Problemes de TAI

Albert Acebrón

2019

TCP

1. Per tal de reduir la congestió, quines diferències veus, a tots els nivells, entre l'aplicació de l'algorisme de van Jacobson i la utilització d'una política de gestió de cues RED? De quina manera podem relacionar la política SFQ amb l'algorisme de Karn (en el sentit de si són totalment independents, o l'un millora/altera l'altre)?

L'algoritme de van Jacobson permet als hosts respondre més ràpidament a canvis en la congestió. Aquesta adaptació ràpida millora els resultats obtinguts amb RED perquè fa que quan la cua es comenci a emplenar els hosts i els paquets s'eliminin els hosts reaccionin depressa i enviin menys paquets i disminueixi ràpidament la congestió.
En cas de que no s'apliqués l'algoritme de van Jacobson, quan la cua RED començos a eliminar paquets els hosts no reaccionarien i seguirien enviant, portant a un augment de la congestió de la xarxa, que el router elimininés molts paquets i que tots els hosts entressin en Slow Start. Això implica un sincronitzament de Slow Start, que es justament el que volem evitar utilitzant RED.

Karn i SFQ són independents.

2. Cóm argumentarieu que tancar automàticament connexions inactives és bo? Com implementaríeu aquest mecanisme de keep alive sense afegir nous bits de control a les capçaleres TCP? Com ho fa la recomanació del RFC? Han d'estar totes dues parts d'acord per tal d'utilitzar el keep alive del RFC? Justifica les respostes.

Tancar connexions inactives es bo perquè permet estalviar memòria en el servidor, ja que el servidor alloca certa memòria a cada connexió oberta.
Implementaría keep alives enviant un missatge TCP que només contingués un byte i després esperaría el ACK. Així no es necessàri cap canvi en el protocol.
Sí, el keepalive del RFC requereix que la part a la que se li envia el keep alive

tingui keep alive activat (i segons el RFC per defecte keep alive ha d'estar desactivat).

3. Si enviem dades de byte en byte en TCP, amb un byte per cada segment de dades, quin tant per cent de xarxa estaríem utilitzant pel cap alt? Com variarà en aquest cas el utilitzar una finestra d'1 byte a utilitzar una de 64 KBytes? I amb la mida màxima que permet l'opció d'escalar la finestra? I si la tasa de pèrdua és del 5%?

Si només enviem 1 byte per segment estaríem utilitzant $\frac{1}{40+1} \cdot 100$ de la xarxa (on 40 és la mida dels headers IP+TCP). Per contra, si la finestra és de 64K, enviariem segments a min(64K, MSS), els quals, considerant un MSS de 536 (el per defecte segons l'estandard), utilitzent un $\frac{536}{536+40} \cdot 100$.
Si augmentem la mida màxima de la finestra utilitzant l'escalat de finestres l'utilització de la xarxa no canvia, ja que la maximum segment size ens limita més que la finestra. L'utilització és de $\frac{536}{536+40} \cdot 100$.
La tasa de pérdua de paquets no modifica significativament el percentatge d'ús de la xarxa, ja que els paquets perduts són simplement retransmessos.

4. Tenim tres routers en seqüència (tots els datagrames que surten d'un entren en el següent),un funcionant amb PFIFO, l'altre amb RED, i l'altre amb TBF. En quin ordre els posaríeu?I si fossin RED, SFQ i TBF? Utilitza els teus coneixements i la informació que puguis trobar per a donar una justificació dels ordres proposats.

En aquest cas ens interessa evitar el problema de la sincronització dels hosts entrant en estat de congestió, el qual portaria a que tots els hosts fessin Slow Start a la vegada i es desaprofités molta bandwidth. Per tal d'evitar això ficarem primer els routers amb polítiques més permissives i després els routers amb polítiques més estrictes, donat lloc al següent ordre:

1. TBF
2. RED
3. PFIFO

Aquest ordre ens permet dropejar paquets de forma progressiva per evitar sincronitzacions.
Raonament: Si no possesim PFIFO últim es podrien acumular paquets i causar eliminacions d'aquests massives, causant sincronitzacions de Slow Start.
Triant entre TBF i RED pel primer lloc agafem TBF primer perquè si fos al revés RED bloquejaria rafàgues espòradiques dels hosts (la probabilitat augmentaria i els paquets es dropejarien).

En el cas de RED, SFQ i TBF:

1. TBF
2. RED

3. SFQ

5. Imagina que en el router de l'Autònoma volem utilitzar cues diferents per a cada connexió per a que el tràfic d'excés sigui descartat de manera justa. Veus algun problema en buscarla justicia total? Com ho fa SFQ? En cas afirmatiu, com ho podries solucionar? Troba o dissenya una política també basada en la justífica que sigui diferent de SFQ, i explica el seu funcionament.

Un possible problema es que un host podria aconseguir transmetre moltes més dades que els altres a base d'obrir moltes conexions diferents. A més depenent de com s'implementés aquesta cua podria no funcionar bé amb ràfegues.
SFQ crea una cua per cada conexió i utilitza round robin sobre aquestes cues per a decidir quin paquet transmetre.
Una solució podria ser crear una cua com la SFQ amb els següents canvis:

- En comptes de classificar els paquets per conexió es classificarien els paquets pel host del que provinguessin.
- S'implementaría una solució similiar a la del PBF (uns tokens que es poguessin acumular i gastar en ràfagues) per tal de deixar passar ràfagues.

El mecanisme per decidir quin paquet enviar seria round robin amb la modificació de que si un host té molts tokens acumulats s'enviarien k paquets seus en comptes de només 1 quan li arribés el torn per round robin, on k es determinaria en funció dels tokens acumulats.

6. Assumint que tant la capacitat de l'enllaç com la finestra de recepció són infinits, quants RTTs calen per a enviar els primers 20 segments de TCP si s'utilitza slow start amb un valor inicial de 1 MSS? i si el valor inicial és de 4 MSS? Podries generalitzar per cas dels k primers segments i valor inicial i MSS? Descriu alguna proposta d'eixamplar la finestrainicial i comenta-la.

Com que capacitat i recepció són infinites només estem limitats per el mecanisme de Slow Start, el qual farà que cada vegada que reben confirmacions enviem el doble de paquets enviats abans:
1 MSS
2 MSS
4 MSS
8 MSS -> 15 MSS enviats
16 MSS -> 31 MSS enviats, ja arribem als 20 MSS
Observem que el temps total és de $4 \cdot R\top$. En cas de començar amb $4 \cdot MSS$, tardaríem $2 \cdot R\top$.En el cas general, si comencem amb i MSS i volem enviar k, el temps serà superior o igual a $\log 2\left(\frac{k}{i}\right)$.

7. Quin és el problema que tindria RED si apliquès la funció de probabilitat directament sobrela mida de la cua i que afectaria als darrers datagrames de les ràfagues? De quina maneraho soluciona? Quina relació té aquesta solució amb el càlcul de l'estimació del RTT pertal de calcular el timeout de retransmissió en TCP? Tindria sentit aplicar van Jacobson enaquest context? Quin serien els efectes?

El problema seria que al tenir una ràfega la cua s'emplenaria molt despressa i al últims paquets de les ràfegues s'els hi aplicaria una probabilitat de dropeig molt alta. Es soluciona aplicant la probabilitat basada en una mitjana de la mida de la cua, de manera que un pic puntual (causat per una ràfaga per exemple) no alteri la probabilitat molt.

8. Quin és el throughput màxim de TCP si el RTT promig és de 15ms, les capçaleres de laxarxa física són sempre 66 bytes, i el MTU és 128 KBytes? Fes ara el promig en funció delMTU i del RTT. En aquesta xarxa, a partir de quin RTT quedaria justificada la utilitzacióde la opció d'escalat de la finestra?

Assumim que la finestra té de mida N MTU. Llavors el throughput màxim serà de $\frac{N \cdot MTU}{R\top} = N \cdot \left(\frac{128 \cdot 1000}{\frac{15}{1000}}\right)$ bytes/s.
No hi ha suficients dades com per decidir a partir de quin RTT seria millor escalar la finestra. En cas de que la transmissió fos perfecta la finestra s'hauria d'escalar a l'infinit.

9. Seria possible tenir TCP per sobre d'Ethernet directament, sense utilitzar IP? I tenir TCPsobre un altre TCP sobre IP (els MSS haurien de ser diferents, és clar)? Raona els motius iles limitacions que trobis en aquestes dues situacions considerant els diferents mecanismesque hem vist al llarg del tema.

Seria possible però aquest sistema només funcionaria per a conectar nodes de la xarxa local (ja que com no tenim IP no podem especificar destinari). Això podria servir per eliminar els headers de IP però si només podem comunicarnos per la xarxa local és una mica inutil.
TCP sobre TCP sobre IP és possible ja que la payload de TCP poden ser dades arbitràries. Pot ser utilitzat per realitzar tunels en sistemes que no deixen passar paquets que no siguin TCP (o paquets que no siguin TCP al port 80) a canvi d'incorrer en un cost més elevat d'enviament (hem d'incloure headers inecessàris).

10. Si estem connectats a Internet utilitzant wireless, i estem descarregant un fitxer gran ambun protocol sobre TCP, explica quin efecte sobre el throughput tindrà embolicar l'antenadurant exactament un minut i mig amb un troç de paper de plata connectat a terra. Tinguesen compte els diferents mecanismes que utilitza TCP. Podries quan-

tificar d'alguna manera(encara que sigui aproximadament) la pèrdua de throughput ocasionada per aquest event?Com es podria minimitzar?

Es perdria tota la informació que s'hagués pogut enviar durant el minut i mig a la velocitat, i, a més la pérdua de paquets activaria el mecanisme de congestió de TCP implementat en el sistema, que al fallar també acabaria portant la finestra a la mida mínima. Finalment el temps de timeout dels paquets augmentaria de forma massiva.
Tot això portaria a que després de retirar el paper de plata de l'antena

11. Quines són les diferències i semblances entre el backoff del timeout de l'algorisme de Karn, el timeout del mecanisme de Keep Alive, i el timer de persistència amb backoff de les emissions en finestra zero del protocol TCP? Per a cada cas, detalla també quin és el problema que volen solucionar, com funcionen, i quin impacte tenen en el throughput global de TCP.

Backoff de Karn: Soluciona el problema del càlcul del timeout en conexions TCP. Funciona a base d'incrementar el timeout exponencialment (multiplicant per 2) cada vegada que el timeout s'activa. Incrementa el throughput del TCP comparat amb utilitzar un timeout constant perquè s'adapta a les condicions actuals de la conexió TCP.

Keep Alive: Soluciona el problema de conexions TCP que es mantenen obertes quan realment el receptor ja les ha tancat o ha desaparegut. Funciona enviant paquets en la conexió períodicament per tal de comprovar si el receptor contesta. En cas de que el receptor no contesti al primer paquet es van enviant més cada x segons, on x incrementa exponencialment. No afecta al throughput del TCP.

Timer de persitència: Soluciona el problema donat per la possibilitat de creació de deadlocks en una conexió TCP causades per un receptor anunciant una finestra de 0 i l'altre costat no responent amb cap més missatge (perquè la finestra seria de 0). Funciona a base d'enviar un paquet cada $\min(5, 1.5 \cdot 2^n)$ segons, on n es va incrementant a cada enviament de paquet mentres la finestra es manté a 0. Tècnicament disminueix una mica el throughput ja que fa que s'enviin paquets que no són estrictament necessàries, però aquesta disminució es negligible perquè l'activació d'aquest timer es molt poc comuna.

NAT

1. Comenta les restriccions que tindran tres xarxes amb espais d'adreçament diferents connectades, de manera asimètrica, a través de dos routers fent NAT d'origen i NAT de destinació. Quantes vegades es traduiran les adreces de destinació? I les d'origen? Com

fa Skype, per exemple, per a connectar dos interlocutors que estan darerra de NAT?

Les limitacions (apart de les limitacions inherents de NAT) seràn que només els hosts d'una xarxa podran iniciar conexions amb els hosts de l'altra xarxa.
Les adreces de destinació seran traduides una vegada (al passar pel router DNAT)i les d'origen una vegada també (al passar per el SNAT).
Skype utilitzava (ja no utilitza P2P) NAT punchthrough per a conectar amb hosts a darrera de NAT, això funcionava a base d'enviar un paquet UDP, el qual generava una entrada a la taula de NAT que permetia a altres hosts d'internet accedir al host.

2. Imagina que construïm una internet paralel.la a la Internet, que utilitzés el seu mateix espaid'adreçament. Podríem utilitzar NAT per interconnectar-les, considerant que totes duessón arbitràriament grans? Es podria fer un túnel d'un host de la internet a un host dela Internet? Raona les teves respostes. Es possible superar la limitació d'adreces IPv4utilitzant NAT? Fins a quin punt és escalable aquesta solució?

No es podrien interconnectar amb NAT. Demostració per contraexemple: si són arbitrariment grans significa que podrien arribar a ser el màxim gran possibles i ocupar tot l'espai d'adreçament IP, de menera que, com totes les IPs estan ocupades, no hi hauria cap adreça lliure per a ser tulitzada pel router(s) que realitzessin NAT.
Realitzar un tunel si que seria viable. Aquest es podria realitzar conectant un host de un internet amb un host de l'altre internet físicament i establint un tunel entre aquests dos.
Es possible superar la limitació d'adreces IPv4 utilitzant NAT, això es pot aconseguir creant petites xarxes que estiguin conectades a internet a través d'un NAT de manera que l'adreça pública del NAT sigui l'única que estigui a internet. D'aquesta manera podem aconseguir conectar diversos hosts a internet utilitzant només una adreça IP.

3. Tenim una xarxa privada amb un servidor (192.168.2.2). El nostre router fa NAT (SNAT) ia més permet l'accés des d'Internet (els datagrames al port 22 seran re-encaminats al port 122 del servidor intern (DNAT)). Mostra el contingut de la taula NAT després que a) unclient s'hagi connectat des d'Internet. b) un altre client, amb el mateix port, s'hagi connec-tat des d'Internet. c) el primer client, des d'un port diferent, s'hagi tornat a connectar. Pertots els casos mostra també les connexions tal com les veuen client, servidor i router (fentun netstat, per exemple). Hi hauria algun problema si el servei ofert per aquest port 22 és SSH?

a)

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP client 1	Port client 1	192.168.2.2	122	TCP	22	P_NAT_1

Client: Conexió TCP entre `IP client 1:Port client 1` i `IP externa NAT:22`
Servidor: Conexió TCP entre `IP interna NAT:P_NAT_1` i `192.168.2.2:122`
NAT:

- Conexió TCP entre `IP client 1:Port client 1` i `IP externa NAT:22`
- Conexió TCP entre `IP interna NAT:P_NAT_1` i `192.168.2.2:122`

b)

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP client 1	Port client 1	192.168.2.2	122	TCP	22	P_NAT_1
IP client 2	Port client 2	192.168.2.2	122	TCP	22	P_NAT_2

Client: Conexió TCP entre `IP client 2:Port client 2` i `IP externa NAT:22`
Servidor: Conexió TCP entre `IP interna NAT:P_NAT_2` i `192.168.2.2:122`
NAT:

- Conexió TCP entre `IP client 2:Port client 2` i `IP externa NAT:22`
- Conexió TCP entre `IP interna NAT:P_NAT_2` i `192.168.2.2:122`

c)

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP client 1	Port client 1.a	192.168.2.2	122	TCP	22	P_NAT_1
IP client 2	Port client 2	192.168.2.2	122	TCP	22	P_NAT_2
IP client 1	Port client 1.b	192.168.2.2	122	TCP	22	P_NAT_3

Client: Conexió TCP entre `IP client 1:Port client 1.b` i `IP externa NAT:22`
Servidor: Conexió TCP entre `IP interna NAT:P_NAT_3` i `192.168.2.2:122`
NAT:

- Conexió TCP entre `IP client 1`:`Port client 1.b` i `IP externa NAT`:22
- Conexió TCP entre `IP interna NAT`:`P_NAT_3` i `192.168.2.2`:122

Nota: Com que en cada conexió el port del client es triat de forma aleatoria els ports utilitzats pel client 1 en les dos reconexions seràn molt probablement diferents.
P_NAT_1, 2 i 3 són també elegits de forma aleatoria per el router NAT

Hi hauria algun problema si el servei ofert per aquest port 22 és SSH?
No, hi hauria problemes si fossin conexions de més d'un host de la xarxa privada a un host extern però com en aquest cas són múltiples hosts externs connectats a un únic host de la xarxa privada no hi pot haver confusió.

4. En el mateix escenari del problema anterior, suposa que tenim dos hosts interns més amb aquests casos: a) tots dos hosts accedeixen al mateix servidor extern utilitzant ports locals diferents. b) igual que abans, però utilitzant el mateix port local. c) el mateix host intern, des de ports locals diferent, es connecta al mateix servidor, mateix port, d'Internet. Mostra la taula de NAT i les connexions a tots els hosts i al router en cadascun dels casos (el que mostraria un netstat, per exemple). Hi hauria algun problema si el servei extern és FTP en mode actiu?

a)

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP servidor extern	Port servei extern	IP host 1	Port host 1	TCP o UDP	Port NAT 1	Port servei extern
IP servidor extern	Port servei extern	IP host 2	Port host 2	TCP o UDP	Port NAT 2	Port servei extern

Host: Conexió TCP entre `IP host 1`:`Port host 1` i `IP servidor extern`:`Port servei extern`
Servidor: Conexió TCP entre `IP externa NAT`:`Port NAT 1` i `IP servidor extern`:`Port servei extern`
NAT:

- Conexió TCP entre `IP host 1`:`Port host 1` i `IP servidor extern`:`Port servei extern`
- Conexió TCP entre `IP externa NAT`:`Port NAT 1` i `IP servidor extern`:`Port servei extern`

Pel host 2 és quasi tot igual.

b)

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP servidor extern	Port servei extern	IP host 1	Port host 1	TCP o UDP	Port NAT 1	Port servei extern
IP servidor extern	Port servei extern	IP host 2	Port host 1	TCP o UDP	Port NAT 2	Port servei extern

Host: Conexió TCP entre `IP host 1`:`Port host 1` i `IP servidor extern`:`Port servei extern`
Servidor: Conexió TCP entre `IP externa NAT`:`Port NAT 1` i `IP servidor extern`:`Port servei extern`
NAT:

- Conexió TCP entre `IP host 1`:`Port host 1` i `IP servidor extern`:`Port servei extern`
- Conexió TCP entre `IP externa NAT`:`Port NAT 1` i `IP servidor extern`:`Port servei extern`

Aquestes connexions NAT no funcionaràn a no ser que el NAT utilitzi alguna tècnica complexa per l'enrutament, com, per exemple, alguna basada en els números de seqüencia, la qual pot fallar també.

c)

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP servidor extern	Port servei extern	IP host 1	Port host 1.a	TCP o UDP	Port NAT 1	Port servei extern
IP servidor extern	Port servei extern	IP host 1	Port host 1.b	TCP o UDP	Port NAT 2	Port servei extern

Host: Conexió TCP entre `IP host 1`:`Port host 1` i `IP servidor extern`:`Port servei extern`
Servidor: Conexió TCP entre `IP externa NAT`:`Port NAT 1` i `IP servidor extern`:`Port servei extern`
NAT:

- Conexió TCP entre `IP host 1`:`Port host 1` i `IP servidor extern`:`Port`

`servei extern`
- Conexió TCP entre `IP externa NAT:Port NAT 1` i `IP servidor extern:Port servei extern`

Hi hauria algun problema si el servei extern és FTP en mode actiu? Sí, que quan FTP transferís el nombre de port a través del qual vol fer la transferència el servidor s'intentaria conectar a aquest port del NAT, però el NAT refusaria la conexió perquè no tindria aquest port registrat a la seva taula.

5. Podríem connectar xarxes privades diferents (p.e. Ethernet i ATM) utilitzant els conceptes bàsics del VPN? I si fosin del mateix tipus? Existeix alguna proposta que faci alguna cosa semblant? Raona la resposta, i comenta les limitacions que tindria una xarxa d'aquest tipus.

Sí, hauriem d'operar el VPN sobre el layer de IP i ja està, llavors el layer físic que s'utilitzes a la xarxa seria irrellevant. Una proposta per fer això seria crea una nova interfície de xarxa que en comptes d'obtenir els paquets de la tarjeta de xarxa física els obtingues d'un tunel IP-en-IP per Internet. Les limitacions d'aquesta xarxa serien una latencia molt alta i un cos molt elevat per a fer operacions com un broadcast (faria falta enviar paquets a tots els hosts de la xarxa).

6. Suposa que els routers que han d'establir un túnel entre dues xarxes d'una mateixa VPNnomés tenen una adreça IP associada a la interfície externa i cap per la interna (la interfícieinterna no té associat ni tan se vol protocol IP). Creus que seria tècnicament possible lainterconnexió dels segments? En aquest cas, com serien els datagrames que circularien perInternet? Quines limitacions i avantatges tindria aquest esquema?

Sí que seria possible, ja que dins dels datagrames que viatgen per internet del tunel hi podem ficar dades arbitràries. Els datagrames que circularien per internet estarien format per un header IP que tingués com a destinació i origen les adreces IP externes dels routers que formen el tunel i, com a payload, tindria les dades binàries que s'envien per la xarxa (en qualsevol protocol en el que estiguin).
Limitacions: Els paquets no passarien per xarxes que realitzen anàlisis de paquets (per exemple les que només deixen passar TCP al port 80).
Avantatges: Podriem utilitzar protocols arbitraris dins de les nostres xarxes.

7. Tenim necessitat d'interconnectar la nostra VPN (de 200 hosts) a Internet (qualsevol hostintern ha de poder accedir-hi) per tal d'utilitzar un servei que utilitza un protocol quefunciona directament sobre IP. Aquest protocol té un identificador en les capçaleres pera

resoldre ambigüitats de fluxos d'informació a nivell d'aplicació. Com faries possibleaquest accés tenint en compte que estadísticament un 2% dels hosts voldran accedir almateix servidor d'Internet simultàniament?

Donat que no tinc suficient informació sobre l'identificador en les capçaleres del protocol com per saber si utilitzar-lo per NAT podria portar a conflictes, li assignaria al NAT unes $(0.02 \cdot 2 \cdot 200$ adreces externes diferents (per a cobrir el 2% de hosts que accedeixen al servidor i una mica més) i aplicaria NAT multi-adreça.

8. Seria possible combinar un esquema NAT per adreces amb un NAPT per tal d'augmentarel nombre de connexions simultànies entre la xarxa privada i Internet? En cas afirmatiu,quin serà el nombre màxim teòric de connexions tenint en compte els paràmetres de cadaesquema?

Sí que seria possible.

Esquema	Màximes conexions
NAPT	2^{16}
NAPT amb k adreces	$k \cdot 2^{16}$
NAT amb k adreces	k

9. Suposa que un router està fent NAPT bidireccional per a permetre l'accés a un host intern des d'Internet, a més de les connexions en sentit invers. Serà possible que aquest host es connecti amb si mateix utilitzant l'adreça i port públics que utilitzaran la resta de hosts a Internet? Raona la resposta i explica els detalls d'aquest cas sobre la taula de NAT.

Depen de la implementació de NAT però si no realitza cap comprovació si que seria possible. El que passaria seria:

1. Host envia datagrama a xarxa interna
2. NAT rep el datagrama i canvia les dades de Source per les seves, envia el datagrama per Internet
3. Un router d'internet rep el datagrama i l'enruta cap al NAT
4. NAT canvia les dades de Destination per la IP i port del host a la xarxa interna i les de Source per les del NAT a la xarxa interna
5. El paquet li arriva al host

Taula NAT:

IP extern	Port extern	IP interna	Port intern	Protocol	Port NAT extern	Port NAT intern
IP NAT	Port associat a host	IP host	Port host	TCP o UDP	Port NAT 1	Port associat a host
IP NAT	Port NAT 1	IP host	Port associat a host	TCP o UDP	Port NAT 1	Port NAT 2

10. Com podrem interconnectar dues VPNs totalment independents que comparteixen l'espaide direccionament? Quines limitacions tindira l'esquema que proposes? Explica les difer-ències que hi hauria en un cas com aquest el considerar un esquema de VPN d'etiquetes(com MPLS/VPN) respecte un més clàssic d'imbricació (túnels).

Per fer aquesta interconnexió simplement hem de realitzar traduccions entre espais de direccionament al NAT (una forma de fer això seria fer que el NAT traduís cada adreça a una diferent que no estigués a l'espai de direccionament utilitzat i que a la xarxa s'enrutissin totes aquestes noves adreces cap al NAT). La limitació d'aquesta esquema es que els hosts d'internet que tinguessin IPs en el rang de les noves adreces utilitzades no serien contactables des de la xarxa (ja que les seves adreces han estat 'segrestades' pel NAT). MPLS també funcionaria en aquest cas però un esquema basat en tunels no.

11. Podem tenir una intranet a n nivells (VPNs imbricades). En el nivell més extern, comafecta n en el càlcul del MTU del primer túnel? Quin és, si existeix, el màxim pràctic pera n si volem assegurar un mínim de 476 bytes per datagrama? Realitza els mateix càlculssi en comptes d'imbricació de túnels fessim NAT a n nivells.

Per a cada nivell hem d'afegir un header IP (ja que el paquet d'un nivell es encapsulat en un paquet IP), de manera que per cada nivell el MTU disminueix en 20 bytes.
MTU del primer Túnel = $MTU - 20 \cdot n$
Assumim que el MTU de les xarxes es de 1500 bytes (són xarxes Ethernet v2). Llavors el màxim per a n és: $1500 - 20 \cdot n \geq 476 \rightarrow n \leq \frac{476-1500}{-20} = 51.2$, màxim valor de n és 51.
Si utilitzem NAT no estem afegint nous headers, només modifiquem headers que ja existeixen, de forma que el MTU no depen del valor n. Això significa que n pot ser infinit i el MTU seguirà sent de 1500.

12. Un error de configuració en els routers d'una VPN ens porta a una situació límit. En lafigura les fletxes mostren les entrades de default dels routers, les interficies i0 connectena les xarxes físiques, i les tun0 són túnels. Explica que passa amb un datagrama queenvia 10.2.0.20 a 10.5.0.5 i quina serà la seva situació final. Tingues en compte la sevamida, fragmentació, adreces, ICMP, capa d'aplicacions, etc. Quin penses que és l'error deconfiguració? Com afectaria què els routers senars fessin NAT?

El datagrama passarà per tots els routers, serà enroutat per l'entrada de default i enviat al següent router fins a arribar a la xarxa original des d'on ha sigut enviat, moment en el que tornarà a ser enroutat pel primer router. El resultat d'això serà que el datagrama entrarà en un bucle de routers en el que es quedarà fins que el TTL arribi a 0 i s'envii un missatge ICMP a la xarxa d'origen.
No hi ha cap error de configuració, el problema es que la xarxa a la que pertany la IP a la qual s'està enviant el datagrama no existeix en aquesta sistema, de forma que es impossible entregar el datagrama.
NAT canviaria les adreces de source cada vegada que el datagrama passes per un router senar però com que l'adreça de destinació seguiría sent no assolible el problema persistiría.

Multicast

1. Un servidor, amb adreça IP 160.231.5.69, envia datagrames al grup de multicast 230.5.16.15.L'adreça MAC del servidor és 00:00:1B:3E:99:F0. Escriu les adreces IP i MAC d'origeni destinació dels datagrames que envia el servidor. Fes el mateix amb la resposta d'unmembre del grup.

Paquet del servidor:

```
Origen MAC: 00:00:1B:3E:99:F0
Destinació MAC: 01:00:5E:05:10:0F
Origen IP: 160.231.5.69
Destinació IP: 230.5.16.15
```

Resposta d'un membre:

```
Origen MAC: #MAC del membre
Destinació MAC: #MAC del router de la xarxa del membre
Origen IP: #IP del membre
Destinació IP: 160.231.5.69
```

2. A quin rang d'adreces IP multicast li correspon l'adreça Ethernet 01:00:5E:00:01:02? I a 01:00:5E:A5:CB:D2?

Ethernet	IPs (en binari)
01:00:5E:00:01:02	1110****.*0000000.00000001.00000010
01:00:5E:A5:CB:D2	1110****.*0100101.11001011.11010010

Els $*$ marquen bits que podrien ser tant zeros com uns.

3. A quants grups multicast pot afegir-se una interfície de xarxa sense repetir cap adreçaEthernet?

Com que la part de l'identificador de grup que es transfereix a la MAC té una mida de 23 bits, la solució és 2^{23} grups diferents.

4. Incrementa el broadcasting i multicasting el tràfic de la xarxa respecte a unicast? Justificala resposta.

Depèn del sistema físic sobre el que estigui montada la xarxa:

- En sistemes basats en circuits fer un broadcast implica establir una conexió amb cada un dels nodes i enviar un datagrama de manera que multicast i broadcast augmenten molt el tràfic.
- En Ethernet el tràfic no augmenta ja que per defecte tots els missatges físics arriben a tots els hosts de la xarxa, multicast/broadcast només determina quins hosts processaran el missatge.

5. Dibuixa un diagrama de temps on es vegin dos hosts diferents afegint-se a un grup, el router multicast fent el polling i els hosts deixant el grup.

Router → Adreça IP multicast de tots els hosts de la xarxa : Poll
Host A o B (el que s'uneixi abans o contesti més depressa) → Adreça IP del grup : Pertinença

Més tard:
Host A o B → Adreça IP del grup : LEAVE
Enviat immediatament després del segon LEAVE:
Router → Adreça IP multicast de tots els hosts de la xarxa : Poll
Ningú respón i el router elimina les dades que tenia sobre el grup i, en cas d'estar a RPM informa a altres routers de la extinció del grup a la seva xarxa.

6. Hi ha manera de fer multicasting IP entre xarxes diferents (p.e. a Internet) si no tenimrouters multicast a totes les xarxes intermitjes?

No, per que els routers de les xarxes intermitges no sabran com enrutar els paquets multicast.

7. Si el hardware de xarxa no suporta multicast, podem utilitzar multicast IP? Com? Quineslimitacions comportarà això?

En aquest cap podem enviar paquets multicast IP (ja que només requereixen canviar l'adreça IP de destinatari) però no en podem rebre (que requereix de hardware amb suport per multicast).

8. A IGMP, què passa si es perd una resposta (del polling) d'un host? I si es perd una petició d'enquesta?

Si es perd una resposta de polling poden passar dos coses:

- El host que ha enviat la resposta és l'únic host del grup que es troba a la xarxa. Llavors el servidor assumeix que com no ha contestat ningú es que no hi ha hosts subscrits a aquest grup a la xarxa i elimina les dades que té del grup, tancant-lo.
- Hi ha més hosts subscrits al grup multicast dins de la mateix xarxa. En aquest cas els altres hosts veuran que no s'ha respost el missatge i quan passi el seu delay de contestar (seleccionat aleatoriament) contestaran al router, obtenint el mateix comportament final que s'hagués obtingut si el paquet no s'hagués perdut.

Si es perd la petició d'enquesta els hosts no ho veuran i no contestaràn. El router, que no sap que el seu paquet s'ha perdut, considerarà la situació com que no hi ha cap host subscrit al grup en la seva xarxa i tancarà el grup.

Arch

1. Instal · la el navegador TOR (Tor Browser: https://www.torproject.org/download/download). Entra a la Deep Web connectant-te a l'adreça: http://hss3uro2hsxfogfq.onion/. Atenció! A la Deep Web et pots trobar amb tot tipus de drogues, armes i serveis il · legals.

- **Fes una cerca per a veure si tenen a la venda coca de Sant Joan. Com es garanteix l'anonimat d'aquesta cerca com a client? I com a servidor? Com es podria trencar l'anonimat?**
- **Quina adreça fas servir? A quin domini pertany?**

L'anonimat de client i servidor es garanteix gràcies a l'enrutament que es realitza dins de la xarxa tor (incloent la primera conexió entre client i servidor, que també es realitza a través d'un altre node i els circuits que es conecten a aquest). Com que totes les comunicacions passen a través de diversos nodes de la xarxa abans d'arribar al client o al servidor cap d'aquests dos està en contacte directe amb l'altre, de forma que els es impossible conèixer la identitat de l'altre, obtenint així l'anonimitat propia de Tor.

- L'adreça utilitzada és hss3uro2hsxfogfq.onion (com que l'enrutament de Tor es realitza sobre internet, el servidor també té una adreça IP, però ens es impossible conèixer-la). A Tor no hi ha dominis com a tal, hss3uro2hsxfogfq és part de la clau pública que utilitza el servidor del hidden service (aquest domini/adreça serveix tant per saber quins són els nodes a través dels quals es pot contactar amb el servidor com per autenticar el servidor).

L'anonimat es podria trencar si un atacant controlés els 3 nodes que s'han triat per enrutar els missatges dins de la xarxa tor, ja que llavors coneixeria tot el camí dels paquets. Igualment no podria conèixer el contingut dels paquets ja que aquests estan encriptats.
Una altra possibilitat que podria eliminar l'anonimat és l'ànalisis dels temps en que els paquets es reben in s'envien per nodes enrutadors dins de Tor, però aquest atac requereix recursos de nivell estatal.

2. Compara les xarxes AdHoc, MANET i DTN. Es podrien intercanviar els diferents protocols d'enrutament per els diferents tipus de xarxes? Inventa un protocol d'enrutament per xarxes DTN.

Comparació de Xarxes

- AdHoc: Es poden utilitzar els protocols d'enrutament utilitzats en MANET i DTN, encara que aquests resultaràn ineficients en xarxes AdHoc perquè estan disenyats per a xarxes amb canvis molt frequents les xarxes AdHoc solen ser molt més estàtiques que MANET o DTN.
- MANET: No es podrien aplicar els protocols d'enrutament utilitzats en AdHoc, ja que si utilitzem el pro-active les taules d'enrutament canvien tant ràpidament que quan arribin a un node ja estaran desactualitzades i si utilitzem enrutament reactive molt probablement els paquets no arribin al destinatari, ja que la xarxa no és totalment connexa (es possible que hi hagin parts de la xarxa aïllades durant un temps). Es poden aplicar els protocols d'enrutament de DTN sense cap problema.
- DTN: No es poden aplicar el protocols d'enrutament AdHoc per les raons explicades per MANET. Els protocols de MANET es poden aplicar, encara que es possible que hi hagi perdua de paquets perquè MANET no utilitza store-carry&forward.

Inventa un nou protocol per DTN

- Tots els nodes mantenen un historial de tot el seu recorregut (per on han anat)
- Quan un node A es troba amb un altre node B:
  - Li transmet tots les dades de recorreguts que té (el seu propi + altres recorreguts d'altres nodes que li han sigut transmesos abans)
  - Per cada paquet que té guardat:

    * Si NO es té informació del recorregut del detinatari del paquet, es sumen les distàncies entre tots els punts dels recorreguts d'A i B. Si aquesta suma es superior a una constant A li transmet el paquet a B. Aquest sistema permet determinar com de diferent l'area per la que es mou B es de la d'A i en cas de que ho sigui molt replica el paquet. Això es bo perquè aconseguim augmentar molt l'àrea per on es pot distribuir el paquet i trobar el destinari.
    * Si es té informació del recorregut del detinatari del paquet, es calcula la distància mínima entre el recorregut del node B i el recorregut del node destinari. En cas de que aquesta distància sigui inferior a la distància mínima entre el recorregut del node A i el recorregut del destinari, transmet el paquet a B.

El protocol es podria millorar tenint en compte els nodes amb els que es trobarà B i que també podrien enviar el missatge al destinatari, és a dir, fent la distància entre recorreguts transitiva.

IPv6

1. Compara les capçaleres de IP versió 4 i 6. Quins camps ja no hi són? Quins s'han mantingut? Quins han canviat de nom o han canviat la seva semàntica?

- TTL passa a ser Hop Limit
- Identification s'elimina perquè ara la fragmentació es realitza en una extensió
- ToS passa a ser Traffic Class i Flow Label (headers utilitzats per classificar tràfic)
- S'elimina Header Length perquè ara la capçelera és de mida fixa
- Protocol s'elimina
- S'elimina el camp de flags i les opcions de IPv4 i es substitueix per un sistema que permet afegir headers opcionals on cadasqun d'aquests determina el següent (mitjançant Next Header).
- S'elimina checksum

2. El checksum ja no hi és en la capçalera d'IPv6. Per què penses que l'han tret? Pot afectar això a la integritat dels datagrames (i.e. és IPv4 més segur)?

Per què penses que l'han tret? Per a evitar que els routers hagin de recalcular la checksum de cada paquet al reduir el TTL.

Pot afectar això a la integritat dels datagrames (i.e. és IPv4 més segur)? No, perquè les comprovacions de la integritat dels datagrames es realitzen en altres nivells, com per exemple en el transport (TCP o UDP), de

manera que les comprovacions d'integritat es realitzen igualment. Mentres a IPv4 era possible no utilitzar checksum en UDP en IPv6 és obligatori per aquesta raó.

3. En IPv6 es multiplica per 2 la longitud de la capçalera mínima (sense opcions) respecte a IPv4, però el temps de processament és molt menor. Com explicaries aquesta aparent paradoxa?

Passa això per 2 raons principals:

- Els routers no poden fragmentar de manera que tot el processament utilitzat en fragmentació s'elimina
- No hi ha checksum a nivell de IP de manera que s'elimina tot el processament associat a computar noves checksums per cada paquet (requerides per la modificació del TTL)

4. Considera un host que pren una adreça link-local codificant la seva adreça Ethernet de 48bits juntament amb el prefix link-local estàndard. Podrien utilitzar ja aquesta adreça a laInternet global? Per què? Serà única aquesta adreça?

No, l'adreça obtinguda a través de la MAC no serveix per l'internet global perquè, mentres l'adreça seria probablement única a tot internet (es possible que un altre node agafi la mateixa adreça però la probabilitat de que això passi es molt baixa) seria impossible a internet enrutar correctament els paquets dirigits a aquesta adreça, ja que fer això requeriría que es tinguessi en compte aquesta adreça a les taules d'enrutament de tots els routers del món.

5. IPv6 introdueix el concepte de fluxos. Explica per a que serveixen i si en IPv4 tenien algun equivalent.

Són simplement una altra forma de classificar el trafic, permetent que tràfic que requereix una latencia menor o pertany a aplicacions més importants tingui preferència sobre altres tipus de tràfic. L'equivalent a IPv4 és el camp ToS (Type of Service).

6. La capçalera IPv6 pot no portar l'identificador del protocol receptor de dades. Com és possible doncs l'arribada concreta dels datagrames als protocols finals?

És possible perquè l'identificador del protocol està contingut al camp Next Header de l'última extensió IPV6. Això significa que per obtenir l'identificador de protocol només s'ha de processar els headers d'extensió fins a arribar a l'últim.

7. Suposa que tenim dos hosts, A (111.1.1.111) i B (55F1:1F55:1221::2112), que volen comunicar-se. A té una pila dual IPv4/IPv6, i està situat en una xarxa IPv4. B només té IPv6 i està en una xarxa IPv6. El router R està connectat a totes dues xarxes i permet l'establiment de túnels. Disenya un esquema que permeti l'intercanvi de datagrames entreA i B. Mostra els detalls d'un datargama circulant d'A a B i d'un altre en sentit contrari.

Es pot solucionar aquest problema establint un tunel IPv6-over-IPv4 a la xarxa de A entre A i R, el qual actuarà de la següent forma:
A envia a B:

1. A crea un paquet IPv6 de A a B i l'empaqueta dins d'un paquet IPv4 de A a R, el qual envia.
2. R rep el paquet i el desempaqueta, obtenint el paquet IPv6 que va de A a B, el qual envia a B
3. B rep el paquet IPv6 de A a B

Paquet de A a B a la xarxa de A:

Header IPv4 (A->R)	Header IPv6 (A->B)	Payload

Paquet de A a B a la xarxa de B:

Header IPv6 (A->B)	Payload

B envia a A:

1. B crea un paquet IPv6 de B a A i l'envia
2. R rep el paquet i l'empaqueta dins d'un paquet IPv4 de R a A. Envia el paquet IPv4
3. A rep el paquet IPv4 de R a A, el desempaqueta i obté el paquet IPv6 de B a A

Paquet de B a A a la xarxa de A:

Header IPv4 (R->A)	Header IPv6 (B->A)	Payload

Paquet de A a B a la xarxa de B:

Header IPv6 (B->A)	Payload

8. Creus que totes les novetats introduïdes a IPv6 poden afectar el throughput de TCP? Justifica la teva resposta, tenint en compte els diferents tipus d'escenari LAN, WAN, LFN,wireless, ...

Si, el throughtput de TCP es pot millorar ja que ara els routers que enrutin els missatges no hauran d'utilitzar tant poder de processament, evitant així que arribin a la seva capacitat de processament i tinguin que dropejar paquets, la qual cosa empitjora molt el throughput de TCP (a no ser que tingui una finestra molt gran).

9. Si canviem la nostra xarxa de IP v4 a v6, haurem de canviar els commutadors (switchs) si no suporten aquesta nova versió del protocol? Afecta el fet de tenir VLANs aquesta decisió?

Depen:

- Si són switches que operen al layer 2 i 1 no fa faltan canviar-los.
- Si els switches arriben a operar al layer 3 si que fa falta canviar-los.

Si tenim una LAN els switches necessariament han d'operar a layer 3 de manera que s'hauran de canviar.

10. Serà possible tenir una VPN on circulin datagrames de totes dues versions de IP? En cas negatiu explica-ho. En cas positiu comenta els detalls sobre l'encaminat i tipus de túnels.

Sí que és possible, un simple tunel IP-over-IP podria transportar datagrames IPv6 i IPv4 ja que:

- A internet el tipus de datagrames que hi hagin dins del tunel són irrellevants, ja que els routers d'internet només veuen el header IP que indica els dos endpoints del túnel.
- Els endpoints del túnel poden empaquetar dades arbitraries dins del datagrama que s'envia pel túnel, així que no hi ha cap problema en empaquetar IPv4 o IPv6.

11. Podem afegir tantes extensions de capçalera com vulguem, o hi ha un límit? Donat que les extensions formen una llista encadenada, seria possible crear un cicle per a fer malfuncionar els routers?

Hi ha un RFC que diu que totes les extensions de capçalera han d'anar dins del primer fragment d'un paquet (abans no era així però a partir d'aquest RFC si, el qual es va crear per solucionar problemes de seguretat), i el tamany dels fragments d'un paquet està limitat de manera que el nombre de extensions que poden haver-hi en un paquet (ja que no hi ha cap extensió que tinguina mida nula).
No es possible crear un cicle ja que Next Header només descriu quin és el següent

header, no apunta a cap lloc. Això significa que es impossible que el processament d'aquests headers sempre avançarà i serà O(n) on n és el nombre d'extensions.

12. L'extensió de fragmentació permet fragmentar extensions? És a dir, permet realment fragmentar datagrames o payloads de datagrames?

Només permet fragmentar payloads de datagrames. En les primeres especificacions de IPv6 es podien fragmentar datagrames (incloent extensions) però es va deprecar aquest comportament per problemes de seguretat.

IPSec

1. En quins protocols es basa IPSec?

L'arquitectura està parcialment inspirada per SSL i TSL (encara que IPsec s'aplica a un layer diferent que aquests).
L'encriptació i autentificació utilitzada en IPsec està basada en protocols críptogràfics símetrics (per l'encriptació) i asímetrics (utilitzats en l'intercanvi Diffie-Hellman i l'autentificació).

2. Suposa que un datagrama IP entra en un túnel IPSec. Escriu les seves capçaleres si s'està utilitzant:

a) Només autenticació (AH)
b) Autenticació i xifrat (AH+ESP)
c) Només xifrat (ESP)

AH:

Capçalera IP	Capçalera AH	Contingut

AH+ESP:

Capçalera IP	Capçalera AH	Capçalera ESP	Contingut	Cua ESP

ESP:

Capçalera IP	Capçalera ESP	Contingut	Cua ESP

3. De quina manera es preserva l'identificador del protocol en el payload del datagrama quan afegim les capçaleres d'AH i d'ESP?

L'identificador de protocol original es posa dins del camp `Next Header`.

4. Per a què serveix el camp d'índex de paràmetres de seguretat a les capçaleres d'IP Sec?

Per a saber quina es la security association que s'ha d'utilitzar per desencriptar i/o autenticar el paquet.

5. En quines situacions utilitzaries SSL i en quines IP Sec? Penses que el servei de WWW del'Autònoma podria oferir-se amb IP Sec? Comenta totes les implicacions que comportaria.

Utilitzaria SSL quan volgués autentificar i encriptar el contingut dels paquets enviats a internet enviats o rebuts per qualsevol altre host d'internet. En canvi, utilitzaria IPSec quan volgués encriptar i autentificar els paquets sencers (no només el contigut) dels paquets enviats entre hosts que controlés jo (perquè hauria de crear les SA necessàries).
El servei de l'Autònoma no es podria oferir un servei web amb IPSec perquè això requeriria que tots els seus usuaris haguessin definit previament les security associations necessàries per poder establir comunicació IPSec.

6. Quines implicacions funcionals té el blocat de datagrames efectuat per un firewall en escenaris on tinguem: a) Multicast, b) VPN/NAT, c) IP Sec.

a) Els firewalls no bloquejen multicast.
b) Els NAT solen aplicar un firewall íntrinsec al ser SNAT (quasi tots els NAT a internet són SNAT) el qual bloqueja totes les conexions que no siguin iniciades per a hosts de dins de la xarxa.
c) Molts firewalls només deixen passar certs protocols amb certs ports concrets (especialment molt firewalls només deixen TCP amb els ports 80 i 443 per tal de només deixar passar comunicacions web) de manera que els paquets IPsec quedarien bloquejats pel firewall.