la taula de routing de R1? Posar només les files noves o canviades.

Xarxa	Gateway	Interface	Mètrica
T12	–	tun1	1
N20	192.168.7.1	tun1	2
ISP2	192.168.7.1	tun1	2

Les “apreses” per RIP.

Orientació: A banda de la ruta directa (sense GW) de propi túnel, hem d’identificar quines rutes indirectes s’“aprenen” a través del túnel

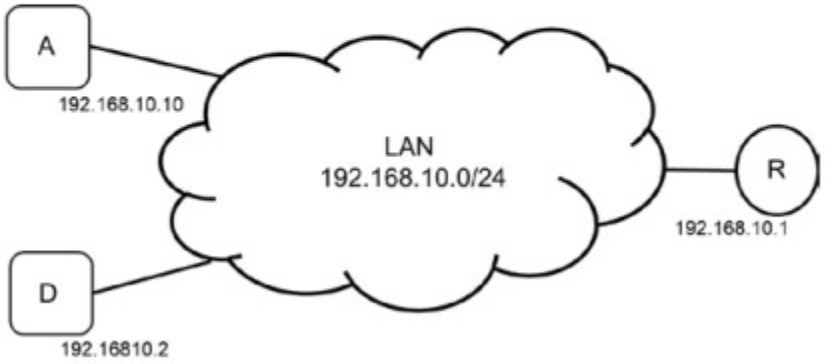
Computer Networks - *Xarxes de Computadors*

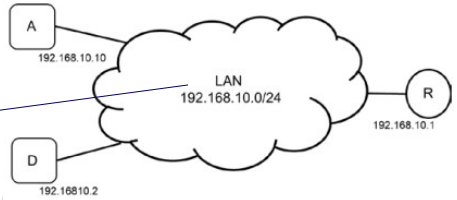
Outline

- Course Syllabus
- Unit 1: Introduction
- **Unit 2. IP Networks**
  - **Resolució examen 2021t-c – Problema 2**
- Unit 3. LANs
- Unit 4. TCP
- Unit 5. Network applications

Problema 2 (2 punts)

La figura mostra una xarxa local amb l'accés a Internet a través del router R. A és un dispositiu i D és el servidor DNS de la xarxa. La xarxa s'acaba d'inicialitzar. R i D estan correctament configurats, A rep la configuració via DHCP i totes les taules ARP estan buides.



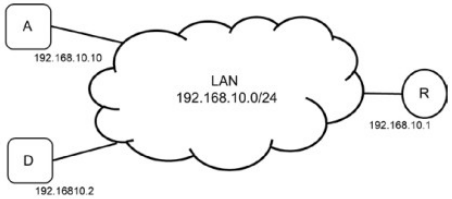


Observació: www.fib.upc.edu no pertany a la LAN

a) Tot just acabada la inicialització, el dispositiu A executa la comanda "*ping www.fib.upc.edu* . Completar la taula següent amb la seqüència de les trames i paquets IP que passen per la xarxa local fins que es rep la resposta de la comanda. D té la informació per resoldre el nom del servidor de la FIB.
Notació: l'adreça IP es representa en majúscula (R, D, A), la corresponent adreça MAC (Ethernet) en minúscula (r, d, a, respectivament). F i f representen respectivament l'adreça IP i l'adreça Ethernet del servidor web de la FIB.

	Ethernet Header		ARP message		IP Header			data
	Source	Destination	Type	Message	Source	Destination	Protocol	Message
1	a	FF:FF:FF:FF:FF:FF	REQ	D?				
2	d	a	RESP	D → d				
3	a	d			A	D	UDP	DNS RQ
4	d	a			D	A	UDP	F
5	a	FF:FF:FF:FF:FF:FF	REQ	R?				
6	r	a	RESP	R → r				
7	a	r			A	F	ICMP	Echo RQ
8	r	a			F	A	ICMP	Echo RP
9								

Observació: no sempre és necessari omplir totes les files



b) Suposem que el servidor DNS local (D) no té la informació (www.fib.upc.edu -> F) i l'ha de demanar al servidor extern dns.edu (E, e). Completar la taula anterior amb les trames Ethernet i paquets IP que passen per la xarxa local indicant on s'han de posar en la seqüència de la taula anterior (indicar el número de línia).

	Ethernet Header		ARP message		IP Header			data
	Source	Destination	Type	Message	Source	Destination	Protocol	Message
3	d	FF:FF:FF:FF:FF:FF	REQ	R?				
3.1	r	d	RESP	R → r				
3.2	d	r			D	E	UDP	DNS REQ
3.3	r	d			E	D	UDP	F
4	d	a			D	A	UDP	F

Orientació: els servidors locals DNS poden fer dues funcions a la vegada:

1) resoldre noms de la LAN

2) fer de 'cache' de resolucions que han obtingut d'altres servidors DNS amb més autoritat. Ho veurem amb més detall a la Unitat 5, la d'aplicacions; per ara només cal que sapigueu que el sistema DNS és un sistema jeràrquic recursiu: el servidor .edu és el que resol .upc.edu, el servidor .upc.edu resol www.upc.edu, etc.