2

SAREAK ELKARREKIN KONEKTATZEA

Kapitulu honetan ondoko hauek aztertuko dira:

- Sarearte batean sortzen diren arazoak zeintzuk diren.
- Zeintzuk diren IP protokoloaren eta Interneteko sarearte-mailaren ezaugarri nagusiak.
- Nolakoak diren IP helbideak. Zertarako eta nola erabiltzen diren IP maskarak.
- Nola bideratzen diren datagramak sareartean zehar: Nolakoak dira bideratze-taulak, nola betetzen diren, nola eguneratzen diren, eta nola erabiltzen diren.
- Zer den eta zertarako erabiltzen diren ARP taulak.
- Zer den eta zertarako erabiltzen den ICMP protokoloa.
- Zer den IPv6.

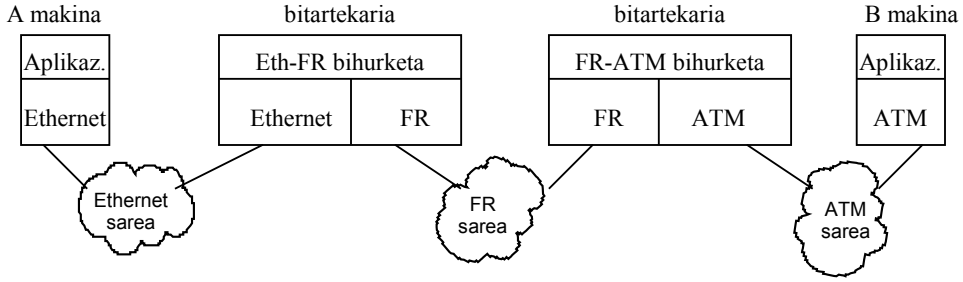
Konputagailuak elkarrekin konektatzeko sareak mota askotakoak izan daitezke. Eremu lokalean, Ethernet da nagusi, baina beste teknologia batzuk ere badaude (Token Ring, adibidez). Eremu zabaleko komunikazioetan ere, badaude aukera teknologiko anitz aurreko kapituluaren azken sare-arkitekturaren (hiru mailakoa) bigarren mailari dagokionez. Erabilienak ATM eta Frame Relay dira. Sare horietako bakoitzak bere arkitektura du, non maila fisikoa eta sarbide-maila ezberdinak diren.

Kapitulu honetan sare ezberdinetan konektaturik dauden makinak elkarrekin nola komunikatu ikusiko dugu.

1 Sare ezberdinak elkarrekin konektatzea

Lehenengo urratsa bi sareen artean konexio fisikoa ezartzea da, bi sareekiko konexioa duen ekipoa jartzea, alegia. Ekipo bitartekari horrek bi sare-txartela izan beharko ditu, bata sare batentzat eta bestea beste sarearekin konektatzeko. Beraz, bitartekariak sare-arkitektura bikoitza izan beharko du, bi sareetan zehar transmititu ahal izateko, eta, gainera, bi arkitektura horien arteko bihurketa egiteko gai izan behar du. Hori guztia 2.1 irudian ikus daiteke, non hiru sare ditugun, bat ATM, bestea Frame Relay, eta hirugarrena Ethernet, eta sare horiek elkarri konektatzeko bi bitartekari daude. Elkarrekin konektaturik dauden horrelako sare-multzoei **sarearteak** esango diegu.

Sareartea: sare heterogeneoek osatutako konputagailu-sarea. Sarearteetan mota guztietako sareak egon daitezke: sare lokalak zein eremu zabaleko sareak, teknologia eta sare-arkitektura ezberdinetan oinarrituta.



2.1 irudia: Sare ezberdinak elkarrekin konektatzea.

Irudiko Ethernet sarean dagoen A makinak bidalitako aplikazioko komando bat ATM sarean dagoen B makinaraino heltzeko, bi bitartekariak zeharkatu behar dira. Lehenengo bitartekariak Ethernet trama jaso, hortik komandoa erauzi, FR trama berri batean sartu, eta beste bitartekariari bidali beharko dio. Bigarren bitartekariak antzeko lana du: FR trama jaso, komandoa hortik atera, ATM zeluletan sartu (horrela deitzen dira ATM sareen paketeak), eta B makinari bidali ATM sarean zehar.

Ondoko animazio honetan aplikazio-mailako informazioaren gorabeherak ikus daitezke 2.1 irudiko sareetan zehar.

2.1 irudian aurkeztutako irtenbidea posiblea bada, baina ez egokia. Ondoko oztopo hauek ditu:

- Sare-bikote bakoitzeko bitartekari berezia diseinatu eta ekoiztu behar da, bakoitzak bi bihurketa egiteko gaitasunarekin. Merkatuan N sare-mota ezberdinak baditugu, Nx(N-1) bihurketa egiteko gai diren bitartekariak ekoiztu beharko dira elkarrekiko konexio unibertsala bermatzeko. Hori ekipo ezberdin gehiegi dira: mota bakoitzetik ale gutxiegi ekoiztuko litzateke prezio onean merkaturatzeko, eta kudeatzeko orduan berezitasun eta elkarren arteko alde gehiegi izango lituzkete.

- Normalean ezingo da tramaren formatu batean dagoen kontrol-informazio guztia (goiburukoak, alegia) beste formatuan bihurtu, ezta bidaltzeko prozedurak ondo bete ere. Adibidez: sare batzuetan hartzaileak igorritako tramaren onespena itzuli behar dio igorleari, errore-zuzenketa egiten baita; baina hartzailea beste sare-mota batean kokatzen bada, errore-zuzenketarik egiten ez duen sare batean, nork itzuliko dio igorleari transmisioan aurrera egiteko behar den onespena? Bitartekari batek egiten badu, ez dugu bermatzen benetan hartzaileak trama ondo hartu duen, izan ere, gerta liteke bitartekariak onespena bidali eta ondoren, bere bideko hurrengo sare bat zeharkatzean, trama matxuratzea.
-
- Bitartekari bakoitzak helbideak itzultzeko taula erraldoiak beharko lituzke. Sare-mota guztietako helbideak beste sare guztietako helbideetan bihurtzeko gaitasuna izan behar du. Hori ez da bideragarria eta, praktikan, eskema horri jarraituz ezingo dira mota guztietako sareak elkarrekin konektatu.

■ Sistema irekiak

Aurreko guztiagatik aspaldi hasi zen benetan unibertsala izan behar zuen beste irtenbide baten bilaketa. Orduan agertu zen **sistema irekien** kontzeptua, sistema itxiaren kontzeptuaren kontra sortutako ideia. Sistema itxiak orain arte ezagutu ditugun sare-arkitekturak dira: bakarrik sare-teknologia bera erabiltzen dituzten konputagailuak elkarrekin konektatzeko balio dutenak. Horren adibideak IBMren SNA sareak, Digitalen DECnet sareak, konpainia telefonikoek sortutako X.25 sareak edo Novellen Netware sareak dira. Sistema ireki bat, aldiz, edozein teknologiatan oinarritutako sareak elkarrekin konektatzeko balio behar duena da, sarearte heterogeneoak eraikitzeko, alegia.

Sistema ireki bat beste edozein sarerekin konekta daitekeen konputagailu-sarea da.

Sistema irekien oinarriak sare-arkitektura bat izan behar du. Sare-arkitektura horrek beste arkitektura guztiak integratu behar ditu, elkarren arteko konexioa bermatzeko. Horixe da ikastaro honi izenburua ematen dion TCP/IP arkitekturak egiten duena.

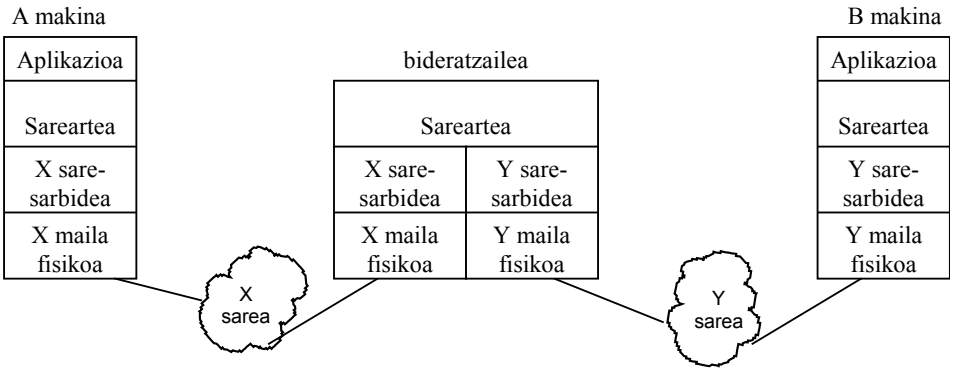
Sistema irekiak definitzeko nazioarteko ekimen instituzionala OSI eredua izan da. Egitasmo horrek definitzen duen sare-arkitektura ez da inoiz gauzatu. Bere patua arkitektura errealekin alderaketak egiteko erreferentzia akademikoa izatea dela dirudi. Bere ekarpen nagusia (bakarra ote?) aurreko kapituluan ikusi ditugun sare-arkitekturaren kontzeptuaren ingurukoak ondo definitzea izan da (mailak, zerbitzuak, entitateak, interfazeak, protokoloak...).

■ Lau mailako sare-arkitektura bat

Sareak elkarrekin konektatzeko behar duguna hau da:

- Informazioa sareartean sartzeko formatu komuna.
- Helbideratze-sistema komuna.

Finean, sareartean sartzeko protokolo komuna behar da, sare bakoitzaren ezaugarriekiko independentea dena. Beste era batean esanda, sareak elkarrekin konektatzeak badu sare-arkitekturan maila bat sartzeko behar den funtsa. Maila horrek goiko mailari eskainiko dion zerbitzua sarearteko komunikazioa izango da, bere beheko mailek sare baten barruko komunikazio-zerbitzua eskaintzen duen modu berean. 2.2 irudian horrelako 4 mailako sare-arkitektura esperimentalarekin eraikitako sarearte baten eskema dugu. Irudiko sareartean bi mota ezberdineko sareak agertzen dira. Biak lotzen dituen ekipo bitartekaria bideratzaile bat da, bi sare-txartel ezberdinak izango dituena. Pakete-kommutagailuetan gertatzen den bezala, bideratzaileetan ez da behar aplikazio-mailarik, beren lana sarearte-mailan egiten baitute; ez dute zertan aplikazio-mailako informazioa aztertu edo prozesatu. Izan ere, sareak lotzen dituzten bideratzaileak sarearteko pakete-kommutagailuak besterik ez dira. Beren lana softwarean egiten dutenez (oraingoz, behintzat, kasu gehienetan), **bideratzaileak** deitzen ditugu. Ingelesezko testuetan *router* eta *gateway* hitzak erabiltzen dira.



2.2 irudia: Konputagailu-sareak elkarrekin konektatzeko lau mailako arkitektura.

Konputagailu-sare heterogeneoak elkarrekin konektatzeko sarearte-protokolo komuna behar da. Horrek sare-arkitekturan beste maila bat txertatzea suposatzen du.

2 Sarearte-mailako arazoak

Aurreko atalean sarearte-maila sortzera bultzatu gaituen protokolo eta helbideratze-eskema komunaren beharra aurkitu dugu. Baina maila horretan konpondu beharko diren arazoak ez dira bi horiek bakarrik. Ondoko hauek guztiak hartu behar dira kontuan:

- Sarearte-helbideratzea.
- Pakete-bideratzea.
- Kongestioak bideratzaileetan.
- Sare-helbideen eta sarearte-helbideen arteko erlazioa.
- Paketeen tamainaren mugak.
- Goiko mailari eskainitako zerbitzu-mota.

Atal honetan banan-banan aztertuko ditugu.

■ Sarearte-helbideratzea

Arazo bera genuen pakete-kommutazioko sareetan. Ez da harritzekoa, funtsean, sarearteak pakete-kommutazioko datu-sareen kasu partikularra besterik ez baitira, bereziki konplexua den kasua izan arren. Hori dela eta, helbideen egitura diseinatzean orduan ikusi genituen baldintzak orain ere kontuan hartu behar dira. Ondoko hauek ditugu:

- Helbide kopurua. Honek baldintzatuko du sareartearen tamaina. Sareartea unibertsala izatea nahi badugu, kopuru hau nahiko handia izan behar du, eta horrek diseinatu behar dugun paketearen goiburukoan helbide bakoitzeko bit dezente gordetzea suposatzen du.
- Helbideen hierarkia. Bideratzaileek izango dituzten tauletan sarearteko edozein helburu-helbidetara ailegatzeko egin behar den hurrengo urratsa egon behar da. Ez da bideragarria bideratzaile guztiek beren tauletan sareartean dagoen konputagailu bakoitzeko sarrera bat izatea, taula erraldoiak eta trataezinak liratekeelako. Hori ekiditeko modua helbideak hierarkikoki antolatzea da. Horrenbestez, helbide askorentzako sarrera bakarra egon daiteke tauletan, eta horien tamaina asko murriztu.
- Helbideen kudeaketa. Sarearte unibertsal batean ez dago sare guztien jabea den inor eta, beraz, ezta kudeatzaile bakarra ere. Horrela izanik, behar-beharrezkoa da helbideak banatuko diren elkarte bat, Ethernet helbideekin egiten den moduan.

■ Pakete-bideratzea

Berriro ere arazo hau pakete-kommutazioko sareetan agertzen dena da. Baina sarearteetan edo sare batean ezberdina da bideratzea. Aldea ondoko honetan datza: sare batean bideratzea sare barruko bideratzaileen arazoa da soilik; erabiltzaileen makinek ez dute inolaz ere horretaz arduratu behar. Behin paketean helburu-helbidea ipini eta sarean sartu dela, sareko nodoen lana da pakete hori bere helmugaraino eramatea, eta sareko nodoek (bideratzaileek/kommutagailuek) bakarrik izan behar dituzte bideratze-taulak. Sarearte batean ez da horrela: konputagailu batek sareartean dagoen beste konputagailu bati pakete bat bidali behar badio, lehenengo urratsa saretik ateratzeko dagokion bideratzaileari paketea helaraztea da. Bideratzaile hori zein den jakiteko

(irteera bat baino gehiago egon daiteke sare batean) helmugako sarearte-helbidea da oinarria. Baina sare barruko bideratzaileek ezin dute sarearte-mailako paketerik prozesatu, ez baitute sarearte-mailarik eta, beraz, ezin dute helmugako helbide hori prozesatu. Lehengo bideratzailerainoko urrats hori zein den jatorrizko makinak erabaki beharko du eta, horretarako, bideratze-taula bat beharko du. Sareetan, aldiz, jatorrizko konputagailuek (erabiltzaileenak, alegia) ez zuten inongo bideratze-taularik behar.

■ Kongestioak bideratzaileetan

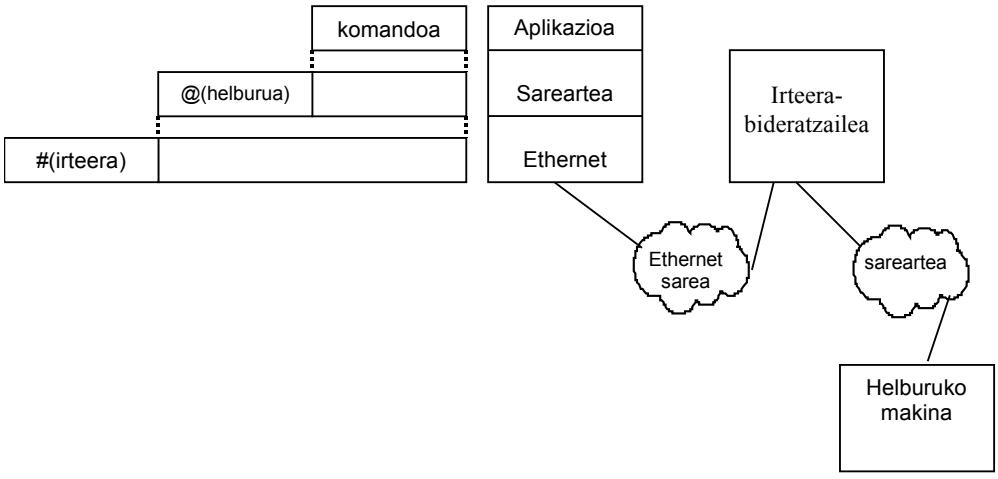
Sareen arteko loturak gutxi izaten dira. Eskuarki, sare bat sarearteko hornitzailearena egiten duen beste sare bakar batekin konektatzen da, eta bere kanpoko trafiko guztia hortik bideratzen da. Horregatik sarearteko bideratzaileetan kongestioa sortzeko arriskua sare baten nodoetan baino askoz handiagoa da.

Arazo hau oso larria da gaur egungo sarearte unibertsalean (Internet), eta bere tratamendua nahiko zaila. Berez, kongestio baten aurrean Interneteko bideratzaileek egiten dutena "ostrukarena" da, ikusiko dugunez.

■ Sare-helbideen eta sarearte-helbideen arteko erlazioa

Aurrean ikusi dugu erabiltzaileen konputagailuek bideratze-taulak izan beharko dituztela, kanpora doan pakete bat dagokion irteera-bideratzailera bideratzeko. Hori jakinda, sarbide-mailako trama bat osatu beharko du (edo pakete, edo zelula, edo...), eta trama horren informazio-eremuan sarearte-mailako paketea sartu. Sarearte-mailako paketearen goiburukoan helburu-helbidea izango dugu, eta sarbide-mailako tramaren goiburukoan irteera-bideratzailea denaren sarbide-mailako helbidea jarri beharko da (adibidez, erabiltzailearen sarea Ethernet baldin bada, bere Ethernet helbidea), 2.3 irudian agertzen den bezala. Orduan, sareko makina guztiek sarearte-mailako helbideen eta sarbide-mailako helbideen arteko erlazioa ere ezagutu beharko dute. Sarbide-mailako helbideari **helbide fisikoa** esaten zaio normalean.

Ondo bereizi behar dira sarearte-mailako helbideak eta sarbide-mailako helbideak (helbide fisikoak). Aurrenekoak helbide globalak dira, eta besteak lotuta dugun sarean bakarrik erabilgarriak.



2.3 irudia: sarearte-helbideen eta helbide fisikoen arteko erlazioa. @ karakterearekin dagoena sarearte-mailako helbide bat da, eta # karakterearekin dagoena helbide fisikoa (Ethernet helbidea, kasu honetan).

■ Paketeen tamainaren mugak

Sarearte-protokoloak ezartzen du sare guztiek onartuko duten paketearen formatua. Formatu horren ezaugarrietakoa bere tamaina maximoa da. Bideko sare guztiek paketeak onartu eta garraiatu behar badituzte, tamaina maximo horrek ondoko baldintza hau bete behar du:

$$\text{Max(sarearte-paketea)} = \min(\max[\text{sare1}, \text{sare2}, \ldots \text{sareN}])$$

Hori oso baldintza murriztailea izan daiteke, sare-aniztasuna handia denean, alde handia baitago sareek onartzen dituzten paketeen tamaina maximoen artean. Adibidez, X.25 sareen tamaina maximoa 128 bytekoa da, eta Frame Relay-rena, ordea, 8192 bytekoa. Sarearte berean X.25 eta FR sareak baditugu, definitutako sarearte-paketearen tamaina maximoa ezin da 128 byte baino handiagoa izan. Horrela bada, FR sareen erabilpenaren eraginkortasuna oso txikia litzateke.

Beste bidea paketea zatitzea da, zeharkatu behar den sarerako handiegia bada. Horrela izanik, ez dago arazorik sarearte-pakete erraldoiak sortzeko. Hala eta guztiz ere, sareartean parte hartzen duten sare guztiek sarearte-protokoloak definitzen duen pakete-zati minimoa onartu beharko dute. Hots, sarearte-protokoloak definitutako paketeak ondoko baldintza hau ezartzen du:

$$\text{Min(sarearte-paketa)} <= \min(\max[\text{sare1}, \text{sare2}, \ldots \text{sareN}])$$

Aurreko adibidea hartuta, ezin da 128 byte baino handiagoa den sarearte-pakete minimoa definitu, paketeak, zatitu arren, ez liratekeelako X.25 sareko paketeetan sartuko.

■ Goiko mailari eskainitako zerbitzu-mota

Sarearte-mailak gainean duen mailari (2.2 irudiko arkitektura esperimentalean, aplikazio-mailari) ematen dion zerbitzua informazioa sarearte batean zehar garraiatzea da. Hori bi eratan egin daiteke: konexioen bidez edo konexiorik gabe.

Konexioen bidezko zerbitzua bada, bi konputagailuen artean elkarrizketari ekin baino lehen, bion arteko sarearteko konexioa ezarri behar da. Konexioa ezartzea komunikazio horri dagozkion ezaugarriak bi muturren artean hitzartzea da. Adibidez, paketeek jarraituko duten bidean ezartzeko, pakete horien tamaina maximoa mugatzeko, edo beste aldeari komunikazio-eskaerari uko egiteko aukera emateko besterik ez. Normalean, konexio baterako sareartean zehar ezartzen den bideari **zirkuitu birtuala** esaten zaio.

Konexioen bidezko zerbitzuak duen abantailarik nagusia hau da: sareartean gertatzen dena kontrolatu daiteke eta, ondorioz, komunikazioaren kalitatea berma daiteke. Honi, ingelesez, QoS ematea deitzen diote (*Quality of Service*). Zehatz-mehatz, konexioen bidezko komunikazioetan eragiketa hauek egin daitezke:

- Aurrez ezar daiteke komunikazioari dagozkion pakete guztiek sareartean zehar egingo duten ibilbidea. Honek sareartearen trafiko-kudeaketa asko errazten du, kongestioak aurreikusi eta bideratzaileen arteko trafiko-zama orekatu daitekeelako.
- Paketeak zein bideratzailetan ibiliko diren jakinda, posible da bideratzaile horietan baliabide erreserbak egitea (lineak eta tokia ilaretan) eta, horrekin batera, paketeek beren bidaian zenbat denbora emango duten aurreikustea.
- Konexio bati dagokion paketeren baten galera atzeman daiteke, eta paketea birtransmititu. Sareartean dagoen sare baten batek errore-zuzenketa egiten ez badu (Ethernet sareek, adibidez, ez dute egiten), sarearte-mailak egingo du. Edota kongestioak ezin badira guztiz saihestu, bideratzaileen pilaketetan galdutako paketeak sarearte-mailak errekuperatu ditzake, berriro ere birtransmisioen bidez.

Horiek dira aldeko aldeak. Konexioen bidezko komunikazioaren kontrako aldeak hauek dira:

- Errore- eta kongestio-kontrolak egiten badira, bideratzailearen lana zaildu egiten da. Pakete bakoitzaren prozesamendua luzeagoa eta konplexuagoa izango da, bideratzaileak denbora gehiago emango du pakete bakoitzarekin, eta, birtransmititzea badago, bufferra luzeagoan hartuko du paketeak (bere transmisioaren onespena jaso arte). Gaur egungo sarearteetan baliabide kritikoa bideratzaileak baldin badira, horien lana zailagoa egiteak ez du oso ideia ona ematen.
- Gainera, bideratzaileetan kontrol batzuk ezartzeak lanak bikoiztea edo behar ez diren lanak egitea ekar dezake. Adibidez, bidean zeharkatzen ditugun sare guztiek errore-kontrola egiten badute. Edo paketeek egiten duten ibilbidean galera-tasa oso txikia suertatzen bada, beharbada hobe litzateke gainean dagoen mailan errore-kontrol xumea egitea. Halaber, aplikazio batzuek ez dute inongo QoS-rik behar, edo behar duten kalitatea beste motakoa da. Denbora errealekoek, hain zuzen ere, behar dutena ez da paketeak bere helburura ondo ailegatu direla bermatzea, paketeak ahal bezain laster ailegatuko direla segurtatzea baizik, nahiz eta arintasun horren truke bidean pakete batzuk galdu.
- Zirkuitu-kommutazioan gertatzen zen bezala, konexioen bidezko komunikazioetan baliabideak erreserbatzen badira, baliabide horien ustiaketa ez da hobezina izango. Konexio batzuen kalitatea bermatzeko beste konexio batzuei uko egin beharko zaie, nahiz eta, benetan, bideratzaileetan denentzako tokia egon.

Konexiorik gabeko zerbitzuen ezaugarriak kontrakoak dira. Konputagailu batek beste batera informazioa bidali nahi duenean, ez du aurretik inongo kontakturik berarekin: paketeak sortu eta bidali. Pakete bakoitza bere sarearteko zeharbidea egiten saiatuko da, komunikazio berari dagozkion beste paketeekiko inongo erlaziorik gabe. Nolabait, paketeek beren burua aski izan behar dute beren bidaian. Horrelako zerbitzua dagoenean, paketeari **datagrama** deitzen zaio.

Datagrama-sarearteen arazoak hauek dira:

- Ez dago QoS bermatzerik. Ezin da jakin datagrama bat bere helburura ailegatuko den ala ez, ezta horretarako zenbat denbora beharko duen ere. Sare hauei *best effort* sareak ere deitzen zaie (euskaraz, *ahal dena* sareak). Ez da ezer bermatzen, baina horrek ez du esan nahi kalitate eskaseko zerbitzua emango denik. Berez, zerbitzuaren kalitatea sareartearen egoeraren eta egin behar den ibilbidearen araberakoa da.
- Sareartearen kontrola askoz zailagoa da. Ez dago kongestioak aurreikusterik ezta trafiko-zama orekatzerik ere.

Eta abantailak ondoko hauek dira:

- Sare-baliabideak hobeto ustiatzen dira, kasu hobezinetik gertuago, erreserba egiterik ez dagoelako.
- Bideratzaileen lana bideratzea besterik ez denez, hori azkarrago egitea badute. Ekipo sinpleagoak izango dira.

2.1 taulak laburbiltzen du bi zerbitzu horiek sarearteetan zer duten alde eta zer kontra:

	Konexioen bidezko zerbitzua	**Datagrama-zerbitzua**
Alde	Sareartearen kudeaketa errazten da Badago QoS bermatzea	Baliabideen ustiaketa hobea da Bideratzaileen lana errazten da
Kontra	Lana alferrik egin daiteke bideratzaileetan Bideratzaileen lana zailtzen da Baliabideen ustiaketa txarra izan daiteke	Ez dago QoS bermatzerik. Zailagoa da sareartearen kudeaketa

2.1 taula: konexioen bidezko zerbitzua eta datagrama-zerbitzua.

Datagrama-sareetan bideratzaileen lana minimizatzen da. Horrek QoS ez izatea dakar.

3 Interneteko sarearte-maila: IP protokoloa

TCP/IP sare-arkitektura garatu zutenean, argi zuten arkitektura horrek edozein sare-mota integratzeko balio behar zuela. Horregatik, arkitektura horretan gure arkitektura esperimentalean definitutako sarearte-maila bezalako maila bat agertzen da, IP izenaz ezagutua. IP siglak sarearte-mailan erabilitako protokoloarenak dira, *Internet Protocol*, alegia. TCP/IP sare-arkitektura Interneten erabiltzen dena izateak arkitektura hau sistema irekien oinarri bihurtu du: TCP/IP arkitekturak jarraitzen duen sistema (sarea)

irekia da, beste edozein sistemarekin (sarearekin) konektatzea baitu, baldin eta beste sistema horrek (sarea) TCP/IP mailak bere sare-arkitektura propioaren gainean instalatzen badu.

Atal honetan IP protokoloaren ezaugarri nagusiak ezagutuko ditugu. Hurrengoetan IP sarearte mailari dagozkion beste alde batzuk aztertuko ditugu: helbideak, bideratzea, eta sarearte-kontrola.

■ IP zerbitzua

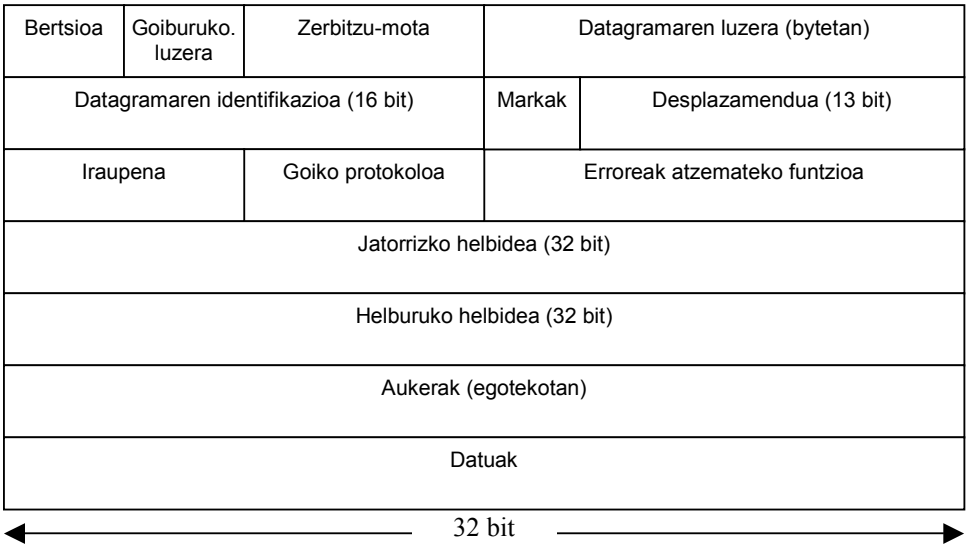
IP mailak eskaintzen duen zerbitzua datagrama erakoa da. Honek mailaren eta protokoloaren beste ezaugarri asko baldintzatzen ditu. Gogora dezagun sarearte-mailako zerbitzua datagrama erakoa izateak dakartzan ondorio batzuk:

1. Bideratzaileen lana errazten da. Datagrama bakoitzaren tratamendua arinagoa da eta, beraz, datagrama horrek denbora gutxiago emango du bideratzailearen bufferretan.
2. Sareek ere ez dute inongo bermerik eman behar. Hau da, sareartean parte hartzeko bete behar diren baldintzak minimoak dira (paketearen tamaina maximoari dagozkionak bakarrik). Honek sareartearen heterogeneotasuna bermatzen du.
3. IP sareek ez dute QoS bermatzen. Horregatik ez dira denbora errealeko aplikazio batzuetarako egokiak izango, bideokonferentzia edota telefoniarako, besteak beste.

IP zerbitzua konexiorik gabeko datagrama-zerbitzua da.

■ IP datagramaren formatua

Datagrama-zerbitzu batean ez da errore-kontrolik egin behar. Horrek asko sinplifikatzen ditu transmititzeko prozedurak, baita datu-unitatearen formatua ere (datagramarena, alegia). IPrena bezain sinplea den zerbitzua emateko, datagramaren goiburukoan behar dugun eremu bakarra helburuko helbidea dela dirudi, datagramen prozesamendua bideratzaileetan bideratzea besterik ez denez. Haatik, IPren goiburukoan askoz eremu gehiago agertzen dira, 2.4 irudian ikus daitekeen legez.



2.4 irudia: IPv4 datagramaren formatua.

Irudian agertzen diren eremu batzuk beharrezkoak dira; beste batzuk, aldiz, ez. IP protokoloa diseinatu zenean guztiz esperimentala zen (70eko hamarkadaren hasieran), eta horregatik agertzen dira beharrezkoak ez diren eremu batzuk. Gero, protokoloaren erabilera hedatu egin da, sareen arteko elkarrekiko konexio unibertsalerako tresna bihurtu arte, baina bere 'haurtzaroaren' arrastoak hor gelditu dira. Formatuaren azterketarekin batera, protokoloaren beraren ezaugarriak ezagutuko ditugu. Azterketa hori eremuen garrantziaren araberako ordenan egingo dugu. Behar-beharrezkoak diren eremu bakarrak ondoko hauek dira:

- Helbideak. Irudian ikusten denez, helburukoa ez ezik, jatorrizkoa ere jartzen da. Bideratzaileek ez dute jatorrizko helbide hori ezertarako behar, baina zerbitzari batzuek identifikatu beharko dute nor den beraiekin lan egin nahi duen bezeroa, eta identifikazio horren ezinbesteko zati bat bere jatorrizko makina izango da. Geroko atal batean aztertuko dugu sakonean nolakoak diren IP helbideak.
- Goiko protokoloa. Eremu hau helmugako konputagailuak bakarrik behar du, eta ez bideko bideratzaileek. IP mailak datagrama nori eman behar dion jakiteko ezinbestekoa da, IP mailaren erabiltzaileak asko izan daitezkeelako. Gure 4 mailako arkitektura esperimentalean (2.2 irudia) sarearte-mailan IP protokoloa erabiltzen badugu, eremu honek jasotako datagrama zein aplikaziori eman behar zaion adierazten du (konputagailu batean sarearekin lan egiten duten aplikazio asko egon daitezke martxan aldi berean).
- Bertsioa. Gehien erabiltzen dena 4. da, IPv4 siglaz ezagututa. Honek datagramak nolako goiburukoa duen adierazten du, bertsio ezberdinek datagrama ezberdinak erabiltzen baitituzte. Bertsio berria IPv6 da. Gero komentatuko dugu zerbait bertsio berri horri buruz.
- Goiburukoaren luzera. Datagrama prozesatu behar duten IP entitateek (bideko bideratzaileenak eta helburuko konputagailuarena) goiburukoa non bukatzen den eta garraiatutako datuak non hasten diren jakin behar dute. Goiburukoan aukerazko eremu batzuk daudenez, bere luzera ez da finkoa, eta eremu hau beharrezkoa suertatzen da.

IP datagrama bat sareko pakete batean sartzeko handiegia baldin bada, zatitu egin behar da. Datu-zatirik txikiena 8 bytekoa izan daiteke; beraz, IP sareartean sar daitezkeen sare guztiek 28 byteko datagramak onartzeko gai izan behar dute (IP goiburukorik txikiena 20 bytekoa da). Praktikan, honek ez du batere murrizten konektatu daitezkeen sareen multzoa. Zatiketa bideratzaileek egiten dute, baina helburuko konputagailuak berreraiki beharko du jatorrizko datagrama, zati guztiak jaso ondoren. Zatiketa lana zama estra bat da bideratzaileentzat; horregatik, aukera hori kendu egin da IPren bertsio berrian, non zatiketa egitekotan jatorrizko konputagailuak egin behar duen, ez bideratzaileek. IPv4 goiburukoari ondoko 3 eremu hauek erantsi behar izan zaizkio zatiketagatik, helburuko konputagailuari datagrama berregiteko behar den informazio guztia emateko:

- Datagramaren identifikazioa. Zati guztiek jatorrizko datagramaren identifikazioa eramango dute. Horrela helburuko konputagailuak zati guztiak bildu ditzake.
- Desplazamendua. Eremu honek zati honen kokapena jatorrizko datagraman adierazten du. Zatirik txikiena 8 bytekoa denez, horrela adierazten da desplazamendua, zortzi byteka. Eta horregatik eremu honek 13 bit behar ditu: datagramaren tamaina maximoa (2^{16}) zati zatirik txikiena (2^3), 2^{13} da.
- Bit-markak (edo *flagak*). Aurrenekoa ez da erabiltzen. Besteak *Ez zatitu* bita eta *Zati gehiago* bita dira (ingelesez, *Don't Fragment* –DF- eta *More Fragments* –MF-). Batak bideratzaileei datagrama hori ezin dela zatitu jakinarazteko balio du (aplikazio batzuek horrela beharko dute). Besteak helburuko IP entitateari hori ez dela jatorrizko datagramari dagokion azkeneko zatia adierazten dio.

Benetan beharrezkoak ez diren beste eremu batzuk honako hauek dira:

- Datagramaren luzera. Goiburukoaren eta datu-eremuaren luzera ez dago finkatuta. Horregatik adierazi behar da goiburukoan zein den luzera hori. Horretarako 16 bit daudenez, eta bytetan neurtzen denez, datagramarik handiena 65.535 bytekoa izan daiteke (datuak gehi goiburukoa). Dena dela, oso arraroa da 1500 byte baina handiagoa den datagrama bat aurkitzea (hori da Ethernet sare batean sartzen den datagramarik handiena), eta sistema askok 576 bytera mugatzen dute datagramaren tamaina (eremu zabaleko sare askok onartzen duten tamaina maximoa). Egia esan, datagramaren tamaina mailen arteko interfazeari dagokion informazioa da eta, beraz, ez zuen goiburukoan egon behar.
- Iraupena. Eremu honi balio bat ematen zaio jatorrizko konputagailuan, eta bideko bideratzaile bakoitzak 1 kentzen dio; eremuaren balioa 0-raino heltzen bada, bideratzaileak datagrama ezabatuko du, inora birbidali gabe. Mekanismo honen helburua datagrama galduak saretik kentzea da (adibidez, bideratze-errore bat badago eta datagramak begizta batean harrapatuta gelditzen badira).
- Erroreak atzemateko funtzioa. Goiburukoari bakarrik ezartzen zaion funtzio matematiko sinplea da. Bideratzaile guztiek birkalkulatu behar dute eremu hau. Praktikan, bideratzaile gehienek ez diote inongo kasurik egiten, gaur egungo sare gehienek beren paketeetan (edo trametan) IPrena baino askoz indartsuagoak diren erroreak atzemateko funtzioak erabiltzen baitituzte (CRC funtzioak gehienetan), eta, gainera, datagramaren eremu guztiei aplikatzen zaizkie funtzio horiek (ez bakarrik goiburukoari). Beraz, eremu honi kasu egitea denbora

galtzea da: txartelak ez lioke IP mailari matxuratuta dagoen datagrama bat pasatuko.

- Zerbitzu-mota (ingelesez, TOS: Type Of Service). Eremu honek datagramen artean lehentasunak ezartzeko balio du. Horrela, bideratzaile batek badaki kongestio bat sortzen denean zeintzuk diren ezabatu behar dituen lehenengo datagramak. Praktikan oso gutxitan erabiltzen da.
- Aukerak. Bideratzaile askok ez diote kasurik egiten. Protokoloaren ezaugarri berriak frogatzeko sartu zen eremu hau goiburukoan. Gaur egun aukera batzuk daude definituta. Adibidez, eremu honetan datagramak jarraitutako bidea adieraz daiteke (bideko bideratzaileak hori grabatzeko prest baldin badaude, noski).

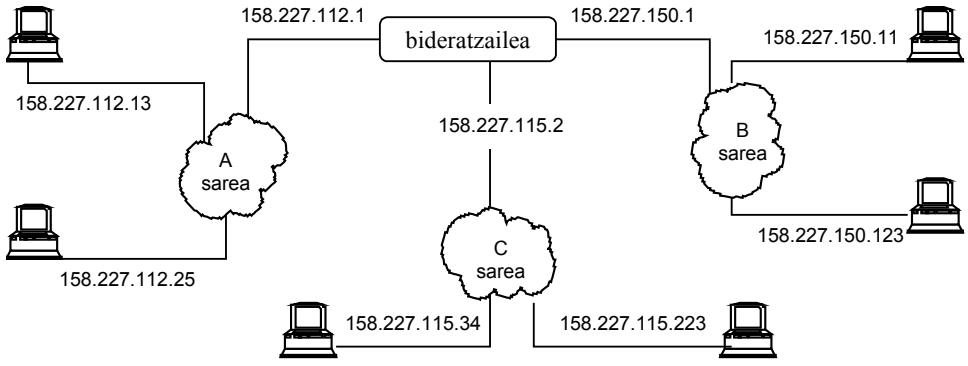
IPv4 datagrama baten goiburuko eremurik garrantzitsuenak helburu eta jatorrizko helbideak eta goiko protokoloa dira.

4 IP helbideak

IP helbide guztiek 32 biteko luzera dute (hau da, 4 byte), beraz, 2^{32} IP helbide posible daude. IP helbideak **notazio hamartar puntudunez** idazten dira. Formatu horretan, 4 bytetako bakoitza notazio hamartarrez idazten da, 0-tik 255-era. Adibidez, IP helbide tipiko bat 192.33.217.137 da, notazio horretan idatzita. 192 zenbakia helbidearen lehenengo 8 biten adierazpena da, era hamartarrean; 33, helbidearen bigarren 8ko bit-sortaren adierazpena da era hamartarrean, e.a. Honela, 193.33.217.137 helbidearen idazkera bitarra ondoko hau da (hutsune batzuk sartu ditugu byteak ondo bereizteko):

11000000 00100001 11011001 10001001

Sare-txartel bakoitzak (IP hizkeran, **sare-interfaze** bakoitzak) bere IP helbidea behar du. Beraz, konputagailu batek dituen sare-loturak bezainbeste IP helbide izango ditu. Horregatik, bideratzaileek IP helbide bat baino gehiago izaten dute, eta erabiltzaileen makinek IP helbide bakarra izaten dute. Adibidez, 2.5 irudian erabiltzailearen makina batzuk eta bideratzaile bat agertzen dira, irudiko hiru sare lotzen dituena.



2.5 irudia: IP helbideak eta sare-interfazeak.

Irudiari buruzko gauza batzuk aipatu behar dira. Lehenengoz, erabiltzailearen makina bakoitzak sare-interfaze bakarra du, eta irudian IP helbide bakarra esleitu zaio. Bideratzaileak, aldiz, hiru sare-interfaze ditu, bakoitza bere helbide propioarekin. Bigarrengoz, A sareari konektatuta dauden sare-txartel guztiek, bideratzailearenak barne, 158.227.112.xxx erako IP helbidea dute. Era berean, B sareari eta C sareari konektatuta dauden interfaze guztiek 158.227.150.xxx eta 158.227.115.xxx erako IP helbideak dituzte, hurrenez hurren. Beste hitzetan, helbide bakoitzak bi zati ditu. Lehenengoak (aurreneko 3 byteak, adibide honetan) sarea identifikatzen du; bigarrenak (azkeneko bytea, adibide honetan) sareari konektatuta dagoen konputagailu bat helbideratzen du, edo, hobeto esanda, sare-interfaze bat helbideratzen du (gogoan izan konputagailu batek IP helbide asko izan ditzakeela, sare-interfaze bezainbeste). Hedatuta dagoen IP hizkeran sarearen identifikazioari **sare-helbidea** deitzen zaio, eta interfazeari dagokion zatiari **makinaren identifikazioa**.

Beraz, IP helbide baten ezkerreko bitek sarea identifikatzen dute, eta eskuinekoek konputagailua (hobeto, sare-interfazea). Baina, zenbat bit esleitzen zaizkio zati bakoitzari? IP sare bakoitzak IP helbideen bit-banaketa berezkoa du. Banaketa hori **sare-maskara**ren bidez adierazten da. Sare-maskarak bi era ezberdinetan idazten dira. Gehien hedatuta dagoenak IP helbideen sintaxia du, non sareari dagozkion bitei 1 balioa esleitzen zaien eta interfazeari dagozkionak 0 diren. Adibidez, 2.5 irudiko C sareko maskara 11111111 11111111 11111111 00000000 da. IP helbideak bezala, era honetan adierazitako sare-maskarak notazio hamartar puntudunez idazten dira, eta aurrekoa 255.255.255.0 idatziko genuke.

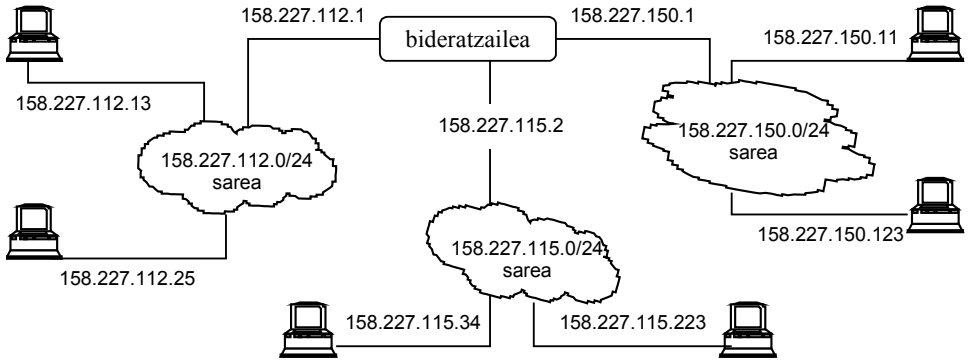
Sare-maskarak adierazteko bigarren era laburragoa da: sarea identifikatzeko erabilitako bit kopurua

sare-helbideari eransten zaio. Adibidez, irudiko C sarearen kasuan 158.227.115.0/24 idatziko dugu, sarea identifikatzeko ezkerreko 24 bit erabiltzen direla adieraziz.

Kontuan izan sarea eta interfazea bereizteko ezinbestekoa dela sare-maskara ezagutzea. Oso akats arrunta da sarearen eta interfazearen arteko bit banaketa zortzinaka egin behar dela uste izatea eta, beraz, sare-helbidea ezagutzea nahikoa dela banaketa hori zein den ondorioztatzeko. Horrela izanik, C sarearen helbidea 158.227.115.0 dela jakinez gero, ez genuke ezertarako maskara erabili behar. Baina sare-helbidea 158.227.115.0 izanda ere, gerta liteke interfazearenak eskuineko 7 bit bakarrik izatea (edo 6, edo 5... edo bakar bat). Anbiguotasun hori desegiteko erabili behar dira sare-maskarak.

IPv4 helbide bat bi zatitan banatzen da: sare-helbidea eta interfazearen identifikazioa. Biak bereizteko sare-maskarak erabili behar dira.

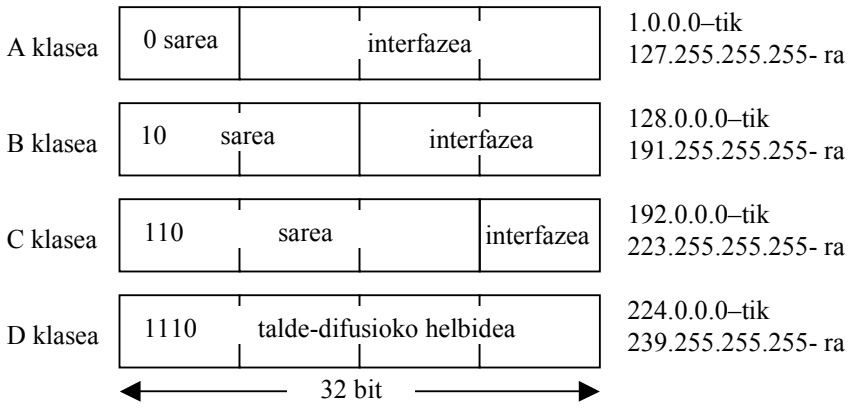
2.5 irudiko sareartea sare-helbideak erabiliz berregiten badugu, 2.6 irudia izango dugu.



2.6 irudia: sare-helbideak eta maskarak.

■ Helbide-klaseak

Ikusi dugun helbideratze-eskema, maskaretan oinarrituta, nahiko berria da. 1993. urtean definitu zen, CIDR izenarekin (Classless InterDomain Routing), eta geroztik erabiltzen dena da. Baina IPv4 helbideen jatorrizko antolaketa beste era batekoa zen, sinpleagoa. Lau helbide-klase bereizten ziren (A, B, C eta D klaseak), helbidearen aurreneko 4 bitak erabiliz, eta klase bakoitzean sarea eta interfazearen arteko bit banaketa finkatuta zeuden. Banaketa hori 2.7 irudian ikus daiteke.



2.7 irudia: helbide-klaseak.

Bosgarren klasea ere, 11110 bitekin hasten zena, definitu zen, baina ez zen erabiltzen: etorkizunerako gorde zen.

Klaseetan oinarritutako helbideratzea ez da jadanik TCP/IP arkitekturaren helbideratze-sistema. Interneten hazkundeak, eta IP helbideen eskaera handiak azaleratu zuen egituraketa hori itxiegia zen, ez zeukan inongo malgutasunik eskaera horri aurre egiteko. Helbide gehiegi xahutzen ziren sistema horretan: erakunde gehienek C klaseko sare-helbide batek ematen dituen 254 IP helbideak baino gehiago behar dituzte, eta

horregatik B klaseko sare-helbide bat esleitu behar zaie. Baina, beste alde batetik, kasu gehienetan erakundeek B klaseko sare-helbide batek ematen dituen 65.534 IP helbideak baino askoz gutxiago behar dituzte, eta, ondorioz, IP helbide gehienak gordeta gelditzen dira, erabili gabe.

Hala eta guztiz ere, sistema eragileen bertsio zaharretan ez da zaila klase-helbideen nomenklatura topatzea. Batzuetan, bi sistema, klaseena eta maskararena, nahastuta agertzen dira, nolabaiteko bateragarritasuna adierazteko asmoz. Baina erabiltzen dena maskararena da. Inguru esperimental batzuetan bakarrik badu interesa oraindik klaseen bereizketa egitea (talde-difusioko sare esperimentaletan, hain zuzen ere).

■ Helbide bereziak

IP helbide baten 32 bitek ahalbidetzen dituzten helbide guztiak ez dira erabilgarriak sarearteko konputagailuak identifikatzeko (edo, hobeto esanda, konputagailu horien interfazeak identifikatzeko). Honako hauek dira kontuz ibiltzeko IP helbide berezi horiek:

- *Loopback* helbideak.

  Bere lehenengo byteak 127 balio duen helbideek ez dute balio konputagailutik at. 127.x.y.z moduko helbide guztiak (2^{24}!!) gordeta daude konputagailuaren barruko entitateak identifikatzeko.

- Difusio helbideak (*broadcast*).

  IP helbide batzuk gordeta daude difusioa egiteko: bere interfazearen identifikazioaren bit guztiak 1ekoak dituztenak. Horrelako helbideek datagramak sareko konputagailu guztiei igortzeko balio dute. Adibidez, 155.233.0.0/16 sareko makina guztiei bidalitako datagrama batek 155.233.255.255 helburuko helbidea izango du.

  Beste aldetik, bere 32 bitak, sarekoak eta interfazekoak, 1ekoak dituen helbidea ere gordeta dago (255.255.255.255 helbidea, alegia): hori difusio mugatutako helbidea da. Konputagailu batek bere sareko helbidea zein den ez dakienean erabiltzen da. IP konfigurazio dinamikoa erabiltzen denean sortzen da egoera xelebre hori, gero ikusiko dugun DHCP zerbitzua erabiltzen denean, adibidez. Kasu horietan, bere nortasuna zein den ez dakiten konputagailuek 255.255.255.255 helbidea erabiltzen dute bere sareko konputagailu guztiei laguntza-deia helarazteko. Espero da hartzaileetako batek erantzungo diola mezuaren bidaltzaileari bere nortasunaren berri emanez.

  Pentsa daiteke 255.255.255.255 eta sareko difusio helbidea baliokideak direla, baina ez da hala. Aurreko adibideari jarraituz, 155.233.255.255 eta 255.255.255.255 helburuko helbideek ez dute tratamendu bera izango bideratzaileetan. Suposatzekoa da 155.233.0.0/16 sarea beste azpisare askok osatuko dutela, eta haien artean bideratzaileak egongo direla. Bideratzaile horietan dago aldea: 155.233.255.255 helburuko datagramak birbidaliko dituzte, 155.233.0.0/16 sareko makina guztiek jaso ditzaten, baina 255.255.255.255 helburukoak iragaziko dituzte. Beraz, azken

horiek, igortzailearen sare-segmentuko konputagailuek soilik jasoko dituzte, eta ez sareko guztiek.

Aurrekoak muga bat ezartzen die helbide baten sareko identifikadoreei: ez dago dena 1ekoak dituen sare-helbidea erabiltzerik, sareko difusio helbidea eta difusio mugatutako helbidea berdinak izango baitziren.

- Sarearen identifikadorea.

  Helbidearen interfazearen identifikazioko bitak ezin dira denak 0koak izan, horrela sortutako helbidea sare-helbidea delako.

■ Azpisareak identifikatzea

Sareak era hierarkikoan egituratzen dira. Sareen sarea den Internet, adibidez, **sistema autonomo** izeneko sareetan egituratzen da, non sistema autonomo bat erakunde administratibo bereko sarea baita. Era berean, sistema autonomo bakoitza beste sare askok osa dezakete, sare-hierarkian beste maila gehituz. Adibidez, Euskal Herriko Unibertsitateko sarea sistema autonomo bat da, 158.227.0.0/16 sare-helbidea duena. Sare horren barruan, beste sare asko daude elkarren artean konektaturik. Oso komenigarria izango da, bereziki bideratze-lanak errazteko, sistema autonomo, edo orokorrean, IP sare baten barruan dauden beste azpisareak identifikatzea. Horretarako erabiltzen da RFC 950 agirian deskribatutako teknika, *subnetting* izenekoa. Teknika horrekin, maskarak sare-helbidea eta interfazearen identifikazioa bereizteaz gain, sarea azpisareetan banatzeko ere balio du.

Sare bat azpisareetan banatzeko maskarak erabiltzen dira.

Azpisareak identifikatzeko, helbideko interfazearen identifikadorearen bitak erabiltzen dira, eta, hala, maskara luzatu egiten da. Har dezagun berriro 155.233.0.0/16 sarea adibide gisa. Demagun sare horren barnean 10 azpisare daudela. Azpisare horiek identifikatzeko, 4 bit behar ditugu gutxienez. Bit horiek kenduko dizkiogu interfazearen identifikadoreari; hau da, helbidearen hirugarren bytearen hasierako lau bitak izango dira. Sare-helbidea era bitarrean adierazten badugu, horiek dira ondoan nabarmenduta dauden lau bitak:

10011011 11101001 **0000**0000 00000000

Eta, hala, honako 16 azpisare-helbide hauek lortuko ditugu, notazio hamartar puntudunez orain:

155.233.0.0/20	155.233.64.0/20	155.233.128.0/20
155.233.16.0/20	155.233.80.0/20	155.233.144.0/20
155.233.32.0/20	155.233.96.0/20	155.233.160.0/20
155.233.48.0/20	155.233.112.0/20	155.233.176.0/20

155.233.192.0/20 155.233.224.0/20
155.233.208.0/20 155.233.240.0/20

Horietako 10, edozein, esleitu diezaiekegu gure 10 azpisareei. Adibidean 4 bit hartu ditugu azpisareak identifikatzeko, baina bit gehiago hartzea ere bazegoen (gutxiago, aldiz, ez). Azpisarea identifikatzeko, zenbat bit beharko ditugun zehazteko bi datu hartu behar ditugu kontuan:

- Bata, noski, zenbat azpisare identifikatu behar ditugun. Horrek bit kopuru minimoa ezartzen du.
- Bestea, zenbat interfaze identifikatu behar diren azpisare bakoitzean. Horrek maskararen bit kopuru maximoa ezartzen du. Gure adibidean azpisare bakoitzean gehienez jota 100 interfaze egongo balira, 7 bit utzi beharko genituzke interfazearen identifikaziorako. Hala, 128 identifikadore izango genituzke, soberan alegia, baina ezin da gutxiago hartu (6 bitekin 64 identifikadore besterik ez genituzke lortuko eta). Beraz, adibidean, maskarak 9 bit izan dezake gehienez jota.

Kontuan hartu azpisareak identifikatzeko maskarak esanahi lokala duela. Normalean, kanpoko ekipoek ez dituzte ezertarako beharko gure azpiasareen identifikadoreak. Beraz, adibideko sareko konputagailu baten helbidea 155.233.16.21/16 izango da kanpotik ikusita, baina, sare barruan, 155.233.16.21/20 erabiliko da.

Irakurleak suposatuko duen bezala, ez dago inongo trabarik azpisareak ere beste azpisareetan banatzeko, beti ere esanahi lokalarekin. Argiago ikusteko, demagun adibideko155.233.0.0/16 sarea erakunde batena dela, eta erakunde horrek 10 egoitza dituela toki desberdinetan. Horregatik sortu behar izan ditugu goiko 16 azpisare-helbideak. Baina gerta liteke, halaber, 155.233.16.0/20 azpisarea kudeatzen duen egoitzeko arduradunak beste azpisare batzuetan egituratu nahi izatea helbideratze-eremu hori, bere sail bakoitzeko azpisarea bereizteko. Demagun 3 sail desberdin daudela eta aurreikusten dela 400 konputagailu izatea, gehienez jota, horietako sail bakoitzak. Orduan, 2 eta 3 bit bitartean erabili ditzakegu sailen azpisareak bereizteko. Demagun 3 bit erabiltzen ditugula; kasu horretan, 8 azpisare-helbide lortuko ditugu 155.233.16.0/20 helbide-espazioan, bakoitza 512 konputagailu barne hartzeko ahalmenarekin. Ondoan, helbidearen hirugarren bytearen 8 balio bitar posibleak ditugu (bigarren azpisare-maskararenak nabarmenduta), baita horietatik sortzen diren 8 azpisare-helbideak ere, notazio hamar puntudunez:

0001 **000**0 → 155.233.16.0/23
0001 **001**0 → 155.233.18.0/23
0001 **010**0 → 155.233.20.0/23
0001 **011**0 → 155.233.22.0/23
0001 **100**0 → 155.233.24.0/23
0001 **101**0 → 155.233.26.0/23
0001 **110**0 → 155.233.28.0/23
0001 **111**0 → 155.233.30.0/23

Horietako 3, edozein, hartuko genituzke egoitza horren sailak identifikatzeko.

Luzera aldakorreko maskarak erabiltzea deitzen zaio era errekurtsibo horretan azpisareak definitzeari (*variable-length subnetting* edo *variable-length mask subnetting*). Teknika honi esker, sare bat azpisareetan banatzean ez dugu erabili behar azpisare-tamaina bera azpisare guztietarako. Hori oso garrantzitsua da helbide-eremuaren kudeaketa eraginkorra lortzeko. Gure adibidearekin jarraituz, gerta liteke azpisareetako baten 6 sailek oso behar desberdinak edukitzea, eta, nahiz eta horietako batek 400 helbide behar izatea posible izan, 50 helbide nahikoa izatea beste 5 sailetako bakoitzerako. Hala, helbideak xahutzea litzateke 50 helbide behar den azpisare bati 512 esleitzea; nahikoa baita interfazeak identifikatzeko 6 bit besterik ez uztea 5 azpisare horietan. Horretarako, 26 biteko sare-maskara erabiliko genuke azpisare horietan. Adibide batean argiago ikusteko, suposa dezagun 155.233.16.0/23 helbidea esleitzen diogula 400 konputagailu beharko dituen sailari. Beste 5ek beharko dituzten 250 identifikadore lortzeko, 155.233.18.0/23 helbide eremua hartuko dugu eta honela azpibanatuko dugu:

0001 001**0** **00**00 0000 → 155.233.18.0/26
0001 001**0** **01**00 0000 → 155.233.18.64/26
0001 001**0** **10**00 0000 → 155.233.18.128/26
0001 001**0** **11**00 0000 → 155.233.18.192/26
0001 001**1** **00**00 0000 → 155.233.19.0/26
0001 001**1** **01**00 0000 → 155.233.19.64/26
0001 001**1** **10**00 0000 → 155.233.19.128/26
0001 001**1** **11**00 0000 → 155.233.19.192/26

Horietako helbide multzo bakoitzak 64 interfaze identifikatzeko ahalmena du, nahikoa 5 sail horien beharrak asetzeko, horietako sail bakoitzari goiko sare-helbideetako bat esleituta. Beraz, gure erakundeko azpisare batzuek 20 biteko maskara erabiliko lukete (egoitza bakoitzekoek), beste batzuek, berriz, 23 bitekoa (400 interfaze-identifikadore behar duen sailekoek), eta beste batzuk, 26 bitekoa (50 identifikadore besterik behar ez duten sailekoek).

Azpisare-kopurua eta eta azpisare bakoitzaren interfaze-identifikadoreen beharren arabera kalkulatzen da maskararen luzera.

Luzera hori aldakorra izan daiteke: sare baten azpisare guztiek ez dute luzera bereko maskara erabili behar.

Aurreko adibideetan sortutako azpisare-helbideen artean, badaude azpisarearen identifikadorearen bit guztiak 0koak dituztenak (155.233.0.0/20, 155.233.16.0/23, eta 155.233.18.0/26) eta azpisarearen identifikadorearen bit guztiak 1ekoak dituztenak (155.233.240.0/20, 155.233.30.0/23, eta 155.233.19.192/26). Hasiera batean, horrelako helbideak erabiltzea eragozten zuen RFC 950 agiriak, helbide-klaseak erabiltzen zituzten sistemetan sortzen zituzten honako arazo hauengatik:

- Azpisarea identifikatzeko, nahasketak sortzen ziren bit guztiak 0koak zituzten helbideen artean. Adibidez, ez zegoen 155.233.0.0/20 eta 155.233.0.0/23 sare-helbideak bereizterik; bideratzaileentzako helbide bera ziren.
- Sare baten difusio helbidea eta sare horren azpisare baten difusio helbidearen artean ere, nahasketak sortzen ziren. Esaterako, gure adibideetako 155.233.31.255/20 eta 155.233.31.255/23 helbideen artean ez zegoen bereizterik bideratzaile batentzat.

Hala ere, bi arazo horiek desagertu ziren maskararen erabilerarekin, eta, gaur egun, badago horrelako sare-helbideak erabiltzea (RFC 1812 agiriak baimentzen ditu). Dena dela, kontuz ibiltzea gomendatzen da, oraindik gerta baitaiteke helbide horiek onartzen ez dituen sistemaren bat topatzea.

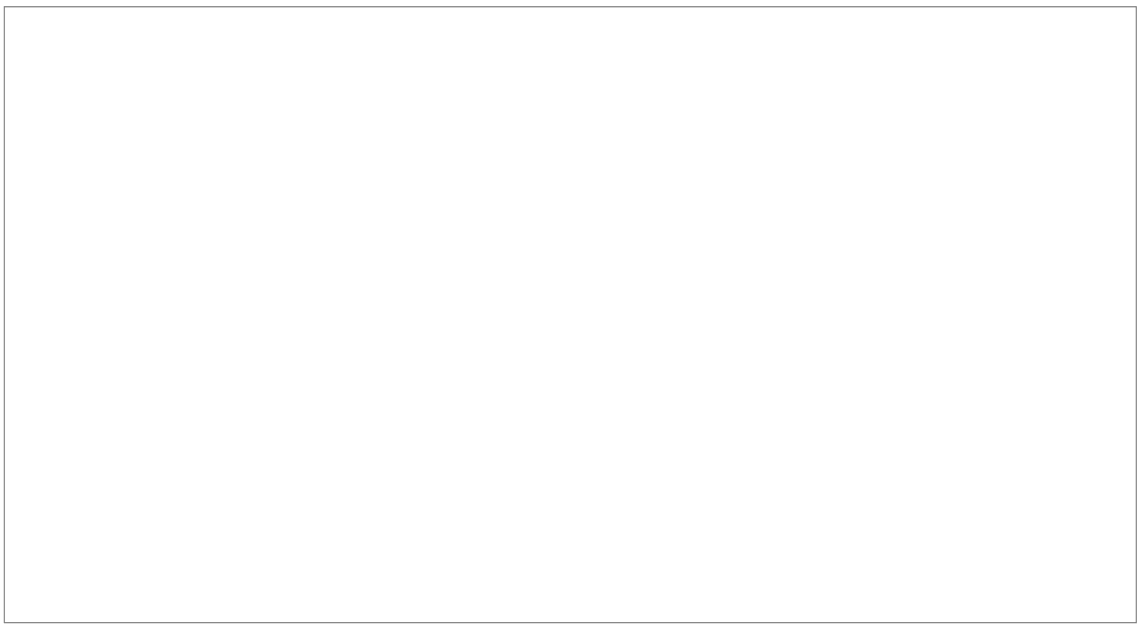
■ Helbideen esleipena

Nola lortzen du konputagailu batek IP helbide bat? Berriro ere, helbideen bi zatiak bereizi behar ditugu. Konputagailuak lortu nahi duen IP helbidea bere sare-interfaze bati (sare-txartelari) esleitzeko izango da, baina interfaze hori sare konkretu batekin konektatzeko izango da. Sare horrek bere sare-helbidea eta maskara izango ditu, non adierazten den sare horretan zenbat sare-txartel konekta dezakegun, eta zeintzuk diren sare-txartel horiei eman dakizkiekeen IP helbideak. Adibidez, 2.5 irudiko sare baten helbidea eta maskara 158.227.112.0/24 da eta, beraz, sare horrekin konekta daitezkeen sare-txartelen IP helbideak 158.227.112.1-tik 158.227.112.254-ra dauden 254 horiek dira. Kontuan izan helbide-sorta guztietan gordeta gelditzen direla interfazearen identifikazioaren bit guztiak 0koak eta 1ekoak duten bi helbide; bata sarearen beraren identifikazioa delako, eta bestea sare-difusiorako helbidea delako. Horrenbestez, helbidearen esleipenak bi urrats ditu:

1. Sareak bere helbide-sorta lortu behar du, bere sare-helbidea, alegia.
2. Sareko konputagailuek sare-helbideak zehazten duen helbide-sortatik bere IP helbidea lortu behar dute.

Gure TCP/IP sarea Internetekin konektatuta egotea nahi izanez gero, sare-helbidearekin batera, sarea kudeatzen duen erakundeak dagokion domeinua ere lortu beharko du (aurrerago ikusiko dugu zer diren *domeinuak* TCP/IPn). Hori guztia ICANN–ek kudeatzen du (*Internet Corporation for Assigned Names and Numbers*), RFC 2050-n agertzen diren gidalerroei jarraituz. Sarearen kudeatzaileak lortu nahi duen domeinu-motaren arabera, ICANN-ek izendatutako erregistratzaile batzuekin edo besteekin hitz egin dezake (eta ordaindu) sare-helbidea eta domeinua lortzeko. Erregistratzaileak hierarkikoki eta geografikoki daude antolaturik. ICANNek mundu mailako ardura du, eta, munduko eskualde bakoitzerako, RIR (*Regional Internet Register*) mailako beste erakunde baten eskuan utzi du ardura hori. Gaur egun, bost RIR dabiltza (ikusi 2.8 irudia): RIPE NCC (Europa, Ekialde Ertaina, eta Asiako eskukalde batzuk), APNIC (Asiako Pazifikoa), ARIN (Ipar Amerika), LACNIC (Latinoamerika), eta AFRINIC (Afrika). RIR horiek, berriz, eskualde txikiagoak hartzen dituzten LIR (*Local Internet Register*) izeneko beste erregistratzaileei esleitzen dizkiete IP helbide sortak, beraiek banatzeko. Hego Euskal Herrian bere zerbitzuak eskaintzen dituzten LIRak zein diren ikusteko, jo http://www.ripe.net/ripencc/mem-services/general/indices/ES.html

helbidera; Iparraldekoak, berriz, http://www.ripe.net/ripencc/mem-services/general/indices/FR.html url-n dituzu



2.8 irudia: RIRen mapa. http://www.ripe.net/ripencc/about/infosheet.pdf url-tik hartua.

Gure sarea isolaturik baldin badago, hau da, Internetekin konektatuta ez badago, ez dugu inongo oztoporik izango nahi ditugun sare-helbideak erabiltzeko, eta ez diogu inori inongo baimenik eskatu behar nahi dugun IP helbide-sorta erabiltzeko. Hala eta guztiz ere, IP estandarretan (RFC 1918) kasu isolatu hauetan erabiltzeko sare-helbide batzuk erreserbatzen dira. Zehazki, honako hauek dira erabilpen pribaturako gordetako IP helbide-eremuak: 10.0.0.0/8, 172.16.0.0/12, eta 192.168.0.0/16.

Behin sareak bere helbide-sorta lortuz gero, sareko makina bakoitzak berea lortu behar du. Horretarako bi dira mekanismoak:

- Eskuzko konfigurazioa: sistema eragileak dituen parametro batzuk bete behar dira, sare-kudeatzaileak esleitutako IP helbidearekin.
- Konfigurazio dinamikoa, sarearen bidez DHCP zerbitzari bat erabiliz (*Dynamic Host Configuration Protocol*). Konputagailuak DHCP [RFC 2131] zerbitzariari IP helbide bat eskatuko dio, eta honek eman egingo dio. DHCPren konfigurazioaren arabera, konputagailu bati esleitzen zaion IP helbidea beti izango da berdina, edo aldatu egin daiteke.

5 IP datagramak bideratzea

■ Bideratze-taulak

Kapitulu honen bigarren atalean ikusi dugu bideratzaileetan

bideratze-taulak egongo direla (pakete-kommutazioko datu-sare guztietan bezala), baita erabiltzaileen konputagailuetan ere. Bideratze-taula horietako lerro bakoitza bide bat da (*route*). Honako informazio hau izango dugu bide bakoitzerako:

- Helburu-helbideak. Salbuespenen bat edo beste izan ezik, ez dira egongo IP helbide soilak, helbide sortak baizik (normalean, sare-helbideak). Maskarak erabili behar dira helburu sortak adierazteko. Datagrama bat bideratzean, konputagailuak bilatuko du bere taulan zein helbide sortari dagokion datagramak daraman helburu-helbidea. Helburu sorta bakoitzeko honako datu hauek egongo dira:
- Hurrengo urratsa. Datagramak bere bidean bisitatu behar duen sarearteko hurrengo bideratzailearen IP helbidea da.
- Interfazea. Makinak duen interfazeen artean, nondik transmititu behar den datagrama bere hurrengo urratsa den bideratzaileraino heltzeko.
- Metrika. Helburura heltzeko kostua, bide hau erabilita. Bideratze-tauletan bide bat baino gehiago ager daiteke helburu batera joateko. Kasu horretan, bideratzaileek metrika eremu hori erabiltzen dute taulan agertzen diren aukeren artean bat hartzeko. Normalean, bidean zeharkatu beharko den bideratzaile-kopurua (*hop* esaten zaio kopuru horri ingelesez) adierazten du metrikak, baina beste irizpideak erabiltzea ere badago.

Bideratze-tauletan informazio gehiago egon daiteke (eta egoten da), baina hau da nahitaezkoa dena. 2.9 irudian Linux sistema baten bideratze-taula ikus daiteke, *route* komandoaren bidez lortuta. Irudiko taulan, helburu-helbidea lehenengo zutabean (*Destination* izenekoan) eta hirugarrenean (*Genmask* izenekoan) adierazten da. Lehenengoan helbide-sorta bat adierazten da, eta hirugarrenean zein den sorta hori interpretatzeko ezarri behar zaion maskara. Maskara hori 255.255.255.255 baldin bada, lehenengo zutabean agertzen den helbidea konputagailu batena da. Besterik ezean hartu behar den bidea (*default* ingelesez) 0.0.0.0 sasi-helbidearekin adierazten da irudiko sisteman.

2.9 irudia: bideratze-taula bat.

Bigarren zutabean (*Gateway* izenekoan) hurrengo urratsa zein den adierazten da. 0.0.0.0 denean, datagramaren helburua zuzenean konektatuta gauden sare batean dagoela adierazten da eta, beraz, ez da hurrengo bideratzaile batera bidali behar.

Azkeneko zutabeak (*Iface* izenekoak) datagrama zein sare-interfazetatik bidali behar den zehazten du. Irudiko taula erabiltzaile baten makinarena denez, eta ez bideratzaile

batena, sare-interfaze bakarra du, *eth0* izenekoa. Beste aukerarik ez dagoenez, dena atera behar da interfaze horretatik. Hala eta guztiz ere, zutabe honetan beste interfaze bat agertzen da, *lo* izenpean. Interfaze hori *loopback* da, hau da, hemendik bidalitakoa gure konputagailura itzuliko da sarerik pasa gabe. Bideratze-tauletan *loopback* izendatzeko *localhost* terminoa erabiltzen da. Ez da benetako interfaze bat, ez baitago inongo *loopback* txartelik konputagailuan. Helburutzat konputagailu bera duten datagramentzat erabiltzen da interfaze birtual hau; horrenbestez, TCP/IP multzoan zehar datagrama horien tratamendua beste datagramena bezalakoa da. *Localhost*-i 127.0.0.0/8 sare-helbidea gordetzen zaio, eta normalean 127.0.0.1 helbidea esleitzen zaio (baina irudiko sisteman 127.0.0.0 dauka). Bideratze-taula bat aztertzen dugunean *localhost* interfazea bazter dezakegu.

Bosgarren zutabea (*Metric* izenekoa) metrikarena da. Taula horretan, zutabe horrek ez du zentzurik, ez baitago bide desberdinen artean aukeratzeko beharrik.

Irudiko taula interfaze bakarra duen makinaren taula tipikoa da. Bere interpretazioa oso sinplea da: helburua sare berean baldin badago (158.227.128.0/21 da irudiko konputagailuaren sare-helbidea), ahaztu bideratzeko arazoak eta bidali dagoen txartel bakarretik, eta, bestela, gure saretik ateratzeko dagoen bideratzaile bakarrera bidali (irudiko taulan, 158.227.136.1 bideratzaileari). Sare batetik irteteko ate bat (bideratzaile bat) baino gehiago baldin badago, bideratze-taulan gutxienez lerro bat agertuko da horietako irteera bakoitzeko.

Bideratze-taulan IP mailako prozesuak zein den datagramak bisitatu behar duen hurrengo makina eta zein sare-interfazetatik bidali behar den lortzen du.

■ Bideratze-taulen erabilera

Datagrama bat prozesatzean, honako urrats hauek ematen dira:

1. Taulako bide bakoitzean, egiaztatu ea bat datorren datagramaren helburuko helbidea bideko helburu-helbidearekin. Bat datozen bideek balizko bideen multzoa osatzen dute.
2. Balizko bideen artean, aukeratu maskara luzeena dutenak. Horiek dira gure datagramari gehien dagozkion bideak.
3. Aurreko urratsean aukeratutako bideen artean, metrika hoberena dutenak hautatu.
4. Hautatutako bideak bat baino gehiago baldin badira, edozein aukeratu.

Adibidez, demagun 155.233.18.78 helburua duen datagrama bideratu behar dugula, eta lehenengo urratsa beteta, taulan helbide horrekin bat datozen honako bost bide hauek ditugula:

Destination	*Gateway*	*Genmask*	*Metric*	*Interface*
155.233.0.0	191.166.12.1	255.255.0.0	3	atm0
155.233.16.0	191.166.12.1	255.255.240.0	4	atm0
155.233.18.0	191.166.12.2	255.255.254.0	4	FR0
155.233.18.64	191.166.12.1	255.255.255.192	3	atm0
155.233.18.64	191.166.12.3	255.255.255.192	1	eth0

2.2 taula: 155.233.18.78 helbidearekin bat datozen bideratze-taulako bideak.

Bigarren urratsa betez gero, 2.2 taulako azkeneko bi bide besterik ez dugu izango. Hirugarren urratsan horietako bat bakarrik aukeratuko dugu, datagrama `eth0` interfazetik bidaliko duena. Laugarren urratsa ez dugu bete behar izango.

Aipatzekoa da datagramak prozesatzeko era honek sare bati esleitutako helbideratze-eremuan hutsuneak egotea ahalbidetzen duela. Jo dezagun berriro aurreko sekzioetako adibidera kontu hau ulertzeko, eta suposa dezagun 155.233.0.0/16 sistema autonomoa kudeatzen duenak helbideratze-eremu horko helbide guztiak esleitu dituela bere egoitzen artean. Urtebete ondoren, 155.233.32.0/20 Iruñeko egoitzako azpisareari dagozkien helbide guztiak erabili dituzte, eta helbide gehiago behar dute. Beste alde batetik, Maulen esleituta duten 155.233.16.0/20 azpisarean ez dituzte erabiltzen dagozkien helbide guztiak. Egoera konpontzeko, kudeatzaileak erabaki dezake Maulek erabiltzen ez duen helbide sorta bat Iruñeari eman. Demagun 155.233.24.0/22 dela helbide sorta hori, eta, beraz, 155.233.27.193 helbidera doan datagrama bat Iruñera bideratu behar dela, eta ez Maulera. Horretarako bideratze-tauletan bide berri bat sartu behar da salbuespena den helbide sorta horretarako, ondoan agertzen den bezala:

Destination	*Gateway*	*Genmask*	*Metric*	*Interface*
155.233.16.0	191.166.12.1	255.255.240.0	4	atm0
155.233.32.0	191.166.12.4	255.255.240.0	2	atm1
155.233.24.0	191.166.12.4	255.255.252.0	2	atm1

2.3 taula: hutsuneak helbideratze-espazioan eta bere tratamendua bideratze-tauletan.

Goiko taulako lehenengo lerroa Mauleko sarera joateko bidea da, bigarrena, Iruñera joatekoa, eta hirugarrena ere, Iruñera. 155.233.27.193 doan datagrama bideratzean, bat etorriko dira lehenengo eta hirugarren bideak, baina hirugarrenak maskara luzeagoa du (20 eta 22 bit, hurrenez-hurren), eta, beraz, azken hori aukeratuko da. Hala ere, hobe da saiatzea hutsunerik ez izaten esleitutako helbide sortetan, bideratze-taulak ahal den txikienak eta garbienak izatearren.

■ Taulen tamaina: bide-elkarketa

Aurreko sekzioaren hasieran ikusi dugunez, IP makina batek bere bideratze-taulako bide guztiekin alderatu behar du prozesatu behar duen datagrama bakoitzaren helburuko helbidea. Erabiltzailearen konputagailuen taulak txikiak dira beti, 2.9 irudikoa modukoak, eta segundoro datagrama gutxi prozesatu ohi dutenez, bideratze-prozesuan kongestio-arazoak sortzeko arriskurik ez dago. Bideratzaileen kasuan, berriz, gauzak oso desberdinak izan daitezke: trafiko guztia Interneteko ardatz-sareko bideratzaileetatik pasatzen da, eta, datagrama bakoitza prozesatzeko, denbora minimoa erabili behar da,

kongestioak saihestearren. Baldintza horietan, oso garrantzitsua da bideratze-tauletan ahal den bide kopuru txikiena egotea.

Bideratze-taulen tamainaren arazoa klaserik gabeko IP helbideak erabiltzen hasi zenean agertu zen. Hori ulertzeko, har dezagun 4000 IP helbide behar zituen erakunde baten kasua. B klaseko sare-helbide bat esleitzea 61.534 helbideak -hain urriak izanik- zakarrontzira botatzea zenez, hobe zen 16 C klaseko sare-helbide (4.064 IP helbide) esleitzea. Hala, IP helbideen eskasiari egin zitzaion aurre, baina, erakundeari 16 sare-helbide esleituz gero, 16 bidek agertu behar zuten bideratze-tauletan erakunde horri igorritako datagramak bideratzeko. Agian, erakunde horren bideratzaileen eta konputagailuen bideratze-tauletan bere burua identifikatzeko, 16 lerro agertzea ez litzateke arazo larria izango, baina Interneteko ardatz-sareko bideratzaileetarako bai. Horiek edozein datagrama bideratzeko gai izan behar dute, edo, beste era batean esanda, beren tauletan, Interneteko sare guztietarako bideek agertu behar dute. Bi milioi C motako sare-helbide baino gehiago daudenez, ardatz sareko bideratze-tauletan milioika bide agertuko ziren laster; ez dago konputagailurik tamaina horretako taulekin datagramak megabit edota gigabit abiaduran prozesatzeko gai dena.

Arazoa konpontzeko, maskarak erabiltzen hasi zen bideak elkartzeko bideratze-tauletan. Aurreko atalean ikusi dugu nola erabiltzen diren maskarak erakunde baten barruan azpisareak bereizteko (*subnetting*). Beste ikuspuntutik hartuta, erakunde baten sare guztien sare-helbideak elkartzeko ere balio du maskarak: hori da 16 C motako sare-helbideak biltzen dituen erakundearen kasua. Horri *supernetting* edota CIDR (Classless InterDomain Routing) helbideratzea deitu zitzaion, teknika hori C motako helbide sortak erakunde bakar bati esleitzeko erabiltzen zenean. Egun, klaserik gabeko helbideak erabiltzen dituen Interneten, bestelako erabilera du teknika horrek: benetan erakunde desberdinekoak diren sare-helbideak elkartzeko bideratze-tauletako bide bakar batean. Horri bide-elkarketa deritzo, Interneteko ardatz-sareko bideratze-taulak erabilerraza izaten jarraitzeko funtsezkoa izan den teknika.

Bideratze-elkarketa funtsezkoa da bideratze-taulen tamaina murrizteko.

Bide-elkarketaren ahalmen osoaz baliatzeko, irizpide geografikoak hartu behar dira kontuan IP helbideak esleitzeko. Gogora ekar dezagun IP helbideen banaketa erregistratzaileen artean. RIR bakoitzak kontrolatzen dituen IP helbideek jarraituak izango beharko lukete, hutsunerik gabekoak, edo, beste era batean esanda, maskara bakar batekin bateragarriak. Egoera ideal batean, posible litzateke RIPE, ARIN, LACNIC edo APNIC eremuan dauden erakunde guztien sareak elkartzea maskara egokia erabiliz. Internet hasiera-hasieratik mundu mailako sarearte gisa planifikatu izan balitz, IP helbideak irizpide geografiko horrekin banatuko ziren hastapenetik, eta RIR bakoitzeko sare guztiak bide bakar batekin identifikatuko ziren beste eremuetako ardatz-sareko bideratzaileetan. Ez zen hala gertatu, eta helbide sorta asko logika geografiko horretatik at daude; hala ere, CIDR helbideratzearekin hasi zenetik, irizpide geografikoa

erabili izan da, bide-elkarketa ahalbidetzeko eta bideratze-taulen tamaina gutxitzeko asmoz.

■ Helbide fisikoa lortu: ARP protokoloa

Bideratze-taulatik IP prozesuak lortuko duena IP helbide bat da, datagramak bisitatu behar duen hurrengo makinarena dena (bideratzaile batena edo bere helburuko konputagailuarena). Orduan, IP prozesuak datagrama eman behar dio beheko mailako prozesuari, sarbide-mailarena egiten duenari, berak trama bat (batzuetan pakete bat, edo zelula batzuk) eraiki dezan eta sarean sar dezan. Sarbide-mailako prozesu horri, datagramaz gain, datagrama horren sareko helburuko helbidea eman behar zaio. Hau da, sareko helbide bat eman behar zaio (ez sarearteko helbide bat), saretik ateratzeko bideratzailearena edo helburuko konputagailuarena dena. Horrelako helbide bati helbide fisikoa deitzen zaio (gogoan izan kapitulu honen 2. atalean ikasitakoa).

Beraz, IP mailako prozesuak bideratze-taularen bidez lortutako sarearte-helbideak eta sare-mailako prozesuari eman behar dizkion helbide fisikoak nolabait lotu beharko ditu. Hori egiteko modu bakarra makinak duen sare-interfaze bakoitzeko itzulpen-taula bat izatea da, non interfaze horren bidez atzigarri dugun sarean dauden makina guztien IP helbideei dagozkien helbide fisikoak ditugun. Beraz, IP datagrama bakoitzaren prozesua, laburtuta, ondoko hau da:

1. Bideratze-taulatik dagokion hurrengo IP helbidea eta sare-interfazea lortu.
2. IP helbide horri dagokion helbide fisikoa itzulpen-taulan lortu.
3. Sarbide-mailari datagrama, helbide fisikoa eta interfazea eman.

Nola eraiki itzulpen-taula horiek? Hori egiteko era zuzena eskuz egitea da, sareko konputagailu bakoitzean. Sareko helbide fisikoak nahiko egonkorrak direnean ez da irtenbide txarra, beharbada. Baina hori ez da, askotan, benetako egoera. Sare lokaletan, adibidez, maiz konektatzen dira makina berriak sarean, edo konputagailu bati sare-txartela aldatzen zaio. Kasu horietan, berriro eskuz, eta berriro sareko konputagailu guztietan, eguneratu beharko genituzke itzulpen-taulak. Hobe dugu lan hori automatikoki egitea.

Automatizazio hori sare bakoitzean ezberdina izango da, sare bakoitzak barneko funtzionamendua eta helbide-egitura berezkoa dituenez. Adibidez, ATM helbideak eta Ethernet helbideak oso ezberdinak dira, baita bi sare mota horien barneko funtzionamendua ere (bata sare kommutatua da, eta bestea difusioko sarea). Beraz, sarearteko helbidea eta helbide fisikoaren arteko itzulpena datagrama birbidaltzeko erabiliko den interfazearen araberakoa izango da. Orokorrean, ondoko hiru era hauetako sare-interfazeak izango ditu sarearteko nodo batek:

- Puntutik punturako lineak (*point to point*). Etxeko konputagailua Internetera konektatzeko erabiltzen dugun interfazea horrelako linea bati dago lotuta: sare telefonikoaren bidez, edo ADSL konexioaren bidez, ISP (*Internet Service Provider*) batekiko lotura zuzena izan ohi dute. Beste alde batetik, urruti dauden bi sareen arteko konexioek ere, askotan, horrelako linea bat izaten dute. Lineako bi muturretan, bi sareak elkar konektatzen dituzten bi bideratzaileak egongo dira.

- Difusioko sare batekiko konexioa. Hori da hain ohikoa den Ethernet txartelaren kasua, baita FDDI edota Token Ring sareen kasua ere.
- Linea kommutatu baterako interfazea, WAN (*Wide Area Network*) batekiko konexioa dena. Hori da X.25 sare zaharren kasua, edota gaur egun gehiago erabiltzen diren ATM eta Frame Relay lineenak.

Puntutik punturako lineetarako ez dago itzulpen-taularen beharrik, beraren sare-interfazetik zuzenean atzigarri dagoen konputagailu bakarra baitago.

Difusio-sareetan bai beharko da itzulpen-taula sortzeko eta eguneratzeko era automatikoa. Horretarako ARP protokoloa sortu da (*Address Resolution Protocol*). Protokolo hori erabiliz, sareko konputagailuak komunikatzen dira, beraien helbide fisiko eta IP helbidea elkarri jakinarazteko. Protokoloaren funtsezko funtzionamendua ondoko hau da:

- Pizten den konputagailuak, ARP difusioko mezu baten bidez, bere helbide fisikoa
- eta IP helbidea sarean zehar iragartzen ditu. Horrela, dagoeneko sarean dauden beste konputagailu guztiek etorri berriaren berri izango dute, eta beraien itzulpen-tauletan sartuko dute (**ARP taula** izenekoan).
- Dena dela, ARP taula cache moduan kudeatzen da, eta sarrera bakoitzak iraupen mugatua du. Horregatik, ARP taulan IP helbide baten itzulpena aurkitzen ez badugu, sarean zehar ARP eskaera bat hedatu beharko da, berriro ere sareak duen difusio ahalmena erabiliz.

Ondoko irudi honetan aurreko adibideetan erabilitako konputagailuaren ARP taula ikus dezakegu, Linuxeko `arp` komandoa erabiliz lortua.

2.10 irudia: ARP taula.

Benetan interesatzen zaizkigun irudiko taulako zutabeak lehenengoa (*Address*) eta hirugarrena dira (*HWaddress*). Lehenengoan IP helbide bat agertuko da beti, eta bestean helbide horri dagokion helbide fisikoa.

Ethernet sareetako itzulpen-taula ARP protokoloaren bidez eraikitzen da. Horregatik ARP taula edo ARP cache esaten zaio.

Azkenik, WANekiko linea kommutatuen kasua berezia da. Teorian, sare kommutatuan dauden beste konputagailu guztiak atzigarriak dira gure ATM edo FR txartelaren bidez. Benetan horrela balitz, IP helbide eta helbide fisikoaren arteko itzulpena asko zailduko litzaiguke, horrelako sare batean ehunka edota milaka konputagailuak egon baitaitezke konektaturik, baina sare-protokolo horietan ez dago difusio-ahalmenik (trafiko handiegia sortuko baitzuen sarean). Baina, konexio horietan zirkuitu birtualak definitzen dira normalean, eta zirkuitu birtual horien beste muturrean dagoen konputagailuari soilik bidali dakizkioke datagramak. Txartel batean zirkuitu birtual bakarra badago definituta, eta, askotan, hala izaten da, puntutik punturako lineekin bezala lan egin behar da: ez dago itzulpena egiteko beharrik, helburu posible bakarra baitago interfaze horren bidez. Zirkuitu birtual bat baino gehiago dagoenean, zirkuitu birtualaren identifikazioak egiten du helbide fisikoarena, eta, beraz, zirkuitu birtual baten identifikazioa lortu beharko genuke birbidali behar den datagramari dagokion hurrengo urratseko IP helbidetik (bideratze-taulako *gateway* zutabetik ateratakoa). Hala ere, zirkuitu bakoitza aparteko interfaze bat bezala kudeatzen du sistema eragileak, eta, beraz, bideratze-taulan, bereizita agertzen dira txartelari dagozkion zirkuitu guztiak. Adibidez, gerta daiteke (eta normalena litzateke) 2.3 taulan agertzen diren `atm0` eta `atm1` interfazeak ez izatea benetan bi txartel desberdin, txartel berean definituta dauden bi zirkuitu birtual baizik. Hala balitz, berriro, ez dago itzulpena egiteko beharrik, bideratze-taulan zuzenean izango baitugu aukeratutako bideari dagokion zirkuitu birtuala.

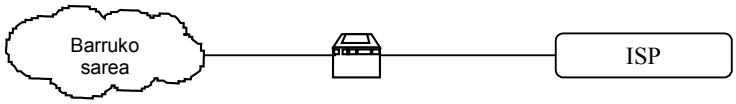
■ Bideratzea Interneten

Orain arte bideratze-taulak nolakoak diren eta nola erabiltzen diren ikusi dugu. Baina, nola eraikitzen dira? Galderaren erantzuna taula erabili behar den makinaren araberakoa da.

Erabiltzailearen konputagailu bat baldin bada, bideratze-taula ez da inoiz izango 2.9 irudian agertzen dena baino askoz konplexuagoa. Horrelako taulek lerro batzuk besterik ez dute izango eta, gainera, oso taula egonkorrak dira: beren edukia oso gutxitan aldatzen da denboraren poderioz, inoiz aldatzen bada. Kasu hauetan taulak eskuz betetzen dira, sistema konfiguratzen denean, eta eguneratzea ere, egin behar denean, eskuz egiten da. Linux sistemetan, adibidez, *route* komandoa erabiliz egiten da.

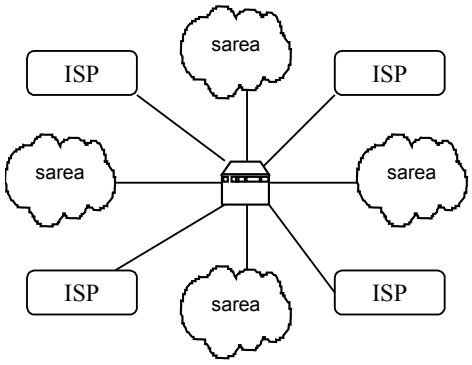
Makina bideratzaile bat baldin bada, gauzak konplikatu egin daitezke. Bideratzaile hori sarearteko periferian baldin badago, eta oso sare gutxitara konektatuta baldin badago, taulen konfigurazioa eskuz egin daiteke. Adibidez, bideratzaile askok sare baten irteerarena besterik ez dute egiten, sarea ISP batekin konektatuz. Bideratzaile horien

taula sareko konputagailu batena bezain sinplea eta egonkorra da. Bi sare-interfaze besterik ez dira egongo, eta taula betetzeko aplikatu behar den logika bakarra hau da: barruko trafikoa sareari dagokion interfazetik bidali, eta beste guztia ISPrekiko interfazetik atera. Funtsean, kanporako datagramek ez dute beste biderik, bideratzaile honek bideratzaile bizilagun bakarra baitu. Hori da 2.11 irudian agertzen den egoera.



2.11 irudia: periferiako bideratzailea. Bere bizilagun bakarra ISPko bideratzailea da.

Baina bideratzaileak sare asko elkarrekin konektatzen baditu, helburu batera heltzeko bide bat baino gehiago baldin badago eta, gainera, bide horien baldintzak maiz aldatzen badira, taulak ez dira hain sinpleak, ez betetzeko, ez eguneratzeko. Horrelako egoera sareartearen ardatza osatzen duten bideratzaileetan aurkitzen dugu, adibidez, 2.12 irudikoan. Kasu horietan, taulak betetzeko eta eguneratzeko prozedura automatikoa behar da.



2.12 irudia: ardatz-sareko bideratzailea. IP helburu-helbide bakoitzeko bide asko egon daitezke.

Interneten, sareak eta bideratzaileak hierarkikoki antolatuta daude. Sistema autonomo baten sarearteko ardatza osatzen duten bideratzaileak **barruko bideratzaileak** dira, eta beste sistema autonomoetako bideratzaileekin konektatzen direnak **kanpoko bideratzaileak** dira. Bereizketa hori ez da zorrotza, eta bideratzaile bat barrukoa eta kanpokoa izan daiteke aldi berean (hori da 2.12 irudiko bideratzailearen kasua).

■ Barruko bideratze-protokoloak

Sistema autonomo baten barruko sareen arteko bideak askotarikoak eta aldakorrak baldin badira, barruko bideratzaileen bideratze-taulak betetzeko eta eguneratzeko era automatikoren bat beharko dugu. Zehatz-mehatz ondoko hau egin beharko da:

1. Bideratzaile bakoitzak berari lotuta dauden sareei buruzko informazioa jasoko du (zeintzuk diren IP helbide atzigarriak sare horren bidez, horren kostua, eta abar).

2. Beste bideratzaileekin informazio hori elkarrekin trukatu, eta horrekin guztiarekin taula bete, algoritmoren bati jarraituz. Algoritmoek egiten dutena sareartea grafotzat hartu eta grafoaren abaguneen arteko bideak bilatzea da.

Bideratzaileen arteko komunikaziorako protokolo bat definitu behar da. Protokolo horrek baldintza hauek ezarriko ditu:

- Bideratze-taulak betetzeko zein algoritmo erabiliko den. Honek hurrengoa baldintzatzen du.
- Bideratzaileek elkarrekin trukatuko dituzten mezuak nolakoak izango diren, zer informazioa bidaliko den mezu bakoitzean, noiz bidaliko diren, eta zer ordenari jarraituz bidalitako mezuen artean. Hau da, edozein konputagailuren arteko komunikaziorako protokoloak ezartzen duena.

Bideratzaile baten taulak aldakorrak direnean, taulak betetzeko eta eguneratzeko prozedura automatikoa behar da. Bideratze-protokoloek ezartzen dute prozedura hori.

Interneten sistema autonomoen barne bideratzerako protokolo batzuk definitu dira. Protokolo horiek betetzea ez da nahitaezkoa; gomendioak dira. Finean, hau barruko arazoa da eta, beraz, sistema autonomoaren kudeatzaileari bakarrik dagokio hori antolatzea. Interneteko gomendioa ez den beste protokoloak erabiltzea badago, horrek ez baitie kanpoko sareei inongo trabarik egiten. Baina normalean Interneteko gomendioak erabiltzea da errazena, dagoeneko software garatuta eta frogatuta dagoelako.

Ondoko hauek dira sistema autonomoaren barruko bideratzerako gehien erabiltzen diren protokoloak:

- RIP (Routing Information Protocol, RFC 1058, 1723).

  Protokoloa hau dagoeneko zahartuta dago, baina, hala eta guztiz ere, oso erabilia izaten jarraitzen du. Taulak eraikitzeko eta eguneratzeko, bideratzaile bizilagunek bideratze-informazioa elkarri bidaltzen diote periodikoki (30 segundoro, gutxi gora behera). Bideratzaile bizilagunak elkarren artean sare edo konexio bat besterik ez dutenak dira. Erabilitako algoritmoa distantzia-bektoreko bideratzearena da (*distance vector routing*).

- OSPF (Open Shortest Path First, RFC 2178).

  RIP zaharra ordezkatzeko diseinatutako protokoloa da. Berriro ere bideratze-informazioaren trukaketa periodikoan datza, baina orain sistema autonomoko barruko bideratzaile guztien artean egiten dute bidalketa. Hau da, bideratzaile batek sistema autonomoko beste barruko bideratzaile guztiei bidaltzen die bere informazioa, eta ez bideratzaile bizilagunei bakarrik. Erabilitako algoritmoa ibilbide laburrenarena da. RIPekin alderatuz, ondoko hauek dira hobekuntzak:

- Helburu bakoitzeko bide bat baino gehiago kalkulatzen du.
- Bideratze-informazioaren trukaketak segurtatzeko neurriak hartzen ditu.
- Bideen kostua datagrama motaren araberako neurriarekin baloratzen du (zerbitzu-motaren eremuaren arabera).
- Talde-bideratzea egiten du (multicast).

OSPFk barruko bideratzaileak hierarkikoki sailkatzen ditu, 4 kategoriatan. Honek asko zailtzen du protokoloa.

- EIGRP (Enhanced Internal Gateway Routing Protocol).

Hau ere RIP ordezkatzeko diseinatutako protokoloa da, baina ez da Interneten gomendio 'ofiziala' (RFCtan argitaratuta), enpresa batek egindako proposamena baizik (Cisco Systems). Enpresa horrek egiten dituen bideratzaileak gehien erabiltzen direnak direnez, bere proposamenak badu garrantzia. OSPF protokoloaren hasierako 'O' hizkia (*open* hitzari dagokiona) protokolo honek eragin du; EIGRP enpresa batena izanez, proposamen 'itxia' da. OSPF, aldiz, 'irekia' da (gogoan izan kapitulu honen 2. atalean ikusitako sistema itxien eta irekien arteko aldea). Protokolo honen ezaugarri hauek dira nabarienak:

- Bideratze-informazioa bideratze bizilagunek bakarrik bidaltzen diote elkarri.
- Distantzia-bektoreko bideratze-algoritmoa erabiltzen da, RIPen bezala.
- Trukaketa ez da periodikoki egiten, bideratzaile baten taulan aldaketaren bat sortzen denean baizik. Horrek asko murrizten du bideratze-protokoloak sortutako trafikoa.
- Bideratze-erabakiak hartzeko neurri ezberdinak hartzen dira kontuan (atzerapena, transmisio-abiadura, fidagarritasuna, trafiko-zama...), eta sare-kudeatzaileak erabakitzen du neurri bakoitzaren pisua erabakia hartzean.
- Bideratze-informazioa bidalketen segurtasunerako prozedurei jarraitzen die.

■ Sistema autonomoen arteko bideratzea

Kanpoko bideratzeileen lana eta barrukoena oso ezberdina da. Bion kasuan arazoa datagramak ahal den biderik onenetik bidaltzea da, baina 'onena' zer den erabakitzeko irizpideak oso izaera ezberdinekoak dira batean eta bestean. Barruko bideratzerako irizpideak teknikoak dira. Kanpoko bideratzean teknikoak ez diren beste irizpideak ere kontuan hartu behar dira; irizpide ekonomikoak, batez ere, baina politikoak edo segurtasunezkoak ere bai. Adibidez, konpainia telefoniko batek agian ez du nahi izango bere bezeroa ez den ISP baten datagramak garraiatu, bere sarea datagrama horien biderik motzenean egon arren. Honek taulak betetzeko eta eguneratzeko behar den informazio-mota eta mekanismoak guztiz aldatzen ditu.

Barruko bideratzean bezala, Interneten RFC batzuk argitaratu dira, kanpoko bideratzaileen arteko komunikazioak estandarizatzeko. Berriro ere, estandar horiek gomendioak besterik ez dira, baina 'de facto' estandarrarenak egiten dute.

Sistema autonomoen arteko bideratze-protokolo aitzindaria EGP da (Exterior Gateway Protocol), baina nahiko baztertuta dago gaur egun. Erabiltzen dena bere ordezkoa den BGP da (Border Gateway Protocol, RC 1771, 1772, 1773). Ondoko hauek dira bere ezaugarri nagusiak:

- Bizilagunek bakarrik bidaltzen diote informazioa elkarri.
- Bidaltzen dena ez da bideari buruzko informazioa (luzera, kostua...), bidea bera baizik (zein sistema autonomo zeharkatu behar diren helburura heltzeko).
- Taulak ez dira automatikoki eguneratzen: sare-kudeatzaileak eguneratzen du eskuz, bizilagunek emandako informazioaren arabera. Beraz, taulak sortzeko ez da inongo bideratze-algoritmorik aplikatzen.

Oso bideratzaile gutxik erabiltzen dute BGP Interneten, baina erabiltzen dutenak oso garrantzitsuak dira. Sistema autonomo gehienak periferikoak dira, hots, datagramen iturburua edo helburua dira. Sistema autonomo horien kanpoko bideratzaileek ez dute BGP behar, beren kanpoko konexioak bat edo bi izaten direlako eta, beraz, ez dago aukeratzeko bide asko. Interneten ardatza osatzen duten sistema autonomoen kasua ezberdina da. Sistema horiek, nolabait, Interneteko handizkariak dira, eta garraiatzen duten trafikoa igarotzekoa da. Beste sistema autonomoekiko konexio ugari dituzte, eta kontuz egin behar dute kanpoko bideratzea. Hauek dira BGP erabiltzen dutenak.

Kanpoko eta barruko bideratzeak oso ezberdinak dira. Ondorioz, batean eta bestean bideratze-protokolo ezberdinak erabiltzen dira.

■ Trafiko-trukaguneak

Bere bezeroei Interneterako sarbidea emateko, ISP batek izan behar du, noski, Internetekiko konexio bat. Konexio hori lehenengo mailako Internet hornitzaile batekin edo gehiagorekin kontratatutakoa izango da normalean. Lehenengo mailako hornitzaile horiek —*Tier 1* delako telekomunikazio-konpainia handiak—handienak dira Internet handizkarien artean. Haiek osatzen dute Interneten ardatz-sarea: elkarren artean konektaturik daude Internet osorako bideak gauzatzeko, eta haien artean hitzarmenak sinatzen dituzte (*peering*), beren bezeroen arteko trafikoa bideratzeko. Beraz, maila goreneko hornitzaile horiek hurrengo mailako ISPei (*Tier 2* izenekoei) saltzen diete Internet globala, eta horiek, berriz, beren bezeroei (Interneten erabiltzaileei zuzenean, edo, agian, Interneten hornitzaile txikiagoei, *Tier 3* ISPak, alegia). Beraz, ISPak era hierarkikoan daude antolaturik: ISP batek bera baino handiagoa den beste handizkari batengana bideratzen du bere gorako trafikoa (*upstream*, hau da, bere saretik kanpora, Internetera, doana), eta txikiagoak diren bere bezeroengana bideratzen du beherako trafikoa (*downstream*, hau da, kanpotik, Internetetik, datorrena).

ISP hierarkia hori hobeto ulertzeko, har dezagun datagrama bat A izeneko ISP bati lotuta dagoen konputagailu batetik B izeneko beste ISP batekin lotuta dagoen beste konputagailu batera joan behar duena, eta suposa dezagun ISP bakoitzak bere maila goreneko hornitzailearekin duela Internetekiko konexio globala. Datagrama ISP batetik, bere hornitzaile globalaren sarera igaroko da; horretatik, beste hornitzaile baten sarera; handik, helburuaren ISPra, eta horrek helburuko konputagailuari helaraziko du. Baina hobe litzateke ertaineko bi ISPak zuzenean konektaturik baleude, hierarkian zirkuitulabur bat sortuz: datagrama azkarrago helduko zen bere helburura. Zoritxarrez, ez da bideragarria munduko ertaineko ISP guztiak zuzenean elkar konektaturik egotea, oso garestia izango zelako ISP bakoitzarentzat. Horregatik, hain zuzen ere, badira maila goreneko hornitzaileak: ertainekoek haietako batekin edo batzuekin kontratazen du bere gorako trafikoaren irteera-linea bat, eta nahikoa da.

Dena dela, horrelako ISP batzuen arteko zirkuitulaburren kostua justifika daiteke bi ISPren arteko trafikoa handia denean. Beraz, ISP batek ez ditu lineak ezarriko beste ISP guztiekin, baina, agian, jarriko lituzke bere bezeroekiko trafiko handia duten beste ISP batzuekin. Are hobea litzateke linea bakar batekin konektatuko balitz beste ISP horiekin; hori da, hain zuzen, trafiko trukaguneek, ingelesez IXP (*Internet eXchange Point*), ahalbidetzen dutena. Trafiko-trukagune bat sare lokal bat da; askotan, abiadura handiko Ethernet bat, non ISP asko konektatuta baitaude. Hala, beren arteko trafikoa zuzenean truka dezakete, maila goreneko hornitzaileen sareetatik igaro gabe. Honako abantaila hauek dakartza horrek:

- Trafiko trukagunean parte hartzen duten ISPen bezeroen datagramak azkarrago heltzen dira beren helmugara, trukagunean dauden beste ISPtara doazenean. Beraz, bezeroek zerbitzu hobea jasoko dute.
- Hori lortzeko, linea bakarra behar dute ISPek, trukagunearekin lotzen dituena. Hau da, ez dute linea bat ezarri behar trafikoa trukatu nahi duen beste ISP

bakoitzarekin, eta, beraz, irtenbide horren bideragarritasun ekonomikoa askoz eskuragarriago bihurtzen da.

- Are gehiago: ISP baten gorako trafikoa asko murritz daiteke, trukagunean zehar bideratuko delako, eta ez bere Internet handizkariaren bidez. Kasu batzuetan, posible izango da handizkariarekin kontratatutako trafikoa jaistea, eta, horrekin batera, handizkariari ordaintzekoa.
- Ez da bitxia Interneten erabiltzaile batek ISP batekin baino gehiagorekin konexioa kontratatzea. Horregatik, askotan, datagramaren helburua trukagunean dagoen ISP baten baino gehiagoren bidez joan daiteke. Kasu horietan, trukaguneak back-up lineak ditu, alegia, bide-erredundantziak.

Hala ere, trukaguneetan, arazoak sor daitezke parte-hartzaileek elkarri bideratutako trafikoa kontrolatzen ez bada. Horrelako kontrolik ez badago, gerta daiteke A izeneko parte-hartzaile maltzur batek bere gorako trafiko guztia B parte-hartzailera bidaltzea, nahiz eta datagramen helburua ez egon han. Hala, A-k ez du kontratatu behar inongo handizkarirekin bere gorako trafikoaren irteera, B-ren lepotik bideratuko du eta.

Horrelako bizkarroikeria sahiesteko, trafikoa elkarren artean trukatzeko hitzarmenak (ardatz sareko aipatutako *peering* akordioak bezalako hitzarmenak) behar-beharrezkoak dira trukagunean. Hitzarmen horiek trukaguneko bideratze-tauletan irudikatuko dira: hitzartutako trafikoa soilik bideratuko da parte-hartzaile baten sarearen zehar. Hitzarmen horiek ISPen arteko kontua bada ere, trukaguneak eska dezake trukaguneko beste ISPekiko hitzarmen kopuru minimo bat edukitzea.

Trafiko-trukaguneak ertaineko ISPek trafikoa elkarren artean trukatzeko sare-guneak dira, Interneten sare-ardatzatik igaro gabe. Hala, ISPek kostuak murrizten dituzte, trafikoa gutxitzen da Interneten, eta datagramak lehenago heltzen dira beraien helburura.

Euskal Herrian, oraingoz, trafiko-trukagune bakarra dugu, Euskonix izenekoa (www.euskonix.net). Europan asko daude, gehienak Euro-IX (European Internet Exchange Association, www.euro-ix.net) elkartearen inguruan bilduta.

6 Sareartearen monitorizazioa: ICMP protokoloa

IP protokoloak ematen duen zerbitzua datagramakoa denez, sareartearen kudeaketa zaila da. Hala eta guztiz ere, sareartearen monitorizazioa egitea badago. Hau da, sarearteko bideratzaileetan gertatzen denaren berri jaso dezakegu, baldin eta bideratzaile horiek informazio hori emateko prest badaude. Adibidez, bideratzaile batek datagrama baten TTL balioa agortuta dagoela atzematen badu, zakarrontzira botako du; bideratzailea "jatorra" bada, datagrama igorri duenari bere bidaiaren amaieraren berri emango dio.

Horrelako komunikazioak gauzatzeko bere garaian ICMP protokoloa definitu zen (Internet Control Message Protocol, RFC 792). Askotan ICMP IP protokoloaren zati bat balitz bezala hartzen da, baina ez da horrela. IPren protokolo laguntzaile bat da, sarearte mailan kokatua. Honekin nahaste-borraste teorikoa sor daiteke, ICMP mezuak IP datagramen barruan, informazioaren eremuan sartzen direlako eta, ondorioz, ICMPk sarearte-mailatik gorako maila baten protokoloa dirudi.

ICMP oso protokolo sinplea da: definitzen duen gauza bakarra mezuen formatua eta erabilera da (noiz bidali). Ez da inongo prozedurarik definitu behar mezu horiek bidaltzeko, datagrama batean sartu eta datagrama hori bidali besterik ez delako. IP duten konputagailuek eta bideratzaileek ez daude ICMP betetzera behartuta, baina komenigarria da betetzea. Bideratzaile batzuek ez diete hartutako ICMP mezuei jaramonik egiten, eta haiek ere ez dute ICMP mezurik bidaltzen, baina portaera hau ez da ohikoena.

ICMP protokoloak bideratzaileek eta erabiltzaileen konputagailuek erabiltzen dituzte, beren sarearte-mailan gertatutakoaren berri emateko. Sare-kontrolerako aplikazioek askotan erabiltzen dituzte.

Hain ezaguna den *ping* programa ICMPn oinarrituta dago. Konputagailu bat sareartean zehar atzigarri dagoen ala ez jakiteko egiten dugun lehenengo gauza berari *ping* egitea da. *Ping*-ek adierazitako konputagailuari ICMP oihartzun-eskaera bat bidaltzen du eta horren erantzunaren zain (beste ICMP mezua dena) gelditzen da. ICMPn oinarritzen den beste programa ezaguna *traceroute* da, konputagailu batetik bestera joateko datagramek jarraitzen duten bidea ezagutzeko erabiltzen dena. Honek 'TTL agortuta' izeneko ICMP mezua erabiltzen du (*TTL expired*, ingelesez; izan ere, ICMP mezuen izen 'ofizialak' ingelesezkoak dira).

7 IPv6

90eko hamarkadaren hasieran hasi ziren IPv4 protokoloaren ordezkoa sortzeko ekimenak. Ondorioz, IPv6 diseinatu zen. IPv4rekin alderatuta, ondoko hauek dira bere ezaugarri nagusiak:

- Helbideratzea zabalagoa du. Izan ere, IPv4 helbideak agortzea izan zen protokolo berria sortzeko arrazoi nagusia. IPv6 helbideak 16 bytekoak dira (128 bit), beraz, IPv4 helbideena baino 2^{12} aldiz handiagoa da IPv6 helbideratze-ahalmena. Helbide-kopuru honekin Lur planetako edozein hondar apurrek izan dezake bere IP helbidea.
- Bideratzaileen lana are gehiago errazten da. Hau da IPv6 protokoloaren helburuetako bat: bideratzaile azkarragoen bidez, trafikoa handitzeari aurre egitea. Hori lortzeko bideak bi dira: bideratzaile azkarragoak ekoiztea, ahal den gehiena hardwarearen bidez eginez, eta datagrama bakoitzaren tratamendua

arintzea. Bigarren hau protokoloak ezartzen du. IPv6ren ondoko ezaugarri hauek sinplifikatzen dute datagramen prozesamendua:

- Goiburukoaren luzera finkoa da. Honek eremuen irakurketa azkartzen du, eremu bakoitza beti toki berean dagoelako.
- Ez dago inongo errore-kontrolik. Lehenago ikusi dugunez, IPv4k goiburuan egiten duen errore-kontrolak ez du ezertarako balio eta, gainera, bideratzaile bakoitzean kalkulu softwareak berregitera behartzen du (gogoan izan TTL aldatzen dela bideratzaile bakoitzean eta, beraz, errore-kontrolaren eremua birkalkulatu egin behar dela).
- Bideratzaileetan ez dago datagramak zatitzerik. Zatiketak IPv4 goiburukoa konplexuagoa egiten du (3 eremu sartu behar dira zatiketak egiteko eta datagramak berreraikitzeko) eta, berriro ere, bideratzaileen lana zailtzen du. IPv6n, datagrama bat handiegia baldin bada, bideratzaileak datagramaren igorleari kontrol-mezu bat bidaliko dio (ICMPv6 protokoloaren bidez), horren berri emanez. Igorleak berak jatorrizko datagrama zatitu eta datagrama txikiagoetan bidali beharko du.

- Trafiko-motak bereizteko mekanismoak hobetzen ditu, *fluxuaren* kontzeptua bereganatuz eta IPv4ren goiburuko *zerbitzu-mota* eremuaren luzera handituz. Datagramak fluxuetan elkar daitezke, bideratzaileek igorleak modu berezian maneiatzeko eskatzen duten datagramak identifika ditzaten. Adibidez, audio eta bideo transmisioak fluxu bezala tratatzea nahi izan liteke. Bestalde, ohiko datu-aplikazioak (fitxategi-transmisioa edota posta elektronikoa) ez dira fluxuak bezala tratatuko. Fluxuen bidez QoS lortzeko bideak irekitzen dira Interneten. Erabiltzaile batek bere datagramak bideratzaileen ilaretan lehentasunezkoak izatea behar badu, datagrama horiek lehenengo mailako fluxuko etiketa eraman dezaten ordaindu dezake. Argi dagoena, edozein modutan, IPv6ren diseinatzaileek fluxuen artean bereizteko beharra aurreikusi zutela, fluxuaren esanahi zehatza ondo definitu ez bazuten ere.

  Bestalde, trafiko-klasearen eremuaren bidez (IPv4-ko zerbitzu-motako eremua), fluxu baten barnean datagrama batzuei lehentasuna eman dakieke.

Hala ere, urteak dira IPv6 definitu zela eta oraindik bere erabilpena oso eskasa da. Ondoko hauek dira zabaltzeko dituen oztopoak:

- Sareko ekipamenduko softwarea aldatzea sarea bera aldatzea da eta, beraz, erabiltzaileei beren softwarea ere aldatzea dakarkie. Hori ezin da egun batetik bestera egin: migrazio luze eta zaila izango da. IPv6 ezartzeak bideratzaileak aldatzea suposatzen du, baita sarearen erabiltzaileen konputagailuen sistema eragileak ere, hor baitago inplementatuta sarearte-maila. Hori guztia kostu handia da, sarearentzat eta erabiltzaileentzat, eta ez batak ez besteek ez dute migrazio hori egingo benetan ezinbestekoa ez bada.
- Horra hor bigarren oztopoa: IPv6 ez da ezinbestekoa. IPv4 espero zena baino dezente gehiago ari da irauten, bere gabezia guztiekin. Arazorik larriena, helbideak amaitzearena, maskaren erabilpenarekin eta helbide-itzulpenarekin desagertu egin da. Azken horrek, NAT protokoloaren

bidez (Network Address Translation), sistema autonomoko konputagailu guztiek IP helbide bakar bat kontsumitzea posible egiten du.

IPv4 protokoloaren ordezkoa IPv6 da. Teknikoki, IPv4 baino askoz hobea da, baina bere hedapenak IPv4ren indarra du oztopo.

8 Laburpena

Sareak elkarrekin konektatzeko sare guztiek onartzen duten protokolo komuna behar dugu eta, beraz, sare-arkitekturan maila bat egon beharko da horretarako, sarearte-maila hain zuzen ere. Protokolo komun hori IP da, Internet arkitekturan definitzen dena.

IP protokoloak datagrama-zerbitzua eskaintzen die bere erabiltzaileei (aplikazioak, gure 4 mailako sare-arkitektura esperimentalean). Horrelako zerbitzuak sarearteak QoS ez ematea suposatzen du, baina zerbitzu azkarra eta unibertsala izatea ere bai.

IP helbideek bi zati dute: ezkerreko bitek sarea identifikatzen dute, eta eskuinekoek konputagailua. Bi zatien arteko bereizketa maskaren bidez egiten da. Maskarak erabiliz, sare baten barnean azpisareak definitu daitezke.

Datagramak bideratzeko taulak erabiltzen dira. Igorleak zein bideko bideratzaileek beren bideratze-taulak kontsultatu behar dituzte datagrama bat sarean sartu behar duten bakoitzean. Gero, taulatik ateratako IP helbidea dagokion sarearen helbide batekin lotu behar dute. Helbide hori datagramaren bidean dagoen hurrengo makinaren helbide fisikoa da, sarbide-mailako traman (edo paketean) jarri behar den helburuko helbidea, alegia. Ethernet sareetan, IP helbideen eta helbide fisikoen arteko lotura ARP tauletan islatzen da. Taula horiek ARP protokoloaren bidez betetzen dira.

Bideratze-taulak betetzeko eta eguneratzeko era asko daude. Erabiltzaileen makinenak eta periferiako bideratzaileenak oso sinpleak eta egonkorrak dira eta, beraz, sistemaren kudeatzaileak normalean eskuz betetzen eta eguneratzen ditu. Sare asko atzigarri dituzten bideratzaileen taulak, aldiz, konplexuak izan daitezke, eta eguneratzen zailak. Kasu horietan bideratzaileek bideratze-informazioa elkarri bidaltzen diote, bideratze-protokoloak erabiliz. Sistema autonomo bereko bideratzaileen artean, barruko bideratzaileak direnean, bideratze-protokolo batzuk erabiltzen dira, eta sistema autonomo ezberdinetako bideratzaileen artean beste batzuk. Barruko bideratze-protokoloak irizpide teknikoetan oinarritzen dira, eta bideei buruzko informazioa erabiltzen dute taulak automatikoki eguneratzeko. Kanpoko bideratze-protokoloen irizpideak, aldiz, ez dira teknikoak, eta trukatzen duten informazioa bidean zer sare zeharkatu behar diren da. Informazio horrekin sistemaren kudeatzaileak taulak eguneratzen ditu, eskuz.

IP mailako informazioa hartzeko ICMP protokoloa erabiltzen da. Protokolo honek kontrol-mezu batzuk definitzen ditu, bideratzaileek eta erabiltzailearen konputagailuek gertaera batzuen berri elkarri emateko erabiltzen dituztenak.

IPv4 protokoloaren ordezkoa IPv6 da. IPv4ren gabezia guztiak betetzen dira protokolo berriarekin: helbideratzeko ahalmena askoz handiagoa du, datagramen tratamendua bideratzaileetan asko errazten du, eta QoS lortzeko oinarriak ezartzen ditu. Hala eta guztiz ere, IPv6 protokoloaren arrakasta ikusteke dugu.