

## 4. Ikasgairako ariketak

- 1** (T.14) Ba al dago TCP konexio bat baino gehiago ezartzea portu berean eta konputagailu berean?
- 2** Zer gertatuko da bezero batek konexio bat irekitzeko procedura hasten badu, eta, lehenagoko SYN segmentua bidali eta gero uzten du procedura? Eta gauza bera egiten badue bezero batzuek, aldi berean?

- 3** Ondoko zein aplikazioentzat ez da egoia IP-ren best effort zerbitzua?

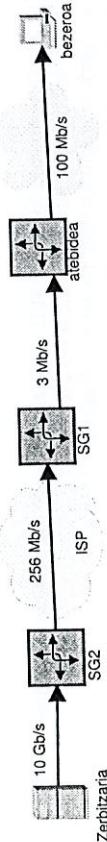
- VoIP aplikazioak (IP bidezko ahotsa).
- Web.
- Erreaktore nuklear baterako suteak atzemateko telealarma.
- Posta elektronikoa.
- TVoIP (IP bidezko telebista).
- Bideratzaile baten ilaren tamainaren urruneko monitorizazioa.

- 4** Sortzen ari zaren aplikazio batean, bezeroak fixtagai bat jaisten du zerbitzaritik noizean behin. Zein garraio-zerbitzua erabiliko zen zuke hauetako kasu bakoitzean? Azaldu erantzunak.

- Fixtagai 500 bytretxo da.
- Fixtagai 500 MiB-ekoia da.
- Fixtagai edozein tamainakoa izan daiteke.

- 5** Demagun irudikoz erakusten den datuak ari garela etengabe jaisten, UDP erabiliz. Biren artean hiru bideratzaila daude: bezeroaren atebidea, eta ISPren bi sargune, bata bezeroari sarrera emanen diona (SG1), eta bestea zerbitzariari (SG2). Demagun zerbitzaria 10 Gb/s abiaduraren ari dela transmitzen.

- Azaldu zergatik sortuko den buaxadura.
- Zein ekipotan hasiko dira datagramak galtzen? Suposatu bideratzaile guztiek erabilizentzutea tamaina bereko bufferrak.
- Beste ekipoaren batetan sortutu al da buxadura?
- TCP erabiliz, gero, ekidituko al dugu buxadura sortzea?



Ondoko ariketak guztiek gai bera ('TCP abiadura') jorratzen dute. Hietean, kalkuluak egiterakoan, kontrolerako bidaiketetarako (goiburukoa, ACK bidaletak...) erabilitako denbora zero dela hartu.

- 6** Bi konputagailu artean 5 MiB-ekoak fixtagai bat bidali dugu 45 segundutan. Bi konputagailuek duten sare konexioa 10 Mb/s-koa dela jakinda, (a) zein da lortutako benetako abiadura? (b) Zergatik dago alde hori abiadura fisikoa eta TCP-k lortutako abiadura artean?

- 7** (12mai) Bi konputagailu artean 5 MiB-ekoak fixtagai bat bidali dugu, ondoko baldintzak betetzen dituen TCP konexio bat erabiliz:

- Igorlekak eta hartzaleak erabilitzenten transmisioko abiadura: 1 Mb/s

- Hartzalearen bufferra: 32 kB.

Deskarga egiteko hartzutako denbora 46 segundo izaten da.

- Ondoko galdera hauk erantzun:
- Zer iruditzen zaizu deskarga egiteko emandako denbora?
  - Aztertu denbora hori jaisteko aukera.

- 8** (12eka) Demagun web zerbitzari batetik deskargatu behar dugula fixtagai bat. Demagun gure arakatzaileak TCP konexio bakarra ezarri duela zerbitzariarekin horretarako.

- A) Kalkuluatu zein izango den deskarga hori egitean lor dezakegun gehienezko abiadura, ondokoak kontuan hartuta:

- VoIP aplikazio (IP bidezko ahotsa).
- Web.
- Erreaktore nuklear baterako suteak atzemateko telealarma.
- Posta elektronikoa.
- TVoIP (IP bidezko telebista).
- Bideratzaile baten ilaren tamainaren urruneko monitorizazioa.

- 9** (12eka) Demagun web zerbitzari batetik deskargatu behar dugula fixtagai bat. Demagun gure arakatzaileak TCP konexio bakarra ezarri duela zerbitzariarekin horretarako.
- A) Kalkuluatu zein izango den deskarga hori egitean lor dezakegun gehienezko abiadura, ondokoak kontuan hartuta:

- Arakatzaileak emandako kreditua 64 KiB da konexio osoan zehar.
- Zerbitzaria baita arakatzailearen konputagailua ere, Gigabit Ethernet sareetan dande konektaturik (1 Gb/s) abiadura fisikoa bi muturretan, alegia.
- RTTaren balioa, konexio osoan zehar, ez da inoiz izango 50 ms baino txikiagoa.

- 10** Azaldu zein baldintza bete behar diren kalkuluatzunetan gehienezko abiadura hori lortu ahal izateko.

- 11** TCP konexio batean zein den lortutako abiadura mugatzan duen parametroa jakiteko algoritmoa idatziz sasikodea erabiliz.

Sarrera honako aldagaiei hauiek izango dira:

- Konexioko transmisio-abiadura fisikoa (F).
- RTTA (RTT). Ez da aldatzen konexioan zehar.
- Konexioko kreditua (K). Ez da aldatzen konexioan zehar.
- Lortutako abiadura (A).

Ireerra string motako MUGA izenezko aldagai izango da. Algoritmoeak lortutako abiadura mugatzan duen parametroaren izena esleitu behar dio aldagai honi.

- 12** TCP erabilitzenten aplikazio banatu baten bezero eta zerbitzariaren artean 100 ms-ko RTTA baldin badago, eta hartzalearen bufferra 32 KiB-koak baldin bada (eta, berez, hori da izango dugun gehienezko kreditua), zein da aplikazio horretxez erabilitako TCP konexio batean lor daitekeen abiadurari handiena, buxadurari ez dagoeila suposatua?

- 13** Aplikazio banatu baten bezeroa eta zerbitzaria FastEthernet (100 Mb/s-ko txartelak) switch (edo kommutagailua) batera lotuta daude. Bezeroak fixtagaiak jaisteen ditu zerbitzarien TCP erabiliz. TCP konexio horietan 1 ms-ko RTTA atzemana dugu etengabe (ez da harritzeko horrenbesteko balio baxua, bi aplikazio entitateek sare-segmentu berean egonda). Hartzalearen bufferra 32 KiB-koak baldin bada (eta, berez, hori da dugun krediturik handiena), zein da fixtagai jaistean lor dezakegan abiadurari handiena? Bidean bideratzaileek ez dagoeila ohartu, eta, berez, kongestiorik ez.

- 14** Ariketa honen aldaera bat (13-5): Aplikazio batek 100 GiB-eko disko bat deskargatu behar du konputagailu batetik bestera, sarean zehar.

- a) Zein garraio-mailako zerbitzu erabili beharko du horretarako? Zergatik?

- b) Zein da aplikazioak lor dezakeen abiadurari handiena, bi konputagailuak FastEthernet

- kommutagailu berari lotura badaude?
- c) Eta bi konputagailuak Interneten badaude, biren arteko RTTa 100 ms izanda, eta biren arteko bide osoan 100 Mb/s-ko abiadura bermatua izank?
- Erabilgariak izan daitezkeen beste danuak:
- Hartzeko bufferren tamaina 80 KIB da (Linux sistemeten ohikoa).
  - Sare lokal baten RTTa ez du inoiz 1 ms gainditzen.

- [12]** (1:35) Zunz optikoaren abiadura maximo teorikoa  $75 \text{ Tb/s}$  ( $1 \text{ T} = 10^{12}$ ) da. Zenbat izan behar du RTT maximoa abiadura hori ondo aprobaezteko, kongestiorik ez dagoela kontuan harturik? Lagunza: gogoratu TCP konexio batean erabili daitekeen krediturik handiena, eskala-faktorearabil gabe, 64 KIB dela.

- [13]** TCP konexio baten bidezko transmisió bat 1 Gb/s-ko abiaduran eta 20 ms-ko atzerapenarekin (RTT) egiten ari da. Lehoaren tamaina maximoa da (eskala-faktorerik gabe). Zein da transmisióaren eraginkortasuna? Eta benetako abiadura? Kalkuluak egingean, ez hartu kontuan goiburuikoen bitak ezta ACK transmititzeko denbora ere.
- [14]** (990) Bi lagun artean negozio txiki bat duzue, non jendeari unean berean Internetetik lortutako informazioa ematen zaio. Horretarako 2 Mb/s jaisteko abiadura duen ADSL konexio bat duzue. Zerbaitzu on bat eskaintzeko garrantzi handia du zerbaitzari batean dauden fixategiak ekartzeko behar den denbora. Gaur egun, 570KIB fixategi bat ekartzeko 3 minuto baino gehiago behar diuzu, eta honek zure lankideka harritzen du, bera segundo batzuk beharko zegelako (570KIB / 2 Mb/s-tan ekartzeko behar den denbora, alegia).

- A) Hainbeste denbora behar izateko arrazoi posibleak zerrendatu, transmisió errereak eta web zerbitzariaren gainzama batzertuz.

- Aipatu dituzun arrazoien artean zein den zuzena azterten hasi zara. Ping bat eginet, web zerbitzari batekiko RTTa 2 segunduko dela ikusten dugu, eta, sniffer bat erabiliz, fixategiak ekartzeko sortutako TCP konexioari buruzko ondorengo datuak lortzen diuzu:
- Harutzaleak igorleari emanako kreditua ez da inoiz aldatzan eta beti 5840 byrekoa da.
  - Ez dura birtransmisorik suertzen.

- B) Datu horiekin, fixategia 3 minuto baino laburragoan ezin dela ekarri erakutsi izaozou zure lankideari. Kalkulatuk egiterakoan, ez harru kontuan TCP-ko konexioa iekiteeari eta piloketa kontrolari dagozkion denbora-galerak.

- [15]** (01EK) Bedi TCP implementazio bat, gehienez, 32KB-ko sarrerako bufferra erabilten duena. Demagun zerbaitzari bat, Fast Ethernet sare batean konektatutik. Zein da zerbaitzari hori eta aipatutako TCP implementazioa erabilten duen makina baten arteko atzerapenik handiena bufferren tamainaren eraginez etengabeko transmisióa mantenzeko? Ez harru kontuan goiburuikoak kalkuluak egingaen. Denagun bideratzaleek 5 ms-ko atzerapena sortzen dutela, bataz bestean. Horrela bida, zerbat bideratzale egoen datezko zerbaitzari baten eta gure makinen arteko bidean TCP konexio batean etenaldirik egon ez dadin? (Ez harru kontuan senialea hedatzeko atzerapena).

- [16]** Egin ezazu grafiko bat, RTTren balioak egonkorria dagoen TCP konexio baten abiaduran duen eragina aztertzeko, ondoko baldintzapean:
- Transmisió abiadura: 10 Mb/s
  - Buxkadura sortzen duen transmisió lehoaren balioa: 16 KiB
  - Kreditua: 12 KiB

- [17]** Egin ezazu grafiko bat, transmisió abiadurak egonkorria dagoen TCP konexio baten

- abiaduran duen ergina aztertzeko, ondoko baldintzapetan:
- Buxkadura arinak besterik ez dira sortzen.
  - Transmititu behar diren fixategiak ez dira txikiak (100 KIB edo gehiago).
  - Buxkadura sortzen duen transmisió lehoaren balioa: 8KiB.
  - Kreditua: 12 KiB
  - RTT = 100 ms.

- [18]** Kalkula exazu Web orri baten 64 KiB bidalzezko behar den denbora, horretarako ireki den TCP konexioak ondoko exaugariak baldin baditu:
- Zerbaitzariak erabilitako sarea Fast Ethernet bat da.
  - Kreditua (ez da aldatzen): 8 KiB.
  - RTT = 125 ms (ez da aldatzen).
  - Buxkadurarik ez da sortuko.
  - Goiburuoko bit-kopuna arbuigarria da (ez hartu kontuan kalkuluetarako).
  - TCP segmentuak prozesatzeko denbora ere arbuigarria da.
  - Ez hartu kontuan zure kalkuluetarako konexioaren hasierako slow-start mekanismoaren eragina.

- [19]** Demagun web zerbaitzari batetik deskargatu behar dugula fixategi bat. Demagun gure arakatzaileak TCP konexio bakarra ezarriko duela zerbaitzaretak horretarako. Eta demagun ondoko hauek direla konexio horren baldintzak:
- Kongestiorik ez, errorerik ez: ez dago birtransmisorik. Arakatzaileak emandako kreditua 16 KiB da konexio osoan zehar. Ez hartu kontuan kongestioa kontrolatzeko beste mekanismorik. Bidali behar den informazio kopurua: 1 000 000 bit. RTTaren balioa, konexio osoan zehar: 0,1 s. Arakatzaileak GET komandoa bidalko du konexioa ezartzeko azken bidalketarekin batera. Zerbaitzariak konexioa amaitzeko eskatuko du bidaltako azken datuekin batera. Baldintza horietan, kalkulatu arakatzaileak fixategia jaioteko erabilitako denboraren zein eluneko suposatzen duen TCP konexioa ezartzeari eta analizeak.

- [20]** (08ot) Bi konputagailu artean MiB batzutako fixategi bat bidaltzen da egunero, ondoko baldintzak betetzen dituen TCP konexio bat erabiliz:
- Igorleak erabilizten duen transmisió abiadura: 10 Mb/s
  - RTT = 80 ms (ez da aldatzen).
  - Kreditua: 10000 B (ez da aldatzen).
  - 8000 B-eko transmisió lehoia erabiliztera ailegalzen denean, buxadura arina sortzen da bidean dagoen bideratzalle batean.
  - Bideko linea eta bideratzaleetan transferentzia honi dagokion trafikoa besterik ez dago.
  - Kontrolerako segmentuak eta goiburuikoak bidaltzeko denbora arbuigarria da.
- Ondoko gaidera hauek erantzun:
- Zein da TCP mailako transmisió abiadura maximoa.
  - Zer izango dugu hobe, igorlearen transmisió abiadura 100 Mb/s-ra igotzea, edo buxadura paitatzen duen bideratzalea 20000 B-eko lehoia arte kongestionatzen ez den beste bideratzale potenteari batekin ordetzatzeari?

- [21]** (08ots) Konputagailu batek beste batzuk egunero bidaltzen dio 100 KiB fixategi bat, TCP konexio bat erabiliz. Ondoko baldintza hauetik kontuan hartuta:

- Fixtagiegaren igorleak erabilitako transmisió-abiadura: 10 Mb/s.  
 • RTT=5 ms (konstantea).

Hartzaleak baimendutako kreditua: 8 KiB (konstantea).

- Bi konputagailuen artean dagoen bideratzaile baten buadxadura sortzen da igorlearen lehoak 7 KiB hartzentz duean.

Kontrol mezuak eta goiburukoak transmititzeko denbora arbuiagarria da.

- Erantzun ondoko galdera hauek:
- a) Zenbat denbora beharko da fixtagenia transmititzeko?
- b) Nolako ergaina izango du ondoko aldaketa bakoitzak kalkulaturako denboran?

- b.1 Igorlearen transmitizioa denbora bikoiztu.
- b.2 Hartzaleak ematen duen kreditua aldatu.
- b.3 Buxadxadura sortzen duen bideratzailea aldatu. 12 KiB-ko lehoia izan arte ez kongestionatzeko.

**22** (07ots) 500 GB disk baten backup egin behar dugu. Backup hori aplikazio batek egindo du automatikoki, diskgoaren edukiaik beste galu batzuetara kopiatuz sare lokal baten bidez. Kopia horri egiteko dugun denbora gehienez 2 ordu denez, sare lokal azkar bat dugu: 10GbE bat (10 Gb/s-tan transmititzen duen Ethernet berisioa). Backup egin behar duen aplikazioak sarearen abiadura fisikoan transmitituko balu, 7 minuto baino zeintxobait gehiago besterik ez, genuke behar diskorean kopia osca egiteko. Hala ere, aplikazioa abiatu eta bi ordu pasata, kopia ez da oraindik bukatu. Arazoa aztertzen hasi zara, eta ondoko informazioa lortu duzu:

- Sarearen abiadura jaitzi dezakeen inongo arazorik (tentreak, buxdurak ...) ez dago.
- Kopia egiten duen aplikazioak TCP konexio bat erabilten du horretarako.
- Kopia egiten duen aplikazioak TCP entitateak 16.384 byteko (16 KiB) hartzeko.
- Konputagailu hartzalearen TCP entitateak 16.384 byteko (16 KiB) hartzeko, bufferra (beste aldeari emango dion kreditua) erabilten du TCP konexio barritzeko, besterik ezean.
- Igorlearen eta hartzalearen konputagailuetan informazioa prozesatzeko denbora eta goiburukoak transmititzeko denbora arbuiagarriak dira.
- Igorlearen konputagailuaren eta hartzalearen konputagailuaren artean dagoen RTT-a 5 ms-koa da. Balio hori ez da aldatzen.

Hori gartzia kontuan harturik ondokoak egin:

- A) Kalkulatu ezazu zenbat denbora beharko da disco osoaren kopia egiteko, konexioa ezartzeko eta amaitzeako denbora, slow-start algoritmoaren eragina kontuan hartu gabe. B) Adierazi ezazu zer egino zenukeen diskoren kopia ezarritako denboran egin ahal izateko. Oharra: TCP erabilii behar da.

**23** Etxean Internetik egiten ditugun deskargatzen 300 Kbps abiadura neutrut dugu, nahiz eta gure konexioa 3 Mb/s izan. Lortutako abiadura hainbeste mugatzen duen faktorea identifikatzeko asmoz, ondoko datu hauek lortu ditugu:

- Deskargak TCP erabilii egiten dira, eta gure konputagailuko TCP implementazioak 8 KB-eko kreditua esleitzen dio konexio bat.
  - Ping erabiliz, zerbitzarietatik gure konputagailura 80 ms-ko batez besteko RTTa neurut dugu.
  - Atxizten ditugun zerbitzariak Ethernet sareetan kokatzen dira, eta informazioa banatzea besterik ez due egiten.
- Datu horiekin guztielkin, zerik eragozten digu deskargatzeko abiadura handiagoa lortzea, zerbitzariaren konexioko abiadurak, TCP konexioen kredituak, ala sarean suertatuko kongestioek? Fixtagieki deskargatzeko denbora ahal den gehiena murritzeko, zer izango da hobe, gure konexioaren abiadura bikoiztu 6 Mb/s-raino, edo ISP aldatzea?

#### Aldarea (10ka)

Interneten kokututako zerbitzari baten eta gure sarean kokututako bezero baten arteko TCP bidezko datu-korreonte bat sortzen duen aplikazio bat ari gara sortzen. Korronte horretan lortu dugun benetako abiadura 1 Mb/s da, baina ez da nahiko gure aplikazioa ondo ibilzeko. Gaia aztertuz, ondoko datu hauek lortu ditugu:

- Zerbitzariaren sare-konexioko abiadura fisikoak 1 Gbps da.
- Bezeroak zerbitzariari emandako kreditua 16 KiB da, eta konstantea da.
- Zerbitzari eta bezeroaren arteko RTTa egonkorra da, 50 ms inguruan.

Egin:

1. Abiadura handiagoa lortzea eragozten duen arazoa identifikatu.
2. Dituengu datuak besterik ez kontuan hartuta, baloratu ea bezeroaren sareak duen ISPA aldatzaera erabaki zuzena den, lortzen ari garen abiadura hobetzeko asmoa dela.
3. Demagun TCPren ordez UDPren erabilzea badagoela. Erabaki zuzena izango al da UDP erabilzeta lortzen ari garen abiadura hobetzearren?

**24** Gure sarean Internetik egindako deskargatzen 0,5 Mb/s abiadura neutrut dugu. Lortutako abiadura hainbeste mugatzen duen faktorea identifikatzeko asmoz, ondoko datu hauek lortu ditugu:

- Deskargak TCP erabiliz egiten dira, eta gure konputagailuko TCP implementazioak 8 KB-eko kreditua esleitzen dio konexio bat.
- Atxizten ditugun zerbitzariekin Interneteko lotura onak dituzte, eta informazioa banatzea besterik ez due egin.
- Gure konputagailuen era zerbitzarien arteko batez besteko RTTa 50 ms da. Traceroute erabiliz, denbora horren osagaiak aztertu egin ditugu, eta honako hau aurkitu dugu: zerbitzarietatik gure ISP-raino doan bidea 5 ms ematen duen datagrammek, 40 ms gure ISPren sareak zeharkatzeko, eta beste 5 ms gure sareak zeharkatzeko gure konputagailuera traino allegatu arte.

Zer egoingoz zenuke deskargatzeko batez besteko RTTa suposu dezagun ISP aldatzea erabakitzuen duzula, eta ISP berriaren batez besteko RTTa Suposu dezagun ISP aldatzea erabakitzuen duzula, eta ISP berriaren batez besteko RTTa 80 ms-raino igotzen dela. Hala ere, deskargatzeko abiadura ere handitzen bada, esperozko da arte. Nola argituko duzu ixurazko paradoxa hau (RTTa handitzen bada, esperozko da abiadura hobetzeko, eta ez handitzea)? Zein neurri hartuko zenuke orain abiadura hobetzeko?

**25** (09ots) ISP batetik bidez konexiotutako bi sareen arteko back-up egiteko aplikazio bat instalatu dugu. Bi sareen ISP-arekiko konexioak 1 Mb/s abiadurakoak dira, bi noranzkoetan (igotzeko eta jaisteko). Egorea horretan backup egiteko denbora asko irudizen zaigunez, lortzen ari garen benetako abiadura neutrut dugu. Abiadura hori 1 Mb/s denbora aurkitu dugu. Gainera, bi sareen artean ping eginez, RTTa 100 ms dela neurri dugu. Backup-ak egiteko denbora murritzeko nahiak, ISPrekiko bi konektioen kontratatuak. Horregatik, berrirro neurri dugu benetako abiadura eta 128 Mb/s besterik ez dela aurkitu dugu. RTTa ere neurri dugu, eta 100 ms dira oraindik ere. ISP-k iniziala egiten dugu gaudenean, ISP aldatzea erabaki dugu. Beste batekin kontratatu ditugu 3 Mb/s denborak lortzen ditugu backup-ean. Berrirro neurri dugu benetako abiadura eta RTTa, eta 1 Mb/s eta 128 ms direla aurkitu dugu.

Hirugarren ISP batengana jo dugu, eta berriro 3 Mb/s abiadura bi konexioak kontratatu ditugu. Baina benetako abiadura eta RTTa neurrtuta, 16 Mb/s eta 80 ms direla topatu dugu.

A) Azaldu zer geratzen ari den: zergatik ez duzu lortzen kontrataturako abiadura? Zure

azalpena behar diren kalkuluetan oinarritu.

Arazoaren jatorria dakinula, 20 ms-ko RTT-a bermatzen dizun ISP berri bat kontratu ditziozu 3 Mb/s-ko bi konexioak.

B) Zein da lortzea espero duzun benetako abiadura?

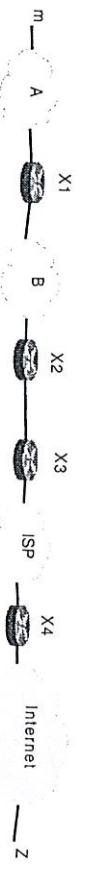
Baina backup egiten, 15 Mb/s benetako abiadura neurru duzu, nahiz eta RTT-a 20 ms izan. B) atala ondo etantzun baduzu, abiadura hori espero zenuena ez dela ikusiko duzu.

C) Zergatik ez dizul lortu espero zen benetako abiadura?

**23)** (09eka) Bitez inidiko S1 eta S2 sareak. Biak Gigabit Ethernet segmentuak dira, bata bestetik oso urru kokatuta, eta biak ISP hornitzalearen bidez lotuta. S1 sarean dagoen Z zerbitzaritik oso fixategi handiko deskargak egiten ditugu. S2 sarean dagoen komputagailura, ISParrekiko bi konexioen abiadura 1 Mb/s-koa da, bi noranzkoetan (gorantz eta beherantz).

#### Aldarea (10 ots)

Irudiko Z zerbitzarrikin m konputagailura informazioa jaisteko TCP konexio bat erabilten duen aplikazio bat egikarizen ari gara.



Deskargatzen emandako denbora luzea denez, transmisioren ezaugariak aztertu ditugu. 10<sup>7</sup> biteko fixategia deskargatzeko 10 segundo behar direla neurru dugu, eta traceroute erabiliz ondoko aterapenak neurru ditugu Z eta m konputagailuharen arteko bidean:

<b>Bidea</b>	<b>Atzerapena</b>
Z → B1	5 ms
Z → NAP1	6 ms
Z → NAP2	20 ms
Z → B2	195 ms
Z → m	200 ms

Deskargatzeko denborak muritzeko, ISPar kontrataturako abiadura 6 Mb/s-raino igo dugu bi konexioetan.

1. A sareko teknologia aldatu FastEthernet izatetik Gigabit Ethernet izatera.
2. A sarean X2 bideraztai lotu.
3. ISP-ik B sarearako kontrataturako abiadura bikoitzu (X2-X3 konexioa).
4. ISP-a aldatu, bere sarea zeharkatzeko orangoan baino denbora erdia beharko dela bermatzen duen beste ISP berri batetik Internetarako konexioa kontratatu.

Azaldu nolako eragina izango duen lortutako abiaduran ondoko erabaki bakoitzak:

1. A sareko teknologia aldatu FastEthernet izatetik Gigabit Ethernet izatera.
2. A sarean X2 bideraztai lotu.
3. ISP-ik B sarearako kontrataturako abiadura bikoitzu (X2-X3 konexioa).
4. ISP-a aldatu, bere sarea zeharkatzeko orangoan baino denbora erdia beharko dela bermatzen duen beste ISP berri batetik Internetarako konexioa kontratatu.

**27 AUTOEBALUAZIOA.** Ondoko akronimoak eta terminoak lotu dagokion definitziarenak.  
Kontuan izan definizio bat egiten dutela termino edo akronimo batekin baino gehiagorekin. Adi: 'kreditu' terminoarenzako bi definizio daude.

Kongestio kontrola	Portua	TCP
UDP	RST	Segmentua
SYN	Benetako TCP abiadura	Three-way-handshake
Slow start	Congestion-avoidance	Fluxu kontroila
Kongestio muga	Beste effort zerbitzu	Kreditu
RTT	FIN	FIN

(1) Garraio mailan, aplikazio entitate baten identifikadorea.

(2) Garraio mailako zerbitzu fidagarria emateko erabilten den protokoloa.

(3) Garraio mailako zerbitzu arina emateko erabilten den protokoloa.

(4) Inongo bermerik ematen ez duen zerbitzua.

(5) Igorelek hartzaila ez duela itzoko bermatzea.

(6) Sareak garratatu dezakeen baino trafiko gehiago ez bidaltzeko kontrola egitea.

(7) Pakete bat igorri denetik pakete horren ACK den erantzuna jaso arteko denbora.

(8) Hartzialeak igorleari baimentzen dion igortzeko byte kopurua.

(9) Buxadura kontrolean erabilirako algoritmoetako bat.

(10) Etingabeko transmisoa lortzeko behar den igortzeko bufferren tamaina minimoa.

(11) Hartzailaearren TCP bufferrean libre gelditzen den byte kopurua.

(12) Kongestioa sortzeko arriskua ekiditeko igortzeko bufferren tamainaren mugua.

(13) TCP konexioa ezartzeko egiten den segmentuan elkar trukea.

(14) TCP konexioa ezartzeko eskaera (irekiera aktiboa) egiteko erabilten den segmentu mota.

(15) TCP konexioa amaitzeko eskaera egiteko erabilten den segmentu mota.

(16) TCP protokoloak definitzen eta erabilten duen informazio unitatea.

(17) TCP konexio bat eteteko erabilten den segmentu mota.

(18) TCP konexio batean lortzen den transmisió abiadura, etenaldiak kontuan hartuta.

## ARIKETA PRAKTIKOAK

Ondoko ariketa hauek egiteko Ubuntu instalatuta duen konputagailu bat behar duzu. Batzuetarako, gainera, sare-konexioa behar da. Ariketa batzuk beste sistema askotan ere egin daitezke. Ariketetan erabilten den softwarea ez baduzu, instalatu beharko duzu.

**28** Linux sistema batean, begirada eman /etc/services fixategia. Hor gorderzen da erabilten den portuen esteipena. Alderatu [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers) gunean dagoen esleipen ofizialarekin (zenbait erregistratutako portuak ez dira berdinak izaten).

**29** Linux sistema batean, unean sarean ibiltzen ari diren aplikazioak erabilten ari diren portuak ikusi, *netstat -tulp* egikaritzu. Nmap aplikazioa instalatua baduzu, egin *nmap -sS* portuak aurrekoarekin.

**30** Sarean dagoen trafikoa analizatzeko balio handiko tresna da *ntop*. Ezagutzen ez baduzu, egin *man ntop* edota bilatu informazioa Interneten. Apache zerbitzaria abiatuta dagoela (*apache2ctl*), egikaritu *ntop* terminal batean (*sudo ntop*), eta gero aztertu

<http://localhost:3000/> helbidean duzun informazioa ondoko galderak erantzuteko: Zein da atzemandako paketeen batez besteko tamaina? Nori dagokio trafiko gehiago, TCPri edo UDPri?

**31** Aztertu zeintzuk diren batez besteko RTTren balioak Interneten, ondoko url honetan: <http://www-wammon.slac.stanford.edu/cgi-wrap/pingtable.pl>. Zenbatekoa izango da BDPA (Bandwidth Delay Product) Europen dauden komputagailuen artean?

**32** Aztertu zein den datagramaren tamainaren ergagina datagramak bere helbururaino heltzeko izango duen denboran. Horretarako egin ping makina bati datagrama-tamaina desberdinak erabiliz ('s aukera ping egiterakoan), eta alderatu erregistratutako batez besteko RTTa. Hartu 20 byte era 1400 byte tamainak, eta egin esperimentu zure sare lokalean dagoen makina baten kontra, eta Interneten urrui dagoen beste baten kontra (adibidez: 202.141.151.30).

**33** Konsultatu zein den zure makiniak erabilten duen hartzeko TCP bufferren tamaina, /proc/sys/net/ipv4/tcp\_mmem fixategia konsultatu. Fixategi horren edukiari buruzko informazioa hartzeko, konsulta egin eskuliburuan: man top.

# AURREKO AZTERKETETAKO ARIKETAK

## 2014/uztailak3

**34]**

Demagum ekitaldi bat transmititzen ari dela Internet bidez, eta zuk ikusi nahi duzula zure etxeeko konputagailuan. Ondokoak dira baldintzak:

- Etxean kontratauta duzun Interneteko Konexioak 5 Mb/s-ko abiadura ematen du jaitseran.
- Igortea ondoko bi kalitatezko transmisiok egiten diu: kalitate estandarrak, 1,5 Mb/s abiaduran, eta HD kalitatean (High Definition), 4 Mb/s behar dituena. Hartzaleak aukeratzen du jaso nahi dien kalitatea.
- Zerbitzariak TCP konexio bat erabiltzen du hartzale bakoitzari bere bideo-seinallea emateko.
- Etxetik zerbitzariari egindako ping-ak 200 ms-ko batez besteko RTT-a neurtu egin du. Etxean duzun makinak 87380 byte-ko hartzeko bufferra esleitzen dio, bestetik ezan, TCP konexio bakoitzari (balio tipiko Linux makinetan).

Galerak:

- A) Ba al dago transmisioa ikuseta kalitate estandarrarekin? Baiezkan, zehaztu zein baldintzak bete behar diren ondo ikusi alal izateko. Ez ezkotan, demonstratu zergatik den ezinezkoa.
- B) Ba al dago transmisioa ikuseta HD kalitatearekin? Baiezkan, zehaztu zein baldintzak bete behar diren ondo ikusi alal izateko. Ez ezkotan, demonstratu zergatik den ezinezkoa.

## 2014/uztailak2

**35]**

Wébgune batetik fitxategi bat jaisetean, arakatzaileak 500 kB/s abiadura neurtuzen du (B=byte). Abiadura hori eskasa indutzen zaigunez, informazio gehiago bilatu dugu, eta ondokoak bildu ditugu:

- Web zerbitzariaren sare-konexia 10 Gb/skoa da.
- Jaitsera bakotzeko TCP konexio bakarra onartzen du web zerbitzariak.
- Fitxategia jaisten ari garela, aldi berean 100 jaitsera ari ziren burutzten zerbizzariak. Gure makinen sare-konexioa ADSL bat da, beheranzko abiadura 10 Mb/s duena, eta goranzkoan 1 Mb/s.
- Jaitsera egiten ari garela, gure arakatzailea da sarea erabiltzen duen aplikazio bakarra.
- Gure konputagailua eta web zerbitzariaren artean 200 ms-ko RTTa neurtu dugu.
- Kongestiorik ez dugu atzematen.

Ondoko galerak hauak erantzun:

- a) Datu nahiko baidizun, azaldu zergatik ez dugun lortzen abiadura altuago bat fitxategia jaistean. Ez badira nahiko datuak, azaldu zein datu edo datuak beharko zenizuzke lortutako abiaduraren zergatia argitzeko.

## ARIKETA AURRERATUAK

**36)** (14.25) TCP segmentuen edukia gehienez ere 65.496 byte dauzka. Zergatik horren zenbaki arraioa (ez da 2ren berretura)?

**37)** Web-aren erabiliztaileak lortzen duen zerbitzua atitzentz duen zerbitzariaren menpe dago batzuetan. Zure ordenadoreak badu web zerbitzari bat exarrita, eta orain beste marka batetik beste zerbitzari bat abiatu nahi duzu. Horrela, zure makina atitzentz duen bezeroaren fabrikatzailearen araberria, zerbitzari batekin edo bestearrekin egingo du lana bezertu horrek. Zer deritzozu ideiarri? Arazoren bat ikusten al diozu garratxo-mailan?

**38)** (95a) TCP/IPren implementazio batzuek segmentuentz tamaina maximoa optimizatzentz dute konektioa irekitzerakoan, eta saiatzen ditu besterik ezean hanzen den tamainakoak (536 byte) baino segmentu handiagoak erabilizten, segmentazio-lana txikiagoa izan dadin. Zehazki, Ethernet sareen kasuan, 1460 byteko segmentua erabiliztea proposatzentz dute konektioraren negoziazketan, beste aldeak alda dezala handiegia egiten baldin bazaio. Horrela, segmentu gutxiago bidaliko dira. Bermatzen al du honek segmentuak ez direla zaituko? Baietz erantzutzen baduzu, adierazi ezazu zergatia. Ezezkoan, eman ezazu nahi ez dugun zatikera hori gertatzentz den TCP konektioko adibide bat.

**39)** TCPn, tenporizadore batzuk epea betzen duenean pilaketaren baten seinale dela interpretatzentz da. Ordorio txarren bat ba al dago epe-betetze hori linearen batean sortutako transmisio-errore baten errua denean?



#### 4. Irakasketa aritzeko

##### 4. Ariketa

a) Fitxategie 500 byte  $\rightarrow$  UDP  $\rightarrow$  adreza de es de fitxategi hau da ea de garrantzitsuenen ongi beltza, horria bidaltzea erredetik boile

b) Fitxategie 500 MiB  $\rightarrow$  TCP  $\rightarrow$  garrantzitsuenen fitxategie osorik beltza ea orduan

c) Fitxategie edekin tenientea  $\rightarrow$  TCP

##### 5. Ariketa

SG2 eta SG1 bideratzen dute informazioa, zutikoa sortzen de irteke dena, baina orduriaz buztatu sortzen da horiek datagunea gelditzea diren bufferrean betetzea daitek abiarazia desberdintasun horiek dela eta datagunea laukia, SG1 bideratzeko gelditzea diren aberekin erabili txikiak jartzen baitago.

TCP erabiltzen da de erabildako buztadura, uhinak eta ~~ordurigeren~~ ordu egungo den.

##### 6. Ariketa

a) 5MiB fitxategie  $\rightarrow$  45 segundo  $\Rightarrow A = \frac{5\text{MiB}}{45\text{s}} = \frac{5 \cdot 2^{20} \cdot 8}{45} = 932 \text{kb/s}$   
Soportua 10Mb/s

b)

Bi arrazoia  $\rightarrow$  Errorea geratu daiteke, eta orduriaz pelineko birbidiak behar. Eta transmisioko erreaktibitatea, igorlearen bufferrean uhinak edo delako, hortaztakoa ean dielderoa zutengabea prozesatzen jartzen da oso gogortasunez.

##### 7. Ariketa

transmisioko abiadura: 1Mb/s

Hutsailaren bufferrean: 32KiB

Fitxategie: 5MiB

Durbora: 46 seg  $\Rightarrow A = \frac{5\text{MiB}}{46\text{s}} = \frac{5 \cdot 2^{20} \cdot 2^3}{46} = 911,8 \text{kb/s}$

a) Durbora uhilku ondo: lortu daitekeen abiaduraren %90a baino

b) Durbora uhilku ondo: lortu daitekeen abiaduraren %90a baino  
horde. Suposatu behar da gertuko denaren eta probaldoren orduriaz gertatzen dela, aurreko beharrerako transmisioko abiadura handitzen da. Ordea, zure hori da bidezko hortzak,

Bi ordezena erdioriaz gorte litxka, kreditua biltegia izatea, etc adoriaz leu hainbat berdadez litxka, edo buztatuaren bat geratzena bidai, leu horretako ez dago inoldeko konputibiderile

### 8. Ariketa

$$\text{Kreditua} : 64 \text{ KiB} \Rightarrow 655 \text{ KB}$$

$$\text{abiedura} : 16 \text{ b/s}$$

$$\text{RTT} : 50 \text{ ms}$$

$$\text{BDP Kreditua} = 16 \text{ b/s} \cdot 50 \text{ ms} = 625 \text{ MB}$$

$$\text{BDP} > \text{Kreditua}$$

Ez de denegabeleko trasmisioa, lehendabeko abiedura sareak duen abiedura baino txikiagoa izango daite.

$$\text{Abiedura} = \frac{64 \text{ KiB}}{50 \text{ ms}} = 10.5 \text{ Mb/s}$$

Bete beharreko baliditatea  $\rightarrow$  buztatuarenak ez de egingo leu de bittransmisioko ez RTT edo 50ms baino txikiagoa izan  
Eta lehendabeko irakurri eta itxiezerik edo 50ms baino txikiagoa izan de bultzatu lotu

### 9. Ariketa

Hasi:

• ~~AKZ~~ ~~K~~<sub>RTT</sub>:

if (A == F) {

return F;

else if (A == (K / RTT))

return K;

return Magastia;

### 10. Ariketa

$$\text{RTT} = 100 \text{ ms}$$

$$\text{Kreditua} = 32 \text{ KiB}$$

$$\text{Abiedura} = \frac{32 \text{ KiB}}{100 \text{ ms}} = \frac{32 \cdot 2^{10} \cdot 8}{100 \cdot 10^{-3}} = 26 \text{ Mb/s}$$

## 11. Artikel

Abiendre fiktiv:  $100 \text{ Mb/s}$

$$\text{RTT} = 1 \text{ ms}$$

$$\text{buffer } 32 \text{ KiB} = 32 \cdot 2^{10} \text{ kB}$$

$$\begin{aligned}\text{BDP Kreditiv} &= A_f \cdot \text{RTT} = 100 \text{ Mb/s} \cdot 1 \text{ ms} \\ &= 1 \cdot 10^5 \text{ b} = 12500 \text{ B}\end{aligned}$$

Kreditiv  $>$  BDP  $\Rightarrow$  Abiendre maxima  $100 \text{ Mb/s}$

$100 \text{ GiB}$  do disko deskerget

a) Bei derregnete gemaß uile erbilli belerter de, horakterde TCP de egliere,

Reuer regelgure berustabelo.

b) Rebiendre maxima  $100 \text{ Mb/s}$  do,

c)  $\text{RTT} = 100 \text{ ms}$

Abiendre  $100 \text{ Mb/s}$

$$\text{BDP} = 100 \text{ Mb/s} \cdot 100 \text{ ms} = 1 \cdot 10^3 \text{ b} = 1250 \text{ B}$$

Kreditiv  $80 \text{ KiB}$

Abiendre  $100 \text{ Mb/s}$

$\text{BDP} > \text{Kreditiv}$

$$\hookrightarrow \text{abidure-Max} = \frac{80 \text{ KiB}}{100 \text{ ms}} = 6.5 \text{ Mb/s}$$

$$75 \text{ Tb/s} \Rightarrow 75 \cdot 10^{12} \text{ b/s}$$

$$\text{Kreditiv} \Rightarrow 64 \text{ KiB}$$

$$\text{BDP} = 75 \cdot 10^{12} \text{ b/s} \cdot \text{RTT} \Rightarrow$$

$\text{BDP} = \text{Kreditiv}$

$$\Rightarrow \text{RTT} = \frac{64 \cdot 2^{10} \cdot 8 \text{ b}}{75 \cdot 10^{12} \text{ b/s}} = 6.99 \cdot 10^{-9} \text{ s}$$

$$\text{RTT} = 6.99 \mu\text{s}$$

## 12. Artikel

Kreditiv:  $64 \text{ KiB}$

Abiendre:  $16 \text{ Mb/s}$

RTT:  $20 \text{ ms}$

$$\text{Abiendre} = \frac{64 \text{ KiB}}{20 \text{ ms}} \approx 26.12 \text{ Mb/s}$$

$$\text{Fragelortesone} \approx 82.62$$

## 13. Artikel

## 14. Arilete

A)

Bei posible de horrebeite deitorn beler idas, horrebebo heibet omrei ega daitele, teknik traxo de ekrastos, TCP kreditiva eslede iden deitete, edo buxelarren ht gertzen de berbitzitile ADSL-ro bitorear,

B)

$$RTT = 2s$$

$$\text{Kreditiva: } 5840 \text{ byte}$$

$$\text{Abiadura: } 2 \text{ Mb/s}$$

$$BDP = Abi \cdot RTT = 4 \text{ Mb} \Rightarrow 500 \text{ kB}$$

$$BDP > \text{Kreditiva} \Rightarrow \text{Ondorear}$$

$$\text{Abiadura crete} = \frac{5840 \cdot 8b}{2s} = 233 \text{ kb/s}$$

$$570 \text{ kB} \hookrightarrow \text{Deitorn} = \frac{570 \text{ kB}}{233 \text{ kb/s}} = 200 \text{ s} \Rightarrow 3 \text{ minu } \cancel{\text{do}} \text{ do seg}$$

## 15. Arilete

$$\text{Kreditiva: } 32 \text{ kB}$$

$$\text{Abiadura: } 100 \text{ Mb/s}$$

$$BDP = 32 \text{ kB} \Rightarrow 32 \text{ kB} = 100 \text{ Mb/s} \cdot RTT$$

$$RTT = \frac{32 \text{ kB}}{10 \text{ Mb/s}} = 262 \text{ ms}$$

Bet era ealogo de gana

## 10. Arilete

$$\text{Abiadura: } 10 \text{ Mb/s}$$

$$RTT: 80ms$$

$$\text{Kreditiva: } 10 \text{ kB}$$

$$BDP \text{ Kreditiva} = 10 \text{ Mb/s} \cdot 80 = 800 \text{ kB}$$

$$BDP \geq \text{Kreditiva}$$

8kB-ko transmision beldoe buxelarre crive

$$\text{Abiadura maxima} = \frac{\text{Kreditiva}}{RTT} = \frac{8000 \text{ kB}}{80 \text{ ms}} = \frac{10 \cdot 10^3 \cdot 8}{80 \text{ ms}} = 1 \text{ Mb/s} \quad \cancel{[600 \text{ kb/s?}]}$$

b) Buxelar sortean duen bidelatzailearen kreditiva igotzea habe de horrela <sup>milobelo</sup> kreditua crizozeta ealogo de, eta abiadura laudiko, Abiadur fisikoa kreditua  $\rightarrow$  bera bixtua geruza abiadura nafiona berdin ealogo da.

## 21. Arithme

a) 100 kB fitategie

transmisió abiedura: 100 Mb/s

Rtt: 5 ms

BDP kreditive = 50 kB

kreditive: 8 kB

BDP > kreditive

Procedure: 7 kB krediteen

$$\text{Abiedura maxima} = \frac{7 \text{ kB}}{5 \text{ ms}} = \frac{57344 \text{ b.t}}{5 \cdot 10^{-3} \text{ s}} = 11'468 \text{ Mb/s}$$

Abiedura maxima: 10 Mb/s

$$\text{Debtore} = \frac{100 \text{ kB}}{10 \text{ Mb/s}} = 0.81 \text{ s}$$

b)

Biblioteca estrena ~~transmisió~~ abiedura kredite enrgico de debore

Bestade es de eza gatellito.

## 23. Arithme

Abiedura lata den: 1 Mb/s

Abiedura fitller: 16 Gbps

$$\text{BDP: } \frac{16 \text{ Gbps}}{\text{50ms}} = \frac{2048 \text{ Gbps}}{50 \cdot 10^{-3} \text{ s}} = 40960 \text{ GB}$$

kreditive: 16 kB

BDP > kreditive

Rtt: 50 ms

$$\text{Abiedura maxima} = \frac{16 \text{ kB}}{50 \text{ ms}} = 26 \text{ Mb/s} \text{ idemgo latache}$$

Ordinatz arroses, ~~bestade~~ bestade buendache enrgigo dek

Ez es latache erabili zuzene idemgo Ez deigileko zoin idemgo den arroses. Ez adieriz, es de zezurra hori konposibila izate

Ez TCP-re erregorriko es ditzelko sortzen erabie

## 25. Arbeit

Abiendrate festgelegt:  $1 \text{ Mb/s} \rightarrow 3 \text{ Mb/s}$  Abiendrate beträgt:  $128 \text{ Mb/s}$

RTT: 100ms  
 $\downarrow$   
~~BDP 100ms~~  
 $\Rightarrow 1 \text{ Mb/s}$   
 $\text{RTT } 128 \text{ ms}$

$3 \text{ Mb/s}$   
 RTT: 80ms  
 Abiendrate:  $16 \text{ Mb/s}$

$$\text{Abiendrate} = \frac{\text{Ureditate}}{\text{RTT}} \Rightarrow \text{Ureditate} = \text{Abiendrate} \cdot \text{RTT} = 16 \text{ Mb/s} \cdot 80 \text{ ms} = 16 \text{ KB - Paket}$$

Ureditate degen aufgrund mehrerer ISP die eskeinten digen Abiendrate  $3 \text{ Mb/s}$  über  
 ca. je 100ms hältten.

~~Abi:  $\star \text{ RTT} = 200 \text{ ms} \Rightarrow \text{Abiendrate} = \frac{16 \text{ kB}}{200 \text{ ms}} = 64 \text{ Mb/s}$~~ 
~~BDP < Ureditate~~

~~Abiendrate tatsächl. =  $3 \text{ Mb/s}$  (ca. 200ms)~~

Espresso der Abiendrate  $3 \text{ Mb/s}$  (ca. 200ms)

~~Bestellte Abiendrate  $\Rightarrow \text{RTT} = \text{Ureditate} = \frac{30 \text{ kB}}{3 \text{ Mb/s}} = 10 \text{ ms}$~~

$\text{BDP} = 3 \text{ Mb/s} \cdot 200 \text{ ms} = 60 \text{ kB}$  aufgrund Ureditate der bestellt er erfordert  
 (ca. 100ms)

$\hookrightarrow$  Ureditaten erfüllt er, bzw. durch bestellt

## 34. Arbeit

$5 \text{ Mb/s}$  Abiendrate, restet

$$\text{RTT} = 200 \text{ ms}$$

$$87380 \text{ bytes : Ureditate}$$

$\text{BDP} > \text{Ureditate}$

$$\text{BDP} = \text{Abiendrate} \cdot \text{RTT} = 5 \text{ Mb/s} \cdot 200 \text{ ms} = 1 \text{ Mb}$$

$$\hookrightarrow \text{Abiendrate maxima} = \frac{\text{Ureditate}}{\text{RTT}} = 375 \text{ Mb/s}$$

Bei idealen Verbindungen unterstellt werden kann es die längste Zeitspanne  
 sonst beliefert die lokale Abiendrate mindestens  $15 \text{ Mb/s}$  kann beliebiger als konstant  
 werden durch Bitarten

Höchste Ureditate ergibt sich  $375 \text{ Mb/s}$  ggf. geringer da beliebiger als die  
 höchste RTT = 200ms annehmen

Höhere RTT bedeutet es gibt Verzögerungen im Netzwerk, die die Abiendrate  
 limitieren da die Abiendrate maxima  $375 \text{ Mb/s}$  überschreiten, obgleich höchste Abiendrate.

## 14. Arribeta

Abicadura máxima = 2Mb/s

Kreditive = 5840 byte

RTT = 2segundo

$$BDP = \text{Abicadura} \times \text{RTT} = 2\text{Mb/s} \times 2\text{s} = 4\text{Mb} \Rightarrow 05\text{MB}$$

BDP > Kreditive, ondorios etengabeko trasmisioa ez da lortuko.

$$\text{Abicadura} = \frac{\text{Kreditive}}{\text{RTT}} = \frac{5840 \text{ byte}}{2\text{s}} = 23'4 \text{ kb/s}$$

Ondorios,

$$570 \text{ kiB desberdaketa} \Rightarrow \frac{570 \text{ kiB}}{23'4 \text{ kb/s}} = \frac{570 \cdot 2^10 \cdot 8}{23360} = 199'9 \text{ s}$$

3 min 19 sec



#### 4. Gaina

##### Arketakoak

#### 5. Arketakoak

A)

Kreditua 64KiB

Gigabit Ethernet  $\Rightarrow$  1Gb/s

RTT = 50ms

$$\text{Abiadura} = \frac{\text{Kreditua}}{50 \text{ RTT}} = \frac{64 \text{ KiB}}{50 \text{ ms}} =$$

$$\left. \begin{aligned} \text{BDP} \text{ kreditua} &\Rightarrow \text{Abiadura} \Rightarrow \text{RTT} = \\ &= 1 \cdot 10^9 \text{ b/s} \cdot 50 \cdot 10^{-3} \text{ s} = \end{aligned} \right.$$

$$= 50 \cdot 10^7 \text{ b} = 50 \text{ Mb} = 625 \text{ MB}$$

$$\left. \begin{aligned} \text{BDP} > \text{kreditua} &\Rightarrow \text{kreditua} \\ \text{etxeko RTT}-\text{ra jarriz} &\text{uzte} \\ &= \frac{64 \cdot 2^{10} \cdot 8}{50 \cdot 10^{-3}} = 105 \cdot 10^6 \text{ b/s} = \\ &= 105 \text{ Mb/s} \end{aligned} \right.$$

B)

Konexio koneten abiadura maximoak lortzeko, konexio  
irakurria da itxiene. Esan dira kontrua izan, eta kontrera gain  
atzeraezteko esan de ezen eate bintzaski ziorrik ere.

#### 10. Arketakoak

Bero - Berbitzari RTT = 100ms

Bufferreak Kreditua = 32KiB

Zin de abiadura maximoa?

$$\text{Abiadura} = \frac{\text{Kreditua}}{\text{RTT}} = \frac{32 \text{ KiB}}{100 \text{ ms}} = \frac{32 \cdot 2^{10} \cdot 8 \text{ bit}}{0,1 \text{ s}} = 26 \text{ Mb/s}$$

## II. Arilitate

Abiadura = 100 Mb/s  $\Rightarrow$  Fast Ethernet

Kreditua = 32 KiB

RTT = 1 ms

Tamaina etengabeko trasmisio berriaileko beharko litakoen kreditua.

$$\text{BDP} = \text{Abiadura} \times \text{RTT} = 100 \text{ Mb/s} \cdot 1 \text{ ms} = 100 \cdot 10^6 \cdot 10^{-3} \text{ s} = \\ = 10^5 \text{ b} \Rightarrow \frac{10^5}{8} = 12500 \text{ Berautz}$$

Kreditua < lehiak ondorioz etengabeko trasmisio berriaileko da

Ondorioz, Abiadura maximo, Fast Ethernetekin eran  
deialdeek handiak, 100 Mb/s

c)

Bi komputagailuek interntzen,

RTT = 100 ms

Abiadura = 100 Mb/s

Buffer tamaina = 80 KiB

$$\text{BDP} = \text{Abiadura} \times \text{RTT} = 100 \text{ Mb/s} \cdot 100 \text{ ms} = 10 \cdot 10^6 \text{ b} = 125 \text{ MB}$$

Lehiak  $\Rightarrow$  Bufferra = Ondorioz ez de trasmisio  
etengabear.

$$\text{Abiadura} = \frac{\text{Kreditua}}{\text{RTT}} = \frac{80 \text{ KiB}}{100 \text{ ms}} = 6'55 \text{ Mb/s}$$

## 5. ikasgaiko ariketak

**1** (97ir) Erabilzaille baten PCa Ethernet sare batean dago konektatutik. Sare horren bidez, eta TCP/IP arkitektura erabiliz, sare berean dagon beste makinarekin konektatzera da. Aplikazioarekin. A. aplikazio horrek P protokoloa erabilizten du bezeroa (PCan degoena) eta zerbitzariaren (beste makinean dagoena) arteko komunikazioa arautzeak. P protokoloa jarraituz, A-k K komandoa, 12 karakterekoa, bidaltzen du. Idarzi ezazu zer informazio-unitate part hartzen duten komando horri bidaltzeko, ondokoak adieraziz.

- Zer protokolo definizituen dientz informazio-unitate bakotzaren egitura.

- Nola kapsulatzen diren unititatek hain artean.

- Nola lortzen den unitate bakotzeko helburu-helbidea.

- Zer errore-kontrol dauden prozesuan guzian zehar.

Suposatu ezazu P protokoloak ez duela inongo errore-kontrolik eta A aplikazioak fidagarrietasun handia behar duela.

*Irradiorikoa: gaidetxen erantzun arkitetura-mailako, informazioaren ateratzeko bidea jarraituz (goitik-behera protokolo-multzoan zehar).*

**2** Bedi TCP/IP arkitekturaren bidez. Ethernet sare batean lotuta dagoen X izeko konputagailu bat. Demagun konputagailu horretatik ondoko lau bidalketa hauek egiten direla:

- DNS galdera bat.
- ICMP mezú bat.
- ARP galdera bat.
- HTTP komando bat.
- Ondoan duzuna bezalako taula bat bete hauetako bidalketa bakoitzeko (4 taula). Taula bakoitzean, lero bat gehitu bidalketan zeozer ikusztik duen arkitekturako malla bakoitzeko, fisikoak ez ezik.

**3** Bedi KSO.org domeinuaren jabea dena, eta hosting eta DNS zerbitzuak eskaintzen dituena. Alegia, A enpresaren zerbitzarietan besteen zerbitzariak egitarritzat dientz, eta A enpresaren DNS zerbitzariak bere bezeroan domeinuetarako DNS jatorrizko zerbitzariena egiten du. Demagun beste enprese bat, B izekoak, 'sareak.tk' domeinuaren jabea dena, eta A enpresaren zerbitzua kontratatuko duena, bere web zerbitzariari eta posta zerbitzariari ostatzeko A-ren makinetan, baita DNS jatorrizko zerbitzua ere bere domeinurako. Zehazki:

- www.sareak.tk izeko web zerbitzaria, webak.enpresa.com izeko zerbitzarian ostatuko du A enpresak.
- smtp.sareak.tk izeko posta zerbitzaria, postak.enpresa.com izeko zerbitzarian ostatuko du A enpresak. Zerbitzari horrek eman behar du posta zerbitzua 'erabiltzailea@sareak.tk' moduko posta helbideei.
- 'sareak.tk' domeinuari dagokion jatorrizko zerbitzaria dns.enpresa.com izeko zerbitzaria izango da.

Hona hemen interfazearen (nslookup-aren) erantzuna:

Server: scsx01.sc.ehu.es  
Address: 158.227.150.40

sc.ehu.es preference = 10, MX = scsx01.sc.ehu.es  
sc.ehu.es preference = 20, MX = lgsx01.g.ehu.es  
sc.ehu.es preference = 30, MX = vchx00.vc.ehu.es  
sc.ehu.es preference = 40, MX = mail.rediris.es  
NS = scsx01.sc.ehu.es  
sc.ehu.es NS = lgsx01.g.ehu.es  
scsx01.sc.ehu.es A = 158.227.150.40  
lgsx01.g.ehu.es A = 158.227.2.34  
vchx00.vc.ehu.es A = 158.227.224.30  
mail.rediris.es A = 130.206.1.2

Erantzun itzazu ondoko galderak.

1. Zein makinak jasoko du patxi@sc.ehu.es helbidera bidaltako mezu bat? Zein dia makina horren IP helbidea? Argitu ezazu zure erantzunean zertan oinarrizten zaren.
2. 'ehu.es' eremuaren Internetetik isolatuta geratuko balitz, galduko al litzareke helbide horretara 'orlegi.zumalabe.org' makinatik bidaltako mezuak?

**4** (13-7) Bedi KSO.org domeinuaren jabea den entitate bat. Entitate berak kudeatzen du domeinua, eta horretarako bere sarean du dns-zone.kso.org izeko zerbitzaria, domeinu horretarako jatorrizko DNS zerbitzariaren lana egiten duena (*authoritative server*).  
  
Baina, orain, entitateak erabaki du domeinuaren kudeaketa ISP bati kontratatza, bere dns-zone.kso.org makina deskontraktatza, eta makina horrek ematen zuen zerbitzua ISPPren sarean dagoen dns-berzeroa.isp.com makinatik harartzeari bere gain.  
(A) Azadiu zein aldatketak egin beharko diren DNS zerbitzari eta erregistroetan aldaketa abiarazi ahal izateko.  
(B) Zertan eragingo duele aldaketa horiek kso.org sareko makinetako DNS konfigurazioan?

**5** (12-5) Demagun A enpresa, 'enpresa.com' domeinuaren jabea dena, eta hosting eta DNS zerbitzuak eskaintzen dituena. Alegia, A enpresaren zerbitzarietan besteen zerbitzariak egitarritzat dientz, eta A enpresaren DNS zerbitzariak bere bezeroan domeinuetarako DNS jatorrizko zerbitzariena egiten du. Demagun beste enprese bat, B izekoak, 'sareak.tk' domeinuaren jabea dena, eta A enpresaren zerbitzua kontratatuko duena, bere web zerbitzariari eta posta zerbitzariari ostatzeko A-ren makinetan, baita DNS jatorrizko zerbitzua ere bere domeinurako. Zehazki:

- www.sareak.tk izeko web zerbitzaria, webak.enpresa.com izeko zerbitzarian ostatuko du A enpresak.
- smtp.sareak.tk izeko posta zerbitzaria, postak.enpresa.com izeko zerbitzarian ostatuko du A enpresak. Zerbitzari horrek eman behar du posta zerbitzua 'erabiltzailea@sareak.tk' moduko posta helbideei.
- 'sareak.tk' domeinuari dagokion jatorrizko zerbitzaria dns.enpresa.com izeko zerbitzaria izango da.

Azaldu **zein DNS erregistroak** gorde behar diren, eta **zein DNS zerbitzarietan**,

- 'www.sareak.tk' izeña edozeinek ebazti ahal izateko,

Erantzuna emateko, horrelako taula bat bete:

- eta 'erabilitzalea@ssareak.tk' moduko helbide bat mezu bat bidali aha! Izateko.

卷之三

- 3) 'empresa.com' domeinurako jatorrizko DNS zerbitzaria dns.empresa.com makina da.

4) Makina baten IP helbide bat azaleak behatzen zuanean, @makinaren izena eran idatzi.

(12-6) ISP izeneko horriztzaileak Internetetarako sarbidea eta Totutako hainbat zerbitzu (DNS ebazpena, domeinuen kudeaketa, zerbitzarien hosting eta abar) ematen die beren bezeroei. Horrietako bezero bat EDX izeneko erakundeak da, edx.com domeinuaren jabea dena. EDX erakundeak horrela antolatu ditu bere zerbitzu nagusiak:

edx.com domeinurako DNS jatorrizko zerbitzua ISP-ri kontratatu dio. Domeinu horri dagokion jatorrizko erantzunak dnszones.isp.com izeneko barnetikо zerbitzariak (zone server) emango ditu.

EDX erakundeko sarearkeria DNS ebazpena eta caching zerbitzua (berrako DNS dns.edx.com makinak emango du, erakundeko sarean bertan kokauta). www.edx.com web zerbitzaria zerbitzariak.edx.com izeneko konputagailuan egikarituko da. Kaptoplik atzigarria izan behar du zerbitzari horrek. Posta jasotzeko eta igortzeko zerbitzari bakarra egongo da, posta.edx.com izeneko konputagailuan kokauta.

Kaptoplik eror daitezeen arriskuetaz babesteko, mugasare bat erabiliko du.

Ondokoak erantzun:

- A) Egin ezazu sate-eskema bat, enuntziatuan agertzen diren makina guztiak kokapena azalduz. Behar diren suhesiak ere kokatu eskeman.

- B) Zerrendatu [dnszones.jsp.com](http://dnszones.jsp.com) zerbitzarian gorde behar diren DNS erregistroak, EDX erakundeko zerbitzuei dagozkienet. Erregistro bakoitzeko ondoko hiru eremu hauek zehaztu: mota, izena, eta balioa. IP helbide bat idatzi behar duzunean, oliko

- C) Demagun posta zerbitzua hortela berrantolatu behar duela erakundeak:

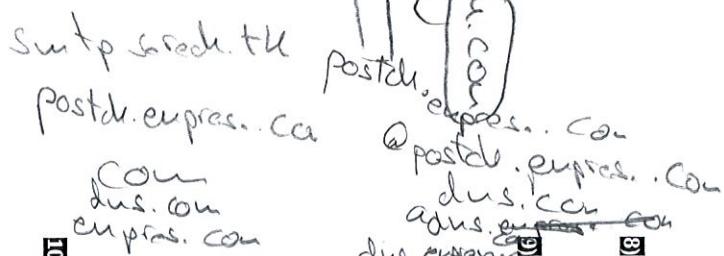
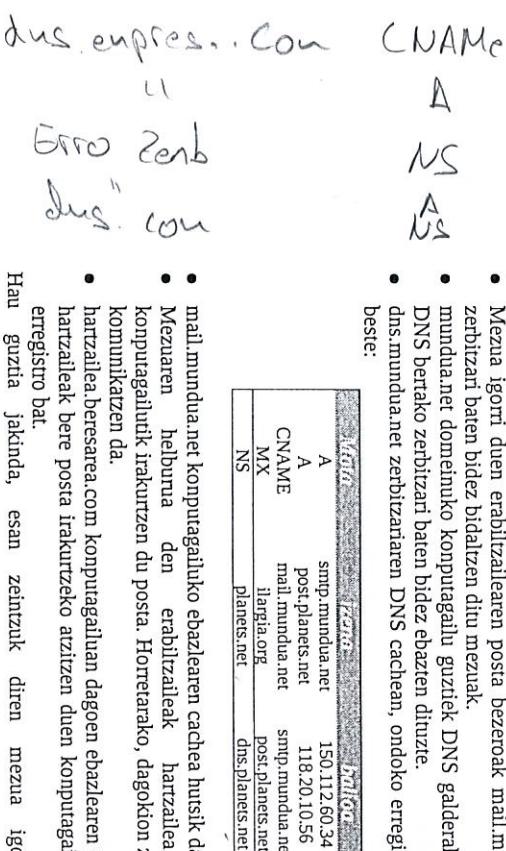
- [posurteek.com](http://posurteek.com) makuaik pasauaiteaeraua egingo ut, eta ez zuu buzuan goruenko. Hau da, beren posta irakurtzelo, erabiltzaileen posta bezeroek beste makina

- Posta igortzeko, posta.edx.com makina erabilten erabilzaileek. Hala ere, ezizen bat (alias) definituko da horretarako:

Berrantolaketa hori kontuan izanik, erantzun ondokoak:  
[smfp.edox.com](http://smfp.edox.com).

- dnszones.isp.com zerbitzarien gordetako erregistroetako dagoenez?

C.2) Demagun erabiltzaile baten posta helbidea erabeedx.com zela berantolaketaari ekin baino lehenago, hau da, bere buzia posteedx.com



- 3** http://www.eventhelix.com/RealtimeMantra/Networking/SMTP\_Sequence\_Diagram.pdf fitxategia deskargatu, eta bere edukia aztertu. Posta bidatzeko emanako urratsaren bat ulertzen ez baduzu, bidalí ezazu gaadera bat irakasgailko forora.

C.) Non kokatuko da, hasierako eskeman, pop3.edk.com zerbitzari berria.

Egin ezazu mezu elektroniko bat bidatzeko emandako urratsak adierazten dituen eskema bat. Komunikaren ondokoak:

  - Igorlearen helbidea igorlea@igorlea.org da, eta hartzalearena hartzalea@hartzalea.org.
  - Parte hartzten duten aplikazio mailako entitate guziak agertu behar dute eskeman.
  - Eskemako urrats bakoitzak aplikazio mailako bi entitateen arteko eragiketa batiegon beharko zai o. Salbespena: DNSri egindako eskaeraek eragiketa bakar batean bilduta.
  - Adierazi zer egiten den urrats bakoitzean, baita zein aplikazio protokoloa erabiltzen den ere. Ez dira adierazi behar eragiketa buruzeko trukatuak komunikatua eta erantzunak.
  - Igorleak web zerbitzari baten bidez atzitzen du posta zerbitzua.
  - 'hartzalea.org' izenari loutako zerbitzariak, 'hartzalea' izeneko erabiltzalerako jasotako mezuak 'hartzalea2.hartzalea.org' izeneko bigarren zerbitzari badi birtbdaltsen dizkio.
  - hartzalea@hartzalea.org erabiltzalearen bezeroa konfiguratura dago hartzalea2.hartzalea.org zerbitzariak mezuak jaisteko, IMAP erabiliz.
  - Ebazleen DNS cacherik ez dutela hartu.

**10** Demagun Iudia.mundua.net izeneko konputagailuren erabiliztaile batetek selenita@ilarria.org posta helbidera mezu bat bidaltzen duela, bere posta bezeroa erabiliz (beraz, ez du posta aritzten web-aren bidez). Suposa dezagun ondoko baldintzeten gabeztala:

  - Mezuak igerri dhen erabiltzalearen posta bezeroak mail.mundua.net izeneko SMTP zerbitzari baten bidez bidaltzen ditu mezuak.
  - mundua.net domeinuko konputagailu guziiek DNS galderak dns.mundua.net izeneko DNS bertako zerbitzari baten bidez ebazten dituzte.
  - dns.mundua.net zerbitzaren DNS cachean, ondoko erroregistro hauek daude, bestea bestea:

- [14] hartzalearenaino (hartzalea.beresarea.com) allegatzeko emango diren urratsek. Ondokoak adierazi urrats bakoitzeko:
- Zeintzuak diren urratseen parte hartzen duten bi konputagailu.
  - Zer egiten den urrats kontuan.
  - Bi konputagailuen arteko komunikazioan erabilitako aplikazio mailako protokola.
  - Eozein bi konputagailuen arteko elkarrekiniza hasten den bakoitzean, urrats berri bat dela hartu.

[15] Demagun erakunde batek horrela antolatzen duela bere posta zerbitzua:

- Kampotik etorritako mezu guztiai sartzena geu.org izeneko SMTP zerbitzariak jasozten ditu. Gero, spam eta hiruask garbituta, mezu biribilatzen dio mezuaren hartzaleari dagoen POP zerbitzariari.
- Beste bi posta zerbitzari daude erakunde honetan, zuzenean erabiltsaileei SMTP eta POP zerbitzua ematen. Zerbitzari hauen izenak postal.geu.org eta post2.geu.org dira.
- Aurreko bi zerbitzari horiek honako beste ezizen hauek dituzte:
- postal zerbitzariarenak: smtp1.geu.org, pop1.geu.org.
- post2 zerbitzariarenak: smtp2.geu.org, pop2.geu.org.

Hau guzia jakinda, esan zein DNS erregistroek egon beharko dute zein DNS zerbitzarietan posta zerbitzua ondo ibili ahal izateko. Ondokoak kontuan hartu:

- Eregistro bakotzeko hiru datu hauek eman: Mora, izena, eta balioa.
- IP helbideak, adierazteko, @ ikurra ipini makinaren izenaren aurtean. Adibidez: @sarposta.geu.org.
- @sarposta.geu.org. genu.org doméniu osorako DNS barutu bakarra dago definitua, dns.geu.org izeneko jatorrizko zerbitzariak zerbitzatzen duena.

[12] Demagun empresa batek empresa.com doméniua duela erregistratuta. Hasierra batean, empresa horrek posta zerbitzai bat abiatu du, bere erabiltsaile guztiak posta zerbitzua emateko. Empresaren buzoi guztiek erabiltsailearen izena@empresa.com moduko helbideak dituzte. Empresa zabaltzen den heinean, posta zerbitzua berrantolatu du, eta buzoi guztiek ondoko hiru posta zerbitzarietan banatu dituzte: bat erosketetarako sailakako, beste bat salmentarako sailakako, eta beste bat kudeaketan aritzzen diren langileentzako. Zerbitzari zaharrak, orain, dagokion beste horietako zerbitzariari bitbidaliko dizkio jasotako mezuak Posta zerbitzari berrien izena, hurrenez hurren, eta postakudeaketa.empresa.com dira.

I Lehendik posta helbide bat zeukaten erabiltsaileek (hau da, zerbitzai zaharrean bere buzoiaik zeuzkatenek), izango al dute helbide hori mantentzea, ala aldatu beharko dute?

- Postontzi berri bat lortzen duten erabiltsaileek, erabiltsailearen izena@empresa.com, postakudeaketa.empresa.com dira.

[13] Ondoko fixategia jaitxi eta bere edukia aztertu:

- moduko helbidea ahal izango dute?

[http://www.eventhelix.com/RealtimeMantra/Networking/http\\_sequence\\_diagram.pdf](http://www.eventhelix.com/RealtimeMantra/Networking/http_sequence_diagram.pdf)

Emandako urratseren bat ulertzen ez baduzu, egin ezazu galdera bat irakasgaiko foroan.

- [14] Bedi geu.org izeneko sare bat, non web eskaera guztiek proxyweb geu.org izeneko web proxyaren bidez egin behar dira. Demagun sare horretan dagoen K izeneko makineko arakatzaleari <http://www.zuek.org/index.html> url-a ematen diogula. Arakatzalean eskatutako orria kargatzeko ematen diren aplikazio mailako urratsek zerrendatu, ondookoak kontuan hartuta:
- Cache guztia hutsik daude.
  - Arakatzaleak badu bere konfigurazioan proxyaren IP helbidea.
  - gen1.org sareko konputagailu guztientzako bertako DNS zerbitzaria dns.geu.org da.
  - zuek.org domeinuan DNS barruti bakarra dago, dns.zuek.org jatorrizko zerbitzariak zerbitzatzen duea.
  - www.zuek.org ezizten bat da, kanpoweb.zuek.org konputagailuarena.

Urrats bakoitzean ondookoak azaldu:

- Zer makinak egiten duen eskaera/erantzuna.
- Zer makinari egiten zaion eskaera/erantzuna.
- Zer aplikazio mailako protokoloa erabilten den.
- Zer eskatzen den edo zer erantzuna jasotzen den.

Adibidez: A makinak B makinari (zuek.org) DNS galdera egiten dio DNS protokoloa erabiliz.

- [15] Bedi sare bat, non Interneten dauden web zerbitzarietarako atzipen guztiai proxi baten bidez segiten dira. Ondokoak suposa ditragun:
- Saneko arakatzale batek eskaratuko orria web proxiak bere cachean edukitzeko probabilitatea 0'4 da.
  - Web proxian dagoen bertako DNS zerbitzariak galdera batu dagokion erantzuna bere cachean edukitzeko probabilitatea 0'5 da.
  - Ondoko bi aukera hauiek aztertu, eta kalkuluatu horietako zeinekin muritzuko dugun gehien sareko arakatzale batek Internetetik web orri bat jaisteko behar duen denboran:
  - A aukera: web proxian cachearen tamaina handitu, eskaratako orria edukitzeko probabilitatea 0'6 izan arte.
  - B aukera: Bertako DNS zerbitzariaren cachearen tamaina handitu, galdera baten erantzuna edukitzeko probabilitatea 0'9 izan arte.

Azkenetik hori egiteko, honako baldintza hauet hartu kontuan:

- Arakatzaleek badute beraien konfigurazioan web proxien helbidea.
- Eskaera egiten duen arakatzalearen cachea hutsik dago.
- Ori bat web proxitik arakatzailera HTTP bidez eramateko batez besteko denbora 20 ms da.
- Ori bat Interneten dagoen web zerbitzari batetik web proxira HTTP bidez transmititzeko batez besteko denbora 500 ms da.
- Web proxian dagoen DNS ebazoleak ez du cacherik.
- Izen bat ebazteko batez besteko denbora 10 ms da bertako DNSak erantzuna bere cachean baldin badu. Bestela, 100 ms behar dira.

- [16] (13-5) Erakunde batek bere web zerbitzaria housing eran du ostatuta kampoko enpresa baten instalazioan. Erakunde horren sarean Internetetik sartzen den trafiko gehienetik posta helbideak erabiltzen dituzten web eskaeren %80a, sare bereko eta atzeman dute sareko erabiltsaileek egiten dituzten web eskaeren %80a, sare bereko

- (15) Ez izen baten izen kanonikoa gordetzen duen DNS erregistroa.

Aholkulari batek proposatu du zerbitzua berantolatzea, eta sareko erabiltaile guziak beren arakatzaileak konfiguratu behar izatea beren eskaerak web proxy baten bidez bideratzeko.

Zure lana proposamen horrek izango duen eragina ebaluaztea izango da. Ondokoak baloratu behar diruzu:

- a) Erakundeko web zerbitzariek duten lan-zaman izandako eragina.

b) Housing zerbitzua ematen duen enpresari kontratatu beharreko banda-zabalera izandako eragina.

c) Enpresako sareen Internetetik sartzen den trafikoaren kopuruan izandako eragina.

d) Deskarga egiteko erabiltaile batek behar duen batez besteko denboran izandako eragina.

e) Erakundeko sareetik at dauen DNS zerbitzariei egindako eskaeren kopuruan izandako eragina.

f) Erakundeko sareen dagoen bertako DNS zerbitzariari egindako eskaeren kopuruan izandako eragina.

- [17] AUTOBALUAZIOA.** Ondoko akronimoak eta terminoak lotu dagokion definizioarekin. Adi: badadue bi termino definitio bera dagokienak.

## ARIKETA PRAKTIKOAK

Ondoko ariketa hauek egiteko Ubuntu instalatuta duen konputagailu bat behar duzu. Batzuetarako, gainera, sare-konexioa behar da. Ariketa batzuk beste sistema askotan ere egin daitezke. Ariketetan erabiltzen den softwarea ez baduzu, instalatu beharko duzu.

**[18]** [www.root-servers.org](http://www.root-servers.org) orrira joan eta esan zenbat DNS erro-zerbitzari dauden atzigarriak IPv6 erabiliz.

**[19]** Linux konputagailu batean, host -v [www.10xemi.org](http://www.10xemi.org) komandoa egikaritu (bestela eskolan banatutako fotokopian begiratu horren emaitza), eta ondoko hauet erantzun:

- Zenbat DNS galdera igori dira?
- Zein DNS erregistroa eskaaten da horietako bakoitzean?
- Zein galderak jaso dute erantzuna?

**[20]** Linux sistemetan, DNS ebazlearen konfigurazioa /etc/resolv.conf eta /etc/host.conf fixatuegian gorderen da. Aztertu fixategi hauen balioa zure konputagailuan. Fixategi hauet buruzko informazioa Interneten bila dezakezu, edo /etc/resolv.conf eta /etc/host.conf egin.

**[21]** Ebazlearen cachearena /etc/hosts fixategiak egiten du Linux sistemetan. Aztertu zure konputagailuan fixategi horren edukia. Fixategi hau erabilizten da zerrenda beltzak sortzeko eta erabilizteko gure konputagailuan, hau da, sartzeko nahi ez dugun gunearako sarreta blokeatzeko gure konputagailuan. Adierazi, edo bilatu Interneten, nola egiten den.

**[22]** Aureko ariketa batean erabilitako host tresnaren oso antzekoa da dig. Bere erabilieretako bat, oso didakikoa, izen bat ebazteko parte hartu behar duen zerbitzariak zeintzuk diren aurkitzea da. Horretarako egin behar dena honako da: erro-zerbitzari bat galdezka hasi,

eta emandako erantzunariak (NS erregistroak) abiatuta, segi galderak egiten hurrengo zerbitzariei, erantzuna lortu arte. Adibidez, demagun F erro-zerbitzari baterik hasten garela [www.ehu.es](http://www.ehu.es) izenaren atzean degoen helbidea jakiteko: dig +norecuse @f.root-servers.net www.ehu.es. Segi bilaketa, A erregistroa lortu arte. Oharra: askotan NS erregistro bat baino gehiago jasoko duzu zerbitzariak erantzunean. Horietako edozein har dezakezu hurrengo galdera egiteko.

- [23]** Egin eza zu berriro aureko artiketa, baina orain [www.eitb.com](http://www.eitb.com) izenari dagokion A erregistroaren bila. Ariztertu emaitzak eta erantzun:
- Zein domeinuan daude .com domeinuko TLD zerbitzariak?
  - eitb.com domeinuarri dagokion DNS jatorrizko zerbitzua EITB? Erantzun empresarean al da?
  - Zein konpaniak ematen dio DNS zerbitzua EITB? Erantzuna emaneko, erabil dezakeazu webean dauden domeinei buruzko informazio-zerbitzuak (adibidez: <http://www.whois.net>).
  - Zein konpaniak ematen dio EITBri bere web zerbitzarietarako hosting zerbitzua? Nonago fisikoki kokatuta [www.eitb.com](http://www.eitb.com) webgunea?

**[24]** Beharrezko al zen +norecuse aukera erabilteera aurreko ariketean? Zergatik?

- [25]** DNS ero zerbitzarien artean, F nodoa da munduan zehar kopia gehien dutenetako bat. Gureganatik gertuen daudenak Lisboa, Paris, Madrid eta Barcelonakoak dira. Internetekin lotutako Linux makina batean dig +norec @F.ROOT-SERVERS.NET HOSTNAME.BIND CHAOS TXT egikaritu, kopia horien artean guri erantzungo diguna zein den jakiteko. Kopia bakoitzaren kodea zein den jakiteko, <http://www.isc.org/ops/root/sites.php> orrian begiratu.

**[26]** Zoaz <http://www.dnsquery.org/> webgunera, eta aztertu [www.eitb.com](http://www.eitb.com) izenari dagokion informazioa, DNS Record Query/Any aukera erabiliz. Lortu al duzu izen horren atzean dagoen makinaren IP helbidea? Makina hori, EITB-ren egoitzan al dago?

- [27]** [www.sendersbase.org](http://www.sendersbase.org) webguneari begirada bat eman, eta erantzun: Munduan dabilen posta elektronikoaren zein ehuneko da spam?

Zein herritik bidalzen da spam gehien?

**[28]** Web deskargak arin daitzeke hainbat TCP konexio paraleloan ezartzen badira arakatzalea eta zerbitzariaren artean. Zure arakatzaleak zenbat konexio iraunkorrak (persistent) ezartzen duen paraleloan ikusteko, eman 'about:config' url-aren tokian arakatzaleari (firefox-en kasuan behintzat) eta aztertu aurkeztutako orria. Agertzen den parametro zaparradan bilatu 'connections' hitza dutenak.

**[29]** SMTP portua (25 portua) irekita duen konputagailu batera egin telnet (gaur egun, ez da erraza topatzea). Erobili ezazu SMTP protokoloa (eta ez SMTP) portu horretan zai dagoen posta zerbitzariarekin mezu bat 'postmaster' konexio iraunkorralu horren erabilizalearen (nahikoa da erabilizalearen izena ematea RCPT TO komandoan) bidaltzeko, eta irxi saioa. Erobili behar dituzun komandoak jakiteko, bibliografia kontsultatu, edo wikipediaren SMTP terminoan begiratu. Zer tan aldatuko zen erabilitako komandoen sekuentzia, testuko mezu hutsa igortzearen ordez testua eta irudiak dituen MIME mezu bat bidaltz gero?

**[30]** Egin eza zu aurreko ariketan egindako telnet saioa, baina orain ESMTP protokoloa erabili zerbitzariarekin saioa hasteko, hau da, EHLO komandoa erabili HELO komandoaren

ordez. Horren erantzunean zerbitzariak onartzen dituen ESMTP gehigarriak zeintzuk diren adieraziko digu. Ingeleszko wikipedia erabili horietako gehigarri bakoitza zer den azaltzeko.

**[31]** Bilatu sarean *trickle* izeneko aplikazioari buruzko informazioa.

- [32]** Bilatu httping komandoari buruzko informazioa sarean, eta instalatu zure komputagailuan. Ondokoa egikaritu: http://www.ehu.es. Zer lortzen duzu?



## 5. Ilosgaike Arrietak

### 2. Arrietak

- DNS geldene bat

Maila	Protokoloa	Ide-untzilearen izena	Ide errenteko edukia
Aplikazioa	DNS	mezu	DNS geldera erantzun
garraioa	UDP	UDP datagrene	DNS mezu
IP	IP	Datagrene	UDP datagrene
Serbideak	Ethernet	frame	IP datagrene

- ICMP mezu

<del>garraioa</del>	ICMP	mezu	ICMP datubak
<del>garraioa</del>	Ethernet		ICMP mezu
Sorentzea	IP	Datagrene	IP datagrene
Serbideak	Ethernet	frame	

- ARP gelden

<del>garraioa</del>			ARP datubak
Sorentzea	ARP	mezu	ARP mezu
Serbideak	Ethernet	frame	

- HTTP ikonadu bat

Aplikazioa	HTTP	Mezu	HTTP ikonadu
garraioa	TCP	Segmento	HTTP mezu
Sorentzea	IP	Datagrene	TCP segmento
Serbideak	Ethernet	frame	IP datagrene

### 3. Arribeta

Gerbitzaria	Erregistro web	Izen	Belira
<del>www.zerbitzaria.org</del>	<del>A erregistro.</del>	<del>www.leso.org</del>	<del>@www.leso.org</del>
<del>TLD.org</del>	<del>NS erregistro</del>	<del>leso.org</del>	<del>dns-zone.leso.org</del>
<del>Giro zerbitzaria</del>	<del>Iregistrazio</del>	<del>dns-zone.leso.org</del>	<del>@dns-zone.giro.org</del>
	<del>dns zone</del>	<del>.org</del>	<del>@TLD.org</del>
	<del>A</del>	<del>TLD.org</del>	<del>@TLD.org</del>

### 5. Arribeta

- A) Zentrait aldeaketa egia da txikia, hoberen dns-zone.org-reko izena aldeaketa de bertsu dns-beberoketako ipn.com jartzea ibango litakorra.
- B) Ez da erreditik sortutako berdintso DNS zerbitzarien lehi gerelatu ogeker gaufigarrak eta hori es da aldeaketa.

### 6. Arribeta

Gerbitzaria	Erregistroa	Izena	Belira
<del>www.zerbitzaria.org</del>	<del>A</del>	<del>sacredtik.tle</del>	<del>@sacredtik.tle</del>
<del>correo.zerbitzaria</del>	<del>NS</del>	<del>.tle</del>	<del>dns.tle</del>
<del>correo.zerbitzaria</del>	<del>A</del>	<del>dns.tle</del>	<del>@dns.tle</del>
<del>www.zerbitzaria.org</del>	<del>NS</del>	<del>sacredtik.tle</del>	<del>dns.corpresa.com</del>
<del>dns.tle</del>	<del>A</del>	<del>dns.corpresa.com</del>	<del>@dns.corpresa.com</del>
<del>dns.tle</del>	<del>Correo</del>	<del>www.sacredtik.com</del>	<del>webdak.corpresa.com</del>
<del>dns.corpresa.com</del>	<del>A</del>	<del>webdak.corpresa.com</del>	<del>@corpresa.webdak.corpresa.com</del>
<del>dns.corpresa.com</del>	<del>MX</del>	<del>sacredtik.tle</del>	<del>smtp.sacredtik.tle</del>
<del>dns.corpresa.com</del>	<del>DNAME</del>	<del>sacredtik.tle</del>	<del>postdak.corpresa.tle</del>
<del>dns.corpresa.com</del>	<del>A</del>	<del>postdak.corpresa.tle</del>	<del>@postdak.corpresa.tle</del>
<del>dns.corpresa.com</del>	<del>NS</del>	<del>.com</del>	<del>dns.com</del>
<del>correo.zerbitzaria</del>	<del>A</del>	<del>dns.com</del>	<del>@dns.com</del>
<del>correo.zerbitzaria</del>	<del>NS</del>	<del>corpresa.com</del>	<del>dns.corpresa.com</del>
<del>dns.com</del>	<del>A</del>	<del>dns.corpresa.com</del>	<del>@dns.corpresa.com</del>
<del>dns.com</del>			

## 10. Ariketa

1. urratsa: lucia.mundu.net konputagailuak dus.mundu.net zerbitzarien eskuazio dio  
mail.mundu.net izane erabiltza esku. DNS protokoloa erabili.
2. urratsa: lucia.mundu.net bezeroak maeu eragaietik mail.mundu.net zerbitzarien  
Protokoloa: SMTP.
3. urratsa: mail.mundu.net erabiltza dus.mundu.net ibilgile.org ~~ez doigilean~~ MX erregistratua  
erabiltza esku. DNS zerbitzariak zera eta lurrerako IP helbidea  
Protokoloa: DNS
4. urratsa: mail.mundu.net zerbitzariak maeu biddleko dio post.planets.net zerbitzarien  
Protokoloa: SMTP
5. urratsa: hostzakile.berezoreo.com -du arretzakile post.planets.net zerbitzariaren berriroko  
izenea biddleko maeue itzuli. HTTP

## 11. Ariketa

Mota	Izena	Balioa
A	sarpost.geu.org	@sarpost.geu.org ] poste 1
CNAME	subptl.geu.org	post1.geu.org ] poste 1
CNAME	peopl.geu.org	post1.geu.org ] poste 1
CNAME	subtp2.geu.org	post2.geu.org ] poste 2
CNAME	post2.geu.org	post2.geu.org ] poste 2
MX	.geu.org	subptl.geu.org ] sarpost
A	post1.geu.org	@post1.geu.org ] poste 1
A	post2.geu.org	@post2.geu.org ] poste 2
NS	geu.org	dus.geu.org ] .org TLD zerbitzari
A	dus.geu.org	@dus.geu.org

## 12. Ariketa

Neiz da lehengo postea izan landa express.com, erabili ditzakego dute, edo  
betean, sotzuen diren postea berriak beraiz zahar honetako bideratua.  
Aurrelik erabiltza daude posible izango litakotela.

## 14. Arktete

1. Urteile: Vermischte unbekannte proxyweb.geu.org (Get www.zuek.org/index.html) es kann nicht geltend sein HTTP bilden.
2. Urteile: proxyweb.geu.org und die des geu.org unterri (www.zuek.org) DNS erlaubt egingo dia
3. Urteile: dns.geu.org unterri es ist Zeitarmeri (www.zuek.org) DNS gelde sein
4. Urteile: es ist Zeitarmeri dns.geu.org unterri org domenico TLD erla NS etc A erregistreit itolden sich
5. Urteile: dns.geu.org unterri.org unterri "www.zuek.org" DNS gelde egingo dia
6. Urteile TLD der dns.geu.org unterri www.zuek.org darinwo dogalize NS etc A erregistreit bueltan
7. Urteile: dns.geu.org unterri dns.zuek.org unterri (www.zuek.org) DNS gelde egingo dia
8. Urteile: dns.zuek.org unterri dns.geu.org unterri ~~es~~ CNAME etc A erregistreit itoldi
9. Urteile: dns.geu.org unterri proxyweb.geu.org unterri, CNAME etc A erregistreit itoldi
10. Urteile: proxyweb.geu.org unterri kmpoweb.zuek.org kmpoweb unterri Get index.html HTTP erlaubt egin
11. Urteile: kmpoweb.zuek.org unterri proxyweb.geu.org unterri index.html erlaubt itoldi HTTP erlaubt.
12. Urteile: proxyweb.geu.org unterri erlaubt unterri itoldi, HTTP bilden

## 15. Ariketa

web proxy 0'6

DNS berbitzari 0'5

}

$$\text{Dibore} = 0'5 \cdot 100\text{ms} + 0'5 \cdot 100\text{ms} + 0'6 \cdot 20\text{ms} + 0'4 \cdot 500\text{ms} = 267\text{ms}$$

web proxy 0'4

DNS berbitzari 0'9

$$\text{Dibore} = 0'9 \cdot 100\text{ms} + 0'1 \cdot 100\text{ms} + 0'4 \cdot 20\text{ms} + 0'6 \cdot 500\text{ms} = 327\text{ms}$$

Aldiz, orduera bideratzeko irango da lau de web proxyrenak berbitzarien.

## 16. Ariketa

- Eratzen den web berbitzarien zure jaitzi eguneko de, orduzkoak berbitzarien web proxyek eguneko beritu leu.
- ea de egingo berde-berdaren emaitza. Nahi izan eborra %80 jaitse eta ia %100
- trikila %80en gertutako litakile
- Dibore jaitzi eguneko de aurreko estatiko objektu berdine esleitzen badu, ibaien edo degiak lau berbitzarien gainetik dimentsioenarekin olearre izatea, eta beraz, deklargazio dibore berdingerak izan behar
- %80 trikitilak de ea berde berdin egiz berberak, eta ondorioz berdin aldatzeak hainbat gurdela de eta edo presio berre errepikatu behar izango.

## 36. Ariketa

A) Eratzen den Mx erregistro bat gehitzailea fakta da, non, lovek, lso.org  
Itena de poste.lso.org gurdela ditua, postortarietan egun den berdine

B.-1) ~~poste.lso.org~~ ~~schmeck-schmeck.lso.org~~ ~~schmeck~~

dns.hosting.com Mx ~~schmeck-schmeck.lso.org~~ poste.lso.org

A schmeck-schmeck.lso.org ~~schmeck-schmeck.lso.org~~

B.-2) Poste.lso.org denean ezer aldak berdintu bide erabili eta ia berdintu

b) Konfigurazio aldak berberak du, Maiztasu jeisteko berbitzarien iden

schmeck-schmeck.lso.org jarriz.

## 37. Arikete

Web zerbitzare  $\rightarrow$  www.mycomp.com iden., 100-130.one.com uduiven

Poste zerbitzare  $\rightarrow$  100-130.one.com uduinde,  $\rightarrow$  poste atitache subp.mycomp.com  
jesotzelo, imcp.mycomp.com

Ubededderdo dust.one.com  $\Rightarrow$  198.51.80.3

Erregistro gurtien beste kopia bet  $\rightarrow$  dus2.one.com  $\Rightarrow$  198.51.80.4

100-130.one.com uduivera IP uduido. 198.51.100.130

DNS. isp.com eschili MFP bidet.

a)

i. .com TLD zerbitzaren

TLD.com	NS	www.mycomp.com	dust.one.com
	A	dust.one.com	198.51.80.3

dust.one.com	CNAME	subp.mycomp.com	100-130.one.com
	A	100-130.one.com	198.51.100.130

CNAME	imcp.mycomp.com	100-130.one.com
-------	-----------------	-----------------

Mx	Mycomp.com	subp.mycomp.com
CNAME	www.mycomp.com	100-130.one.com

TLD.com	NS	www.mycomp.com, .	dus2.one.com
---------	----	-------------------	--------------

	A	dus2.one.com	198.51.80.4
--	---	--------------	-------------

NS	one.com	dust.one.com
----	---------	--------------

NS	one.com	dus2.one.com
----	---------	--------------

Urratse	Nork	Nori	Galdere/erantzunen edukia
1. urrats,	nabitxileak	ebaleari	www.mycomp.com
2	ebaleak	DNS.isp.com	www.mycomp.com
3	DNS.isp.com	error	www.mycomp.com
4	error	DNS.isp.com	NS, www.com - tLD.com
5	DNS.isp.com	TLD.com	www.mycomp.com
6	TLD.com	DNS.isp.com	NS, mycomp.com dust.one.com
7	te DNS.isp.com	dust.one.com	NS, mycomp.com dus2.one.com
8	dust.one.com	DNS.isp.com	NS CNAME www.mycomp.com 100.130.one.com
9	DNS.isp.com	ebaleari	A 100.130.one.com 198.51.60.130
10	ebaleak	nabitxileari	198.51.100.130

Konfigurazioa egiteko argotako parte berbitzarrak (snmp.mycomp.com) eta jasotako berbitzarrak (imep, sntp, com). Konfiguratu behar portuak ezarri behar diren de arritzaikak eta portutik zelotu.



## 6. ikasgaiko ariketak

### Lehenergo zatia-suhesia eta mugasarea

**1** Bedi Internetekin lotuta dagoen sare bat, ondoko zerbitzu hauek eskaintzen dituena:

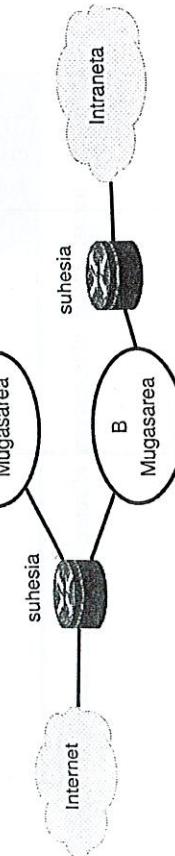
- Web zerbitzuak:
  - Intraneteko erabilzaileentzako soilik atzigarriak diren informazioa eta web aplikazioak.
  - Interneteko atzigarriak diren informazioa eta web aplikazioak.
  - Intraneteko erabilzaileentzako sartidea Interneten dauden web zerbitzariak azitzeko.
  - Interneteko edozein erabilzailearekin posta elektronikoa elkar bidaletzea, gure sareko POP3 eta SMTP zerbitzariak erabiliz.
  - SIP telefonia zerbitzua intraneteko erabilzaileentzako, gure sare barruko eta kanpolo beste erabilzaileentzako hitz egin ahal izateko.
  - Internetek intraneterako sartidea, baimendutako erabilzaileentzako.
  - DNS zerbitzua:
    - Intranetako konputagailuen DNS eremuko jatorrizko DNS ebazpena, Internet osoari eskainita.
    - DNS ebazpena, intraneteko erabilzaileei solik emanda.

Sare-eskema bat marratzu ezazu, intraneta, Internet, behar diren mugasareak, eta goian zerrerdatutako zerbitzu guztia gauzatzeko beharko diren zerbitzariak kokatu. Ondoko hauek kontuan izan:

- Sareko segurtasuna lehentasuneko helburua da.
- Intraneteko erabilzaileek atzizten dituzten web orriak iragazi behar dira.
- Sartzen eta ateratzet den posta elektronikoa iragazko duen posta-pasabide bat erabilikoa da.

**2** Bedi irudiko sarea. Ondoko zerrendako makina bakoitzak inidiko zein azpisarean kokatu behar den adierazi:

Web proxya. *(B) mungo sareen suhesia, A mungo sareen suhesia*  
 POP zerbitzaria. *B mungo sareen suhesia, A mungo sareen suhesia*  
 NAT zerbitzaria. *B mungo sareen suhesia, A mungo sareen suhesia*  
 VPN zerbitzaria. *B mungo sareen suhesia, A mungo sareen suhesia*  
 Barrutiko web zerbitzaria. *B mungo sareen suhesia, A mungo sareen suhesia*  
 Kompakto web zerbitzaria. *B mungo sareen suhesia, A mungo sareen suhesia*  
 Posta pasabidea. *B mungo sareen suhesia, A mungo sareen suhesia*  
 SMTP zerbitzaria. *B mungo sareen suhesia, A mungo sareen suhesia*



**3** Ondoko iragazki-taula suhesia batena da. Aztertu eta esan zein kanpolo trafikoak zeharkatu du suhesia, taula horren arabera. Taulan agertzen diren helbideen esleipena ondoko da:

- 192.168.1.0/24 --> suhesiak babesten duen sarearen helbidea (irudian maskara falta zaio);
- 192.168.1.1 --> suhesiaren barruko helbidea;
- 192.168.1.2 --> posta-zerbitzaria;
- 192.168.1.3 --> web zerbitzaria.

Oharra: agertzen diren portuak TCP portuak dira.

Ondoko bi kasu haueretako eman erantzuna: 1) suhesiarena Linux makina batetik egiten du, ip tables erabiliz eta besterik ezeko aukerarik inongo katean definitu gabe, 2) suhesiarena CISCO makina batetik egiten du, ACL erabiliz.

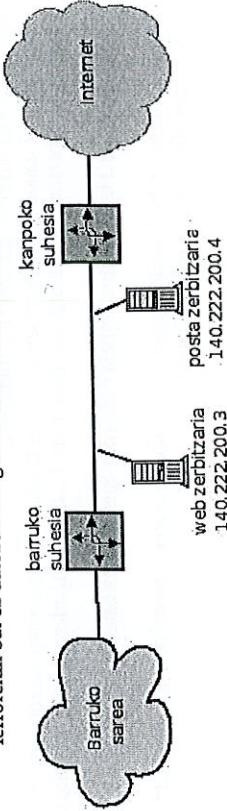
Source Address	Source Port	Destination Address	Destination Port	Action	Description
1 Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet
2 192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
3 Any	Any	192.168.1.1	Any	Deny	Prevent External users from directly accessing the Firewall system.
4 192.168.1.0	Any	Any	Any	Allow	Internal Users can access External services
5 Any	Any	192.168.1.2	SMTP	Allow	Allow External Users to send email in
*	Any	192.168.1.3	HTTP	Allow	Allow External Users to access WWW server

**4** Bedi irudiko sarea. Internetetik barruko sarean sartzeko mugasare bat dago. Egin ezazu mugasareko kanpolo suhesiaren bibrildalketen iragazki talde, ondoko zutabe hauek izango dituena:

jatorrizko @IP	jatorrizko portua	heburuko @IP	heburuko portua	Onartu/baztertu

Ondoko hauek kontuan hartu:

- Sareko segurtasun arauak ez dute onartzan barruko sareko inongo makinatik.
- Internetea aterazea.
- Posta zerbitzariak bera bezalako beste SMTP zerbitzarietik besterik ez diu harremanak egingo, beti TCP portuen artean.
- Web zerbitzariak TCP 80. portuaren bidetx emango du zerbitzua.
- Espirituik adierazi zein den besterik ezean egin behar dena, hau da, taulako inongo lerrorekin bat ez datozen datagranei ezarri behar zaiena.



- 5** Demagun unibertsitate baten sare-arduraduna zarela. Unibertsitate hori hiru campus desberdinietan dago kokatuta, eta campus bakoitzak bere sare propria du. Beraren arteko komunikazioak Interneten bidez burutuko dira, VPN teknologia erabiliz. Beraz, campus bakoitzak badu bere Interneteko konexio propioa. Sare-zerbitzu garrantzitsuenak horrela daude antolaturik:
- Web zerbitzu: Unibertsitatetik kampo atzizteko zerbitzari bat dago, campusetako batean. Campus zentral horretan, baita beste konputagailu batean intranetarako web zerbitzaria ere badago. Unibertsitateko saretek kaporako web sarrerentzako proxy web bana dago campus bakoitzean.
  - Posta zerbitzua: Campus bakoitzak badu bere bertako SMTP zerbitzaria. Posta hartzeko, unibertsitate osorako pasabide bakarra dago, 25 portuan Interneten datorren posta hartzen duena. Posta hori gero banatuko du campus bakoitzean dauden DNS bertako zerbitzari bana dago, campus bakoitzeko ebazleen erabilten dutena.
  - Campus bakoitzean DHCP zerbitzaria dago.
  - NAI zerbitza ere ematen da campus bakoitzean.

Unibertsitateko sareko topología definitu eskema baten bidez, segurtasunaren ikuspean. Beharrezkoak diren mugasareak zehaztu, baita aipautako zerbitzuak ematen dituzten zerbitzarien koparea ere.

#### **Bizarreren zinarioa: aplikazio seguruntza**

- 6** Gako publikoko zifratze-sistema batean, posible al da M mezua ondoko eskema jarraituz zifratuta bidatzea A erabiltaile batek B erabiltaileari (ez dira gako-filtraziorik egon)?

Pub\_B(Pub\_A(E<sub>ZK</sub>(A(E<sub>ZK</sub>\_B(M))))

Baiezkotan, zer bidali dugu? Ezezkotan, Zergatik?

- 7** Demagun saio baterako gako simetrikoa ezartzeko garaien, ondoko gako publikoko zifratze-teknikenetan oinarritutako prozedura erabilten dugula: komunikazioaren muturren batek (A-k) gako simetriko berri bat sortu, hau zifratu (bere gako ezkutuarekin) eta honen emaitza beste muturrekoaren (B-ren) gako publikoarekin berriro zifratu eta, azkanean, beste aldera bidali egiten du. A eta B-en artean inongo harremanik ez badago saio segurua ezarri baino lehen, zer arazo praktikoa du deskribatutako protokoloak?

- 8** Demagun A bidalzaileak M mezua ondoko eskema jarraituz bidaltzen duela:

[E<sub>A</sub>(M), Aren identifikazio]

Hau da, mezua zifratzen du igorlearen gako ezkutuarekin, eta igorlearen identifikazioarekin batera igortzen du zifratutakoa.

- Bermatuta al daude komunikazioaren konfidentzialtasuna, igorlearen kautasuna, eta mezuaren osotasuna, eta ukorik ez, baldin eta harzalek igorlearen gako publikoa badu?
- Alderatu sistema hau sinadura digitala erabilten duen sistema batekin.

- 9** Bi kideen arteko saio baterako gako simetrikoa ezartzeko protokolo bat diseinatu. Ziurtaginetan oinarritu zure protokolo hori.

**10** SSL oso erabilia da Interneten bidezko erosketa elektronikoetan. Bibliografiaren begiratu zelituzk diren SSL-k ematen dituen urratsak saio segurua ezarzteko bi aldene arrean. Normalean, komunikazioari hasiera ematen dionak (arakatzaileak) denda birtualeko zerbitzariari inongo ziurtagintzik ez diola aurkeztu suposatzen duen protokoloaren berriro erabilten da Interneten. Zer ergaina du arakatzaileak ziurtagintzik ez aurkezteak bion arteko komunikazioaren segurtasunengana? Erantzuna ematean, banan-banan aztertu komunikazio segunaren hitu alde bakoitzia.

#### **Aldarea (12ekai)**

Aplikazio protokolo bat ari gara diseinatzen. Komunikazioaren segurtasuna bermatu behar dugu, eta, beraz, A eta B erabiltaileen arteko informazioa trukatzen hasi baino lehenago, conexio segurua ezarri beharko dugu bi muturren artean. Horretarako ziurragintzik digitalak erabiliko ditugu, eta ondoko procedura hau definitu dugu aplikazio mailan conexio seguna ezartzeko:

- 1) A-k B-ri Ziurt(A) bidaltzen dio.
- 2) B-k  $\beta$  saio honetarako gako simetrikoa sortzen du.
- 3) B-k A-ri Pub\_A( $\beta$ ) bidaltzaen dio.

Une honetatik aurrera conexioa ezarrita dago, eta dena  $\beta$  gako simetrikoaz zifratuta bidaliko diote elkartu.

Aztertu ezazu ea bermatzan den komunikazio segunaren ezaugartia bakoitza.

- 11** Demagun zure arakatzailean ondoko weborria duzula:

Eta url-ren ondoan duzun giltzarrapoan klikatz, beste informazio hau eskuratu duzula:

[gestion-servicios.ehu.es](http://gestion-servicios.ehu.es)  
The identity of this website has been verified  
by TERENA SSL CA.  
Certificate information

Your connection to question-services, eh? Es ist eine Verbindung zu den Dienstleistungen, die Sie benötigen.

卷之三

The connection is encrypted using AES\_256\_CBC, with SHA1 for message authentication and DHE\_RSA as the key.

The server does not support the TLS

### Site information

卷之三

zen duen erabiltzaile izena eta dagoki

urerrera egin duzu.  
ori guztia ikusita, ondoko galderak erantzun eta zure erantzun guztien zergatziak

- zatu:

  - i) Zer geratuko zen, gure arakatzaileak izan ez balu aurrekargatuta TERENA SSL CA erakundeari dagokion ziurtagiria?
  - ii) Bermatuta al dago zerbitzari honekiko komunikazioaren konfidentzialtasuna?
  - iii) Bermatuta al dago komunikazioaren parteidean noratasuna zein den?
  - iv) Bermatuta al dago komunikazioan elkar trukatuako mezuin osotasuna?
  - v) Demagun baduzu zerbitzari honek onartzen duen ziurtagiri elektroniko bat dibidizet, txartel batean). Zertan aldatzten dira (b), (c) eta (d) erantzunak? Beharrezkoak ziztazteke kasu horretan erabilizalea+pasahitza zerbitzariari bidaliza?

[12] Kriptografia asimetrikoa erabiliz, badago M mezu baten ko

- hartzalearen (demagun B dela hartzaila hori) gako publiko alde batetik, igorlearen nortasuna (bedi A) kautotu daitetik maziferatu. Horretan oinarriturik, komunitateko baten konfiderentzia

ermatzeko ondoko zifraze-seskema proposatu dugu:  
[Pub B(M), E&K A(M)]

- Arazoren bat ikusten al diazu sistema honi? Gako  
informatiboaren arabera, **azkena** batzuk  
ondoko galderak erantzun:

**[3] Demagun ziurtagi digitalak erabilten dituen aplikazio seguru bat ari zarela sortzen.**  
Idatzerazu denerolokoda erahiliz, ziurtari bat egindako orribilko durreratik  
B. Arazoren bat ikusten badiozo, nola konpondu zenuke?  
C. Osatu eskema meznaren osotasuna eta ukoezintasuna ere bermatzearen.

14) Zintagiajik ian kirzeke weh anilizis bat sohi kebar duu; Daus

**14) Ziuratgiria jaunbateko web aplikazio bat sortu behar duzu. Bere funtzionamendua honakoak izango da:**

- SSL saioa ezarriko dute erabiltailearen arakatzailea eta zerbitzariaren artean. SSL saio ezartzaileak, Web zerbitzariak aurkeztuko dio arakatzaleari bere ziurtagiria. Erabiltaileari ez zait eskaerak inongo ziurtagiria.
- Zerbitzariak erabiltailearekin ziurtagiria ematen behar dituen moduak zehaztu.

- dizkio.*

  - Datu horiek jaso eta gero, zerbitzariak erabiliztalearnako gako pare bat [publikoarezkutua] sortuko du, ziurtagiria sortu eta sinatuko du, honen kopia gordeko du bere datu-basean, eta bidaliko dio [gako\_exkutua, ziurtaginak] bikotea erabilitzaleari.

Adierazi zergatik horrela jauktutako ziurtagiri bat ezin da onartu komunikazio seguru bat ezartzeko, edozein izanda sinatzalea.

**15)** A bezeroa era B zerbitzariaren artean saio segurua ezartzeko protokolo bat definitu behar da. Ideia konfidentzialtasuna bermatuko duen gako simetriko bat ezaugarri izango da, gero gako simetriko hori erabiliz erabiltzailearen izena eta pasahitza bidaltzeko. Definitutako protokoloa honako hau da:

1. A-k B-ri  $\alpha$  ausazko zenbakia bidaliko dio.
  2. B-k bere ziurtagiria itzulikio dio.
  3. A-k bigartean ausazko zenbakia bat,  $\beta$ , bidaliko du, baina orain B-ren gako publikoaz zifratuta.
  4. A-k era B-k protokoloak ezarritako kalkuluaren egindo dute  $\alpha$  eta  $\beta$  zenbakietatik abiatuta gako simetrikoa lortzeko.
  5. A-k bere erabilizalearen izena era pasahitza bidalikio du, ezarritako gako simetrikoaz zifratuta.

A) Demostratu ezazu protokolo hau ahula dela errepikapen erasoen aurtean.

B) Protokoloa aldatu, errepikapen-erasoei aurre egin ahal izateko.

**16** Egin ezazu PGPrekin zifratutako jatorrizko mezu berreskuratzeko urratsez prozeduraren eskema.

**[17]** Demagun zure bikotea Australiara joan dela urtebeteko, eta berarekin komunikatzeko posta elektronikoa erabilten duzula. Komunikazioaren segurtasuna bermatzeko PGP erabilten duzu, baina zure bikotea maietmindi nahi duen lagun batet zure bikotearen gako ezkutua lortu du. Bere asmoa zure norutasuna ordetzatzea da, zure izenaren mezua iraingariak zure bikoteari bidaltzeko zuen arteko harremana mintzea lortu arte. Lortuko aldu?

- [18] Demagun aurreko arketako zure etsaiak zuk bidalitako mezu bat atzematen duela, irakurun duela (badu hori egingo, zure bikotearen gako ezikutua baitu) eta edukia aldatzen duela. Nola atzemanago zuen zure bikoteak aldatxeta?

**[19]** Aurreko arriketan gertantakoaren ondorioz, zer edo zer arrarao sumatten hasi zarete, era zure bikoteari gakoak aldatzea proposatzen diozu. Posta elektronikoarekin errezeloak dituztenez, gako publiko berriak elkar bideratzeko posta arrunta erabiliztea adostu duzue. Bainaz zure etsaiak horren guztiaren gainean dago, eta zure anizoko postaria, joktu-zortek itxita dagoen fundamentalurik gabeko laguna, sobormatu egin du zuik igortziako era jasotako

- posta zuri pasatzeko. Horrela, trukatutako gako publikoak ordezkatu diu.
- Deskrribatu ezazu sortutako egoera: nolako mezuak, irakurgarriak ala ez, jasoko dituzue zuek biok?
- Beharrezko al zen PCP posta ez erabiltzea gako publiko berriak bidaltzeko? Zergatik?

- 20**) Suposa dezagun postaria onartzen dueña sobornoa, eta zure lehiakideari ematen dizkio zuen posta, baina gero ez ditu ordezkatzuen gako publikoak zure aurkariak emandako gako fartsuekin. Zertan aidatzan da aurreko egoera?

- 21**) (13-5)A eta B erakundeek agiria trukatu nahi dituzte era seguruan Internet erabiliz, posta elektronikoaren bidez. Ez dute ziurtagiria erabili nahi, eta, horren ordez, beren gako publikoak elkarri eman diote.

- Ba al dure agiria era seguruan elkarri bidaltzea eskuragarri dagoen softwarea erabiliz, edo horretarako softwarea garatu beharko dute?
- Edozein kasua izanda (softwarea garatu edo dagoena erabili):
  - azaldu nolakoa izango den M agiri bat bidaltzeko eta jasotzeko procedura, konfidentialtasuna besterik ez bermatua.
  - azaldu nolakoa izango den M agiri bat bidaltzeko eta jasotzeko procedura,
  - osotasuna eta kautotasuna bermatuz.
- Beste erakunde askorekin duten harremanetarako zabaldu nahi bada sistema hau, arazoren ikusten al diazu?

- 22) AUTOEBALUAZIOA.** Ondoko akronimoak eta terminoak loru dagokion definizioarekin.

Simadura digitala	802.11i	Kriptografia simetrikoa
Posta pasabidea	Barroko mugasarea	WEP
Kriptografia	Kerberos	Konfidentialtasuna
Mugasarea	Gotorlekua (Bastion)	Gako-zerbitzaria
IPsec	TLS/SSL	X.509
Intraneta	Kanpoko mugasarea	Kautozea
Ziurtagiri digitala	VPN	Kriptografia asimetrikoa
Suhesia	Extranet	HTTPS
WPA2	WPS	Osoasuna
Ukonik ez	Diffe-Hellman	

(1) Erasoetako bereziki babesu behar diren zerbitzariak dituen sare lokala.

(2) Bi sareen arteko trafikoa iragazten duen makina.

(3) Saretuk etor daitekeen erasoetako sareko makientzako atzigarriak dauden zerbitzaria. Onartutako mezuak beste posta zerbitzariei bithitzen die, hauek erabiltzei helarazteko.

(4) Kanpoko SMTP zerbitzarietako jasotako mezuak iragazten duen posta zerbitzaria. Onartutako mezuak beste posta zerbitzariei bithitzen die, hauek erabiltzei helarazteko.

(5) Kanpoko makientzako atzigarriak egongo diren zerbitzariak dituen mugasarea.

(6) Soilik gure barruko sareko makientzako atzigarriak dauden zerbitzarian dituen mugasarea.

(7) Kanpoko erabiliztaleeneko sareko makientzako atzigarriak dauden zerbitzaria. Kanpoko erabiliztaleeneko sareko makientzako atzigarriak dauden zerbitzaria. Kanpoko erabiliztaleeneko sareko makientzako atzigarriak dauden zerbitzaria. Kanpoko erabiliztaleeneko sareko makientzako atzigarriak dauden zerbitzaria.

(8) Kanpoko batzuentzako era kontrolatuun irekita dagoen intranet batzen zatia.

(9) Trukatuako informazioa soilik igorleak eta hartzaleak ezagutzen dutela bermatzen duen komunikazioaren ezzagaria.

(10) Komunikazio batean, beste aldearen nortasuna bermatzea.

(11) Trukatuako informazioa igorleik hartzaileraino bidean ez dela aldatu bermatzen duen komunikazioaren ezzagaria.

## ARIKETA PRAKTIKOAK

Ondoko ariketa hauek egiteko Ubuntu instalatuta duen konputagailu bat behar duzu. Batzuetarako, gainera, sare-konexioa behar da. Ariketa batzuk beste sistema askotan ere egin daitezke. Ariketetan erabilizten den softwarea ez baduzu, instalatu beharko duzu.

- 23)** Emaitza zuen begirada bat zure arakatzaileen aurrekargatuta dituzun ziurtagiri jaulkitzaileen ziurtagiri zerrrendan. Nork sinatzen ditu jaulkitzaile horien ziurtagiria?

- 24)** Zure fixategi bat zifratu eta desifratu era simetrikoan. gpg softwarea erabiliz. GPG erabilera bunuzko informazioa lortzeko, egin 'man gpg' edo Interneten bilatu tutorialen bat.

- 25)** Sortu gako pare bat (ezkutua eta pribatua), gpg softwarea erabiliz.

- Igorleak mezu bat igori duela ukaezina dela bermatzen duen komunikazioaren ezzagaria.
- Informazioaren konfidentialtasuna bermatzeko zifratez-tekniken azterketa eta erabilera.
- Zifratzeko eta deszifratzeko gako bera erabilizten duen kriptografia.
- Zifratzeko eta deszifratzeko gako desberdinak erabilizten dituen kriptografia.
- Gako simetrikoak banatzeko sistema bat, gako-sorbiziari batzen oinarriuta.
- Komunikazio-sailo baterako gako bera erabiliz, gako simetrikoak adosteko algoritmo bat, gakoaren konfidentialtasuna bermatzen duena.
- Mezu baten osotasuna eta ukorik ez bermatzen duen teknika.
- Konfiantzako norbaitek digitalki sinatuak agiri bat.
- Gako publikoak banatzeko ziurragiri digitalen formatu estandarra.
- Ziurtagirietan oinarritutako saio segunak ezarteko protokoloa.
- TLS/SSL protokoloak erabilizten duen HTTPren aldaera.
- Internet bidez egindako sare pribatu batzen azpisareen arteko komunikazioaren segurtasuna bermatzen duen teknika, tunel zifratuetan oinarrituta.
- IP datagramen segurtasuna bermatzeko estandarra.
- Seguna ez den wifi sareen komunikazioetarako estandar bat.
- 802.11i estandarren implementazioa.
- Wifi sareen komunikazioaren segurtasuna bermatzen duen estandarra.
- 802.11i estandarren implementazio aksasdun bat, seguna ez dena.

## Teoria aplikatua: ariketak (4, 5, 6 gaiak).

### 1. ariketa (3 puntu)

Ainara Internet bidezko TB hornitzalle baten bezero da (ITVP). Honetaz aparte Internetera atzipena ematen dion ISP baten bezero da. ITVP TB hornitzaleak 3 zerbitzu maila eskaintzen ditu: urezkoia (irudi eta soinu maila bikaina, 8 Mb/s behar ditu), zilarrezkoia (kalitate ona, 4 Mb/s) eta bronzezkoia (kalitate estandarra, 2 Mb/s). Bere ADSL konexioa 20 Mb/s-koa denez, Ainarak urezko maila erabili abalizatea espero du. Hala ere, TB soiliak brontzeko mailan ikusteko gai da.

Zuk, laster informatikan ingeniarria izango zarenetz, Ainaran komputagailuak TCP konexioetan 64 KiB-eko (64\*1024 byte) jasotze buffera erabilten ari dela egiaztatzen duzu. Ondoren, ping erabiliz, konturatzun zara paketeen joan-etorriko denbora (RTT) 200 ms-takoa dela. ISPA harremanetan ari denez, ITPV hornitzairearekin konektibitatea hobetzeko hurengoko taula prestatu nahi duzu. Taulan zehaztuko duzu Ainarak TB kaltitate maila ezberdinaren ikusleko joan-etorriko denborak (RTT) izan beharko lituzkeen mugako balioak.

Balio honeratikgora	-	Ezin da TB ikusi
Balio hauen artean		Ainarak TB brontzezko kaltitatean ikusi ahalko du
Balio hauen artean		Ainarak TB brontzezko edo zilarrezko kaltitatean ikusi ahalko du
Balio honeratikbehera	-	Ainarak TB nahia duen kaltitatean ikusi ahalko du

### 2. ariketa (4 puntu)

Goi mailako “.myself” domeinua (TLD) kudeatuz negozioa egin nahi duzu, horretarako “John Doe myself” edo “peter.parker.myself” bezalako domeinua salduz. Zure bezeroek beraiek kudeatuko dituzte beraien zerbitzarriak (jatorrizko DNS zerbitzarriak, web, e-posta eta abar). Negozioa martxan jaritzeko ICANN-en baimena lortu duzu. Ez dituzunetan ikusgai zerbitzari propioiak kudeatutu nahi, beste enpresta bateko bi erabililiko dituzu ds33.irondns.com (198.51.100.33) eta ds34.irondns.com (198.51.100.34). Dagoeneko erro zerbitzariak ezarpen hauen ezagun dira.

- Adieraz ezazu zein informazio eman beharko ditzuten zure bezeroek “.bezeroa.myself” bezalako izen bat erabili abaliz izan dezaten.
- Adieraz ezazu zein DNS erregistro (RR) gehitu beharko duzun zure zerbitzarietan “.bezeroa.myself” bezalako domeinu bat Interneten ikusgai egon dadin.
- Azal ezazu zein konfigurazio gehitu beharko den www.bezeroa.myself bezalako web zerbitzari bat Interneten ikusgai egon dadin. Argi eta garbi adierazi zer gehitu beharko den, **zein zerbitzarietan eta a norrk** egin beharko duen.
- Azal ezazu adibidea@bezeroa.myself bezalako e-posta helbideak abalizatuko zer egin beharko den DNS eta e-posta zerbitzarietik dagokienet.

### 3. ariketa (3 puntu)

Izenpeko emandako txartel bat (smartcard) dantuk. Txartel horrek ziurtagiri bat dantza, beste gauza batzuen artean, nire izena, NAN zenbakia eta e-posta helbidea dantza. Txartelak gaitu ezkutu (privatu) bat ere badauka, baina arazoa da Izenpeko txartelarekin batera eman zidan PIN-a ez dudala gogoratzen.

Ziurtagiriaren baliozko epea oraindik amaitu ez dela zuri bagaudet:

- HTTPS zerbitzari batera, adibidez nire bankukora, konekta al naiteke ziurtagiria erabiliz nire identitatea autentifikatzeko (kautzoteko)?
- Erabilgarria al da ziurtagiri hau bankuaren identitatea autentifikatzeko?
- Onartutako beste edozein biderez bitartez autentifikatzea lortzen badut (eta beraz, ziurtagiria baliozatzea), ziurtatu al dezerake bankuak nire e-posta helbidea zein den?

- Bidali al diezadakoe bankuak zifratutako mezurik? (mezu irakurtzeko gai izan beharko naizi.)
- Zein paper jokatzen du Izenpeko (zertaz arduratzen da)?

Paper zaharreran bila ibili ondoren txartelaren PINa aurkitu dut. Esan didatenez, horrekin txartela erabili ahal izango dut dokumentuak sinatzeko. PINa beste inork ezagutzen ez duelu zuri bagaudet:

- HTTPS zerbitzari batera, adibidez nire bankukora, konekta al naiteke txartela era PINa erabiliz nire identitatea autentifikatzeko (kautzoteko)?
- Bidali al diezadakoe bankuak zifratutako mezurik? (mezu irakurtzeko gai izan beharko naizi.)
- Zer gertatuko da norbaitek txartela lapurtzen badit? Axola al du txartelaren atzealdean nire PINa idatziz badute erronulagaiu batekin?



## 6. Añade

B) wujojosecc

we pexya

ATP serbi:tam

Bertho Dus Zerbi:tam

UPU Berbi:tam

MAT

PDP zafib:tar:

ATP zafib:tar:

Burrova we serbi:tam

Lokk Postabuse

Upplo we serbi:tam

Bemtho jdmvane Dus serbi:tam

PDP zafib:tar:

ATP zafib:tar:

ATP zafib:tar:

## 4. Añade

Józefino QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

QDP idemílico para llevarte ATP llevarte para Ocio/Break

cooperación entre las autoridades de policía y las autoridades de justicia

## 7. Añade

que publica ordenes en la que tiene que ver con el

Acuerdos entre países en la que tienen que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

## 8. Añade

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el

que publica ordenes en la que tiene que ver con el



28. Aciu

