

eman ta zabal zazu



Universidad  
del País Vasco

Euskal Herriko  
Unibertsitatea

# Konputagailu-Sareen Oinarriak. Laborategirako eskuliburua.

Egilea(k)

JM. RIVADENEYRA  
ALEX MENDIBURU  
JOSÉ MIGUEL ALONSO

**EUSKARAREN ETA ETENGABEKO PRESTAKUNTAREN  
ARLOKO ERREKTOREORDETZAREN SARE  
ARGITALPENA**

**Argitalpen honek UPV/EHUko Euskararen eta Etengabeko  
Prestakuntzaren arloko Errektoreordetzaren laguntza izan du**

**ISSN 2603-8900**

<u>Sarrera.....</u>	<u>4</u>
<u>1. laborategirako teoria: IPv4 helbideak, ICMP, eta ARP.....</u>	<u>5</u>
<u>1. laborategirako galdetegia.....</u>	<u>10</u>
<u>1. laborategia: Sarrera.....</u>	<u>11</u>
<u>2. laborategirako teoria: Datagramak birbidaltzea.....</u>	<u>21</u>
<u>2. laborategirako galdetegia.....</u>	<u>24</u>
<u>2. laborategia: Birbidaltzea konfiguratzea.....</u>	<u>25</u>
<u>3. laborategirako teoria: DHCP.....</u>	<u>30</u>
<u>3. laborategirako galdetegia.....</u>	<u>33</u>
<u>3. laborategia: DHCP.....</u>	<u>34</u>
<u>4. laborategirako teoria: NAT.....</u>	<u>40</u>
<u>4. laborategirako galdetegia.....</u>	<u>42</u>
<u>4. laborategia: NAT/NAPT.....</u>	<u>43</u>
<u>5. laborategirako teoria: Ipv6.....</u>	<u>49</u>
<u>5. laborategirako galdetegia.....</u>	<u>57</u>
<u>5. laborategia: IPv6.....</u>	<u>58</u>
<u>6. laborategirako teoria: Suhesiak.....</u>	<u>66</u>
<u>6. laborategirako galdetegia.....</u>	<u>70</u>
<u>6. laborategia: Suhesiak.....</u>	<u>72</u>

## Sarrera

Konputagailu-sareen oinarriak (KSO) irakasgaia Donostiako UPV/EHUko Informatika Fakultatean irakasten den Ingeniaritza Informatikako graduko irakasgaia da (2. mailakoa). Hor, konputagailu-sareen oinarriak azaltzen dira, TCP/IP arkitektura eredutzat hartuz.

Ematen den teoriaren osagarri gisa, zenbait praktika egiten dira laborategian. Laborategi horietan, ikasleak 1. irudian ikusi daitekeen ekipoeekin egiten du lan: Cisco bideratzailea, Linux bideratzailea, Cisco *switch*ak, eta bi konputagailu eramangarri (erabiltzailearen konputagailuak simulatzeko).



**1. Irudia: laborategiko lanpostu bat.**

Praktika hauetan, hainbat kontzeptu lantzen dira. Hain zuzen:

- IParen eta azpisarearen arteko lotura ( IP – *Ethernet*). ARP Protokoloa.
- *Wireshark* softwarea. Sarean zehar doazen datagramak harrapatzeko eta aztertzeko tresna (*sniffer*).
- Oinarrizko bideratzea: sare berean, sareen artean.
- DHCP zerbitzua: DHCP zerbitzaria eta DHCP *Proxy*a abiatu.
- NAT zerbitzua.
- IPv6 konfigurazioa: *Stateless* konfigurazioa eta IPv6-IPv4 tunela
- Suhesien oinarrizko konfigurazioa: *iptables*ak (Linux) eta ACLak (Cisco).

Dokumentu honetan, praktiketan erabiltzen den materiala biltzen da. Praktika bakoitzeko hiru dokumentu daude. Lehenean, laborategi horretan landuko den teoria azaltzen da. Bigarrena laborategia prestatzeko diseinatuta dagoen galdetegi bat da, ikasleak bete behar duena laborategira etorri baino lehen. Hirugarrena praktika betetzeko enuntziatua da, ikasleei banatzen zaiena. Bertan, pausoz pauso adierazten da ikasleak egin beharrekoa, eta galderak txertatzen dira kontrol gisa, ikasleak egindakoa aztertu eta ulertu dezan.

# 1. laborategirako teoria: IPv4 helbideak, ICMP, eta ARP

## IPv4 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, 192.33.217.137 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.

### Helbideen egitura

Bigarrenkoz, 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. Honek helbide bakoitzak bi zati dituela adierazten digu. 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 **makinareen 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-maskararen** bidez adierazten da. Sare-maskarak bi era ezberdinetan idazten dira. Lehen gehien erabili izan denak IP helbideen sintaxia du, non sareari dagozkion bitei 1 balioa esleitzen zaien eta interfazeari dagozkionak 0 diren. 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. Bigarren notazio hau gero eta gehiago erabiltzen da, erosoagoa eta interpretatzeko errazagoa baita. Bigarren notazio honetan ere, helbideak sinplifikatu daitezke 0koak kenduz. Notazio honekin batera, IP helbideen egituraketa izendatzeko beste terminologia ere zabaldu da, eta oso ohikoa da sare-helbidea **sare-aurrezenbakia** deitzea, eta sare-maskararen ordez, **aurrezenbakiaren luzera** aipatzea.

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.

### Azpisareak

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<sup>1</sup>. 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 gero ikusiko ditugun bideratze-lanak errazteko, sistema autonomo, edo orokorrean, IP sare baten barruan dauden beste azpisareak identifikatzea. Horretarako maskarak erabiltzen dira. Beraz, maskarak sare-helbidea eta interfazearen identifikazioa bereizteaz gain, sarea azpisareetan banatzeko ere balio du.

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 **00000000** 00000000

Eta, horrela, honako 16 azpisare-helbide hauek lortuko ditugu, notazio hamartar puntudunez adierazita:

155.233.0.0/20	155.233.96.0/20	155.233.192.0/20
155.233.16.0/20	155.233.112.0/20	155.233.208.0/20
155.233.32.0/20	155.233.128.0/20	155.233.224.0/20
155.233.48.0/20	155.233.144.0/20	155.233.240.0/20
155.233.64.0/20	155.233.160.0/20	
155.233.80.0/20	155.233.176.0/20	

Horietako edozein 10 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.

---

<sup>1</sup> Zehatza izanda, Interneteko sistema autonomo bat sarearteko bideraketarako unitate bat da. Izan ere, gerta daiteke entitate administratibo bakar batek kudeatutako sareek sistema autonomo bat baino gehiagotan banatuta egotea. Sistema autonomoaren definizioa RFC1930 agirian dago.

Irakurleak suposatuko duen bezala, ez dago inongo trabarik azpisareak ere beste azpisareetan banatzeko. Argiago ikusteko, demagun adibideko 155.233.0.0/16 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 egokitzeko 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 hartzeko ahalmenarekin. Ondoan, helbidearen hirugarren bytearen 8 balio bitar posibleak ditugu (bigarren azpisare-maskararenak nabarmenduta), baita horietatik sortzen diren 8 azpisare-helbideak ere (hauek, notazio hamar puntudunez idatzirik):

0001 **0000** → 155.233.16.0/230001 **1000** → 155.233.24.0/230001 **0010** → 155.233.18.0/230001 **1010** → 155.233.26.0/230001 **0100** → 155.233.20.0/230001 **1100** → 155.233.28.0/230001 **0110** → 155.233.22.0/230001 **1110** → 155.233.30.0/23

Horietako edozein 3 hartuko genituzke egoitza horren sailak identifikatzeko.

Luzera aldakorreko maskarak erabiltzea deitzen zaio era errekursibo 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 0010 **0000** 0000 → 155.233.18.0/260001 0010 **0100** 0000 → 155.233.18.64/260001 0010 **1000** 0000 → 155.233.18.128/260001 0010 **1100** 0000 → 155.233.18.192/260001 0011 **0000** 0000 → 155.233.19.0/260001 0011 **0100** 0000 → 155.233.19.64/260001 0011 **1000** 0000 → 155.233.19.128/260001 0011 **1100** 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 (erakundeko egoitza



bakoitzeko sareek), beste batzuek, berriz, 23 bitekoa (400 interfaze-identifikadore behar duen sailekoek), eta beste batzuk, 26 bitekoa (50 identifikadore besterik behar ez duten sailekoek).

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.

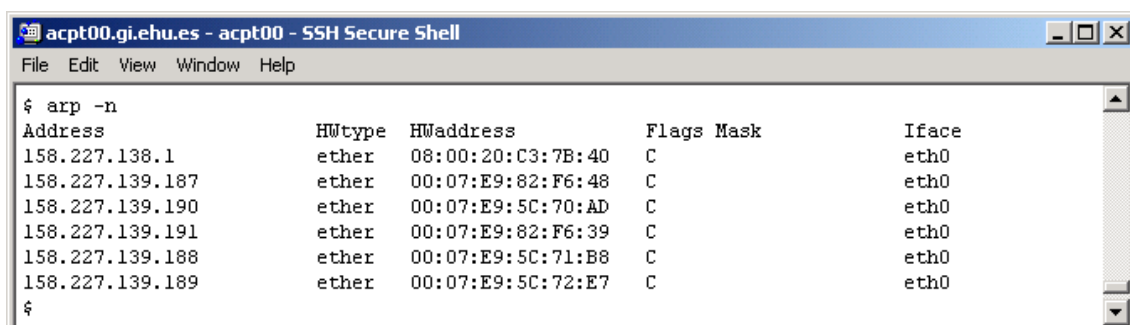
## ARP protokoloa

IP helbide eta helbide fisikoen arteko itzulpen automatikoa egiteko ARP protokoloa sortu da (*Address Resolution Protocol*). Protokolo hori erabiliz, sareko konputagailuak komunikatzen dira, beraien helbide fisiko eta IP helbidea elkarri jakinarazteko eta norberaren itzulpen-taula osatzeko. Ethernet moduko difusio sareetan, 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. Horrela izanik, gerta daiteke interfaze baten itzulpena ez aurkitzea gure ARP cachean, interfaze hori sarean egon arren. 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 konputagailu baten ARP taula ikus dezakegu, Linuxeko `arp` komandoa erabiliz lortua<sup>2</sup>.



Address	HWtype	HWaddress	Flags Mask	Iface
158.227.138.1	ether	08:00:20:C3:7B:40	C	eth0
158.227.139.187	ether	00:07:E9:82:F6:48	C	eth0
158.227.139.190	ether	00:07:E9:5C:70:AD	C	eth0
158.227.139.191	ether	00:07:E9:82:F6:39	C	eth0
158.227.139.188	ether	00:07:E9:5C:71:B8	C	eth0
158.227.139.189	ether	00:07:E9:5C:72:E7	C	eth0

### 1.1 irudia: ARP taula.

<sup>2</sup> `ip neigh show` komandoa erabiliz ere lor dezakegu taula hau.

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.

Hasiera batean ARP protokoloa Ethernet sareetarako definitu zen. Izan ere, argitaratu zenean (RFC 826 agirian) emandako izena *Ethernet Address Resolution Protocol* izan zen. Gaur egun askogatik gehien erabiltzen diren sare-konexioak Ethernet direnez, bere erabilera nagusia IP helbideetatik Ethernet helbideak lortzea izaten jarraitzen du. Baina definitu dira ARP aldaerak beste motako sareetan ere erabiltzeko. Bere jatorrizko definizioan ARP mezuak Ethernet tramen informazio eremuan bidaltzen dira. Beste teknologiko sareetan erabiltzeko, teknologia horien trametan ARP mezuak nola sartu definitu behar izan da.

## ICMP protokoloa

IP protokoloak ematen duen zerbitzua datagrama erakoa denez, sareartearen kudeaketa zaila da, trafikoaren kontrol zehatza egiterik ez baitago. Hala eta guztiz ere, sareartean gertatzen denaren monitorizazioaren bat 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). IP-ren protokolo laguntzaile bat da<sup>3</sup>, 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. Hala ere, normalean, IPren batera inplementatu ohi da ICMP.

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. Bideratzaile batzuek ez diete hartutako ICMP mezuei jaramonik egiten, eta haiek ere ez dute ICMP mezurik bidaltzen, baina portaera hau ez da ohikoena.

Bere erabileraren adibide bat hain ezaguna den *ping* programa da, ICMPn oinarrituta baitago. Konputagailu bat sareartean zehar atzigarria dagoen ala ez jakiteko egiten dugun lehenengo gauza berari *ping* egitea da. *Ping*-ek adierazitako konputagailuari ICMP oihartzun-eskaera bat (*echo request* izeneko ICMP mezua) bidaltzen dio eta horren erantzunaren zain (*echo reply* ICMP mezua dena) gelditzen da. ICMPn oinarritzen den beste programa ezaguna *traceroute* da, konputagailu batetik bestera joateko datagramak jarraitzen duten bidea ezagutzeko erabiltzen dena. Honek ‘TTL agortuta’ izeneko ICMP mezua erabiltzen du (*TTL expired*, ingelesez; ICMP mezuen izen ‘ofizialak’ ingelesezkoak dira).

---

3 Berez, ICMP protokoloa IP-ren zatia dela ezartzen da RFC1812 eta RFC1122 agirietan.



## 1. laborategirako galdetegia

1. Idatzi zure Linux makinako sare-interfaze guztien konfigurazioa ikusteko komandoa.
2. Demagun 192.168.23.100 helbidea duen makina bati BI *ping* egin nahi dizkiozula, Linux makina batetik. Idatz ezazu horretarako behar den komandoa.
3. *Wiresharken* bi motako filtroak erabiltzen dira, baina guk, laborategian, horietako bat bakarrik erabiliko dugu. Idatz ezazu filtro mota horren izena.
4. Idatzi behar den komandoa, M1 makinaren eth0 interfazeari 1. laborategiko 2. irudiaren arabera dagokion helbidea esleitzeko. Oharra: erabili **ifconfig** komandoa.
5. Demagun zure arp taulan 192.168.1.1 helbideari dagokion sarrera dagoela. Idatzi komando bat sarrera hori ezabatzeko.
6. *Wiresharkek* arp eta icmp trafikoa harrapatzeko behar den *capture* filtroa idatzi.
7. Idatzi IOS komandoa lan modu pribilegiatutik konfigurazio orokorreko modura pasatzeko.
8. Idatzi IOS komandoa konfigurazio orokorreko modutik, FastEthernet0/0 izeneko interfaze baten konfigurazio modura pasatzeko.
9. Demagun CISCO bideratzaile batean lanean ari zarela kontsola bidez, eta FastEthernet0/0 izeneko interfaze baten konfigurazio moduan zaudela. Idatz ezazu interfaze horri 192.168.64.11/24 helbidea esleitzeko behar den komandoa.
10. Demagun EC makinako interfaze bat ez dagoela gaituta. Idatz ezazu behar den IOS komandoa interfaze hori gaitzeko.

# 1. laborategia: Sarrera

Helburuak:

1. Praktika honen eta ondorengo lan inguruarekin trebatzea: Linux sistema eragilea, sare-konfigurazioa Linuxen, *ping* komandoaren erabilera, CISCOren IOS sistemarekin lehen urratsak ematea, eta *Wireshark* analisi-protokoloaren oinarritzko erabilera.
2. Oinarritzko kontzeptuak berrikustea: helbide fisikoa (MAC), IP helbidea, maskara, ARP taula, ICMP protokoloa.

Denbora: 2 ordu eta 25 minutu

Lan-metodologia:

1. Dokumentazioa irakurri, eta bete galdetegia *moodlen*, epe barruan.
2. Ariketak egin, gidoian agertu ahala, eta behar dituzun apunteak hartu.
3. Erabili dituzun makina GUZTIAK itzali eta utzi lanpostua aurkitu duzun bezala.

**OHARRA: EZ PIZTU MAKINAK PIZTEKO AGINDUA IRAKURRI ARTE.**

## Laborategiaren deskripzio fisikoa

Lanpostu bakoitzean, honako ekipamendu hau aurkituko duzu:

### 1. Erabiltzailearen makinak (2)

Eramangarriak dira. Kontu handiz ibili behar duzu horren konfigurazio fisiko eta logikoa zegoen bezala uzteko.

Konputagailu horien sistema eragilea Linux Mint da, Xfce interfazearekin. Honako erabiltzailea eta pasahitza hauek erabiliko ditugu:

erabiltzailea: **ehu**

pasahitza: **rlinux**

Egingo ditugun laborategietan, eskuineko konputagailuari M1 deituko diogu, eta M2, ezkerrekoari.

### 2. Linux bideratzailea

Mahaiaren erdian dugun PCa da. Horrek *Lubuntu* dauka, eta gure ariketetan bideratzaile gisa erabiliko dugu (horretarako, bi sare-txartel ditu).

erabiltzailea: **root**

pasahitza: **rlinux**

Ondorengo laborategietan egingo ditugun ariketa eta sare-eskemetan, makina horrek **EL** izena izango du.

### 3. CISCO bideratzailea

Linux bideratzaileaz gain, CISCO 2811 bideratzaile bat dago<sup>4</sup>. EL makinatik kontrolatuko dugu, *kermit* urruneko programa erabiliz. Erabiltzailea: **root**. Pasahitza: **enable**.

Hemendik aurrera, izena **EC** izango da bideratzaile horren.

### 4. Kommutagailuak

Mahai bakoitzean, bi CISCO kommutagailu dituzu.

### 5. Kableak

Lanpostu bakoitzean, RJ-45 konektorea duten 4 pare kordatu zuzen (horiak eta grisak) dituzu, pare kordatu gurutzatu bakarra (urdina edo gorria), eta serie kablea DB-9 konektoreekin (urdina). Azkeneko hori EC bideratzailea eta beraren kontsola (EL) lotzeko beharko dugu.

Eramangarriak dira. Kontu handiz ibili behar duzu horren konfigurazio fisiko eta logikoa zegoen bezala uzteko.

Konputagailu horien sistema eragilea Linux Mint da, Xfce interfazearekin. Honako erabiltzailea eta pasahitza hauek erabiliko ditugu:

erabiltzailea: **ehu**

pasahitza: **rlinux**

Egingo ditugun laborategietan, eskuineko konputagailuari M1 deituko diogu, eta M2, ezkerrekoari.

## LINUX lan-inguruko zenbait tresna eta komando arrunt

Sare-konfigurazioa ezartzeko, testu-moduko komandoak erabil daitezke (terminala erabiliz idazten ditugunak, eta, parametroak ezagutzeko, `man` komandoa erabil dezakegu), edota Linuxeko mahaigainak eskaintzen duen ingurune grafikoa. Ingurune grafikoa desberdina izan daitekeenez sistema batetik bestera, guk komando bidezko interfazea erabiliko dugu (estandarra delako eta, askotan, ahaltuagoa).

### *Ifconfig* programa

Sare-txartelak konfiguratzeko erabiltzen da: IP helbidea ezarri, maskara zehaztu, edota interfazea aktibatu eta desaktibatu. Aukera anitz ditu.

Informazio gehiago eskuratu behar baduzu: egin ***man ifconfig***.

---

4 Bi mailetan dagoena CISCO 1700 eredua da. Gure laborategietarako, baliokideak dira.

**1. ariketa: ifconfigen erabilera arrunta**

*Gogoratu: laborategian egindako ariketak errepasatu ahal izateko, gomendagarria da pantailan agertzen den informazioa gordetzea. Horretarako:*

*a) Ireki LibreOffice fitxategi bat.*

*b) Pantailan, galderei erantzuteko interesgarria den emaitza bat lortzen duzun bakoitzean, kopiatu LibreOfficen.*

*c) Makina itzali aurretik LibreOffice fitxategiaren kopia bat eraman zurekin.*

Hasierako ariketa hau taldekide bakoitzak egin behar du bere kabuz, M1 makinan batek eta M2 makinan besteak.

Egiaztatu M1 eta M2 makinetako sare-kable arruntak paretako sare-gune bati lotuta daudela. ORAIN, PIZTU M1 eta M2, eta sartu, lehen esandako erabiltzaile eta pasahitza erabiliz.

1. Zure makinako interfazeen zerrenda eta haien konfigurazioa ikusteko, egin **ifconfig** (baliokidea: **ip add sh**). Zenbat interfaze agertu dira? Zein dira haien izenak?
2. Gure laborategietan, *eth0*<sup>5</sup> izena duena besterik ez zaigu interesatuko. EHUko sarera lotzen zaituen interfazearen konfigurazioa aztertu (**ifconfig eth0** edo, bestela, **ip add sh eth0**), eta honako galdera hauei erantzun

Zein da *eth0* interfazeak esleituta duen IPv4 helbidea? Apuntatu helbide hori paper batean, hurrengo ariketan beharko duzu eta. Zein da helbide horri dagokion IP maskara eta sare-difusiorako IP helbidea? Zein da helbide fisikoa? Zenbat byte onartzen dituzte gehienez *eth0* interfazea erabiliz bidaltzen diren tramek, beren datu-eremuan? Zenbat trama jaso/igorri dira? Zenbat jasotze/igortze-errore izan dira? Zenbat talka? Zein da jasotako/igortitako tramen batez besteko tamaina?

### *ip* programa

Sare-konfiguraziorako erabiltzen diren tresna batzuen ordezkoa da *ip* programa. Hasiera batean, *ifconfig*, *route* eta beste batzuen erabilera baztertzeko agertu da, baina errealitatea bestelakoa da oraindik. Guk betiko tresna horiek erabiliko ditugu, baina *ip* programaren erabilera baliokidea ere aipatuko dugu askotan.

Informazio gehiago eskuratu behar baduzu: egin **man ip**.

### *Ping*

Sare-administrazioan gehien erabiltzen den tresnetakoa da. Makina bat sare-bidez atzigarri dagoen ala ez jakiteko erabiltzen da. *Ping* oso programa sinplea da, eta ICMP protokoloan oinarrituta funtzionatzen du: bidali ICMP `echo request` mezu bat atzigarri dagoen jakin nahi dugun makinara, eta itxaron hark erantzun arte ICMP `echo reply` mezuarekin.

Informazio gehiago eskuratu behar duzunean: egin **man ping**.

---

<sup>5</sup> Konputagailuaren txartel kopuruaren eta konfigurazioaren arabera *eth*-ren ondoren dagoen zenbakia desberdina izan daiteke.

## 2. ariketa: pingen erabilera arrunta

*Ping* bat bidali M1etik M2ra, bidalketa kopurua 5era mugatuz (-c aukera erabili). Nola identifikatu behar duzu M2 idatzitako *ping* aginduan?

1. Zenbat oihartzun-eskaera (*echo*) geratu dira erantzunik gabe? Bidalketa guztien zein ehuneko da hori? Zenbatekoa da igarotako denborarik laburrena eskaera igorri eta erantzuna jaso arte? Eta luzeena? Bataz bestekoa? Bataz besteko aldea?
2. Zein da erantzunen TTL balioa? Egin orain *ping* bera 10.30.13.6 helbideari, eta alderatu erantzunen TTL balioak. Zenbat bideratzaile zeharkatu ditu ICMP *echo reply* mezu bakoitzak zure ustez? Argibidea: M1 eta M2 sare fisiko berean daude. Beste makina, aldiz, ez.

### Arp

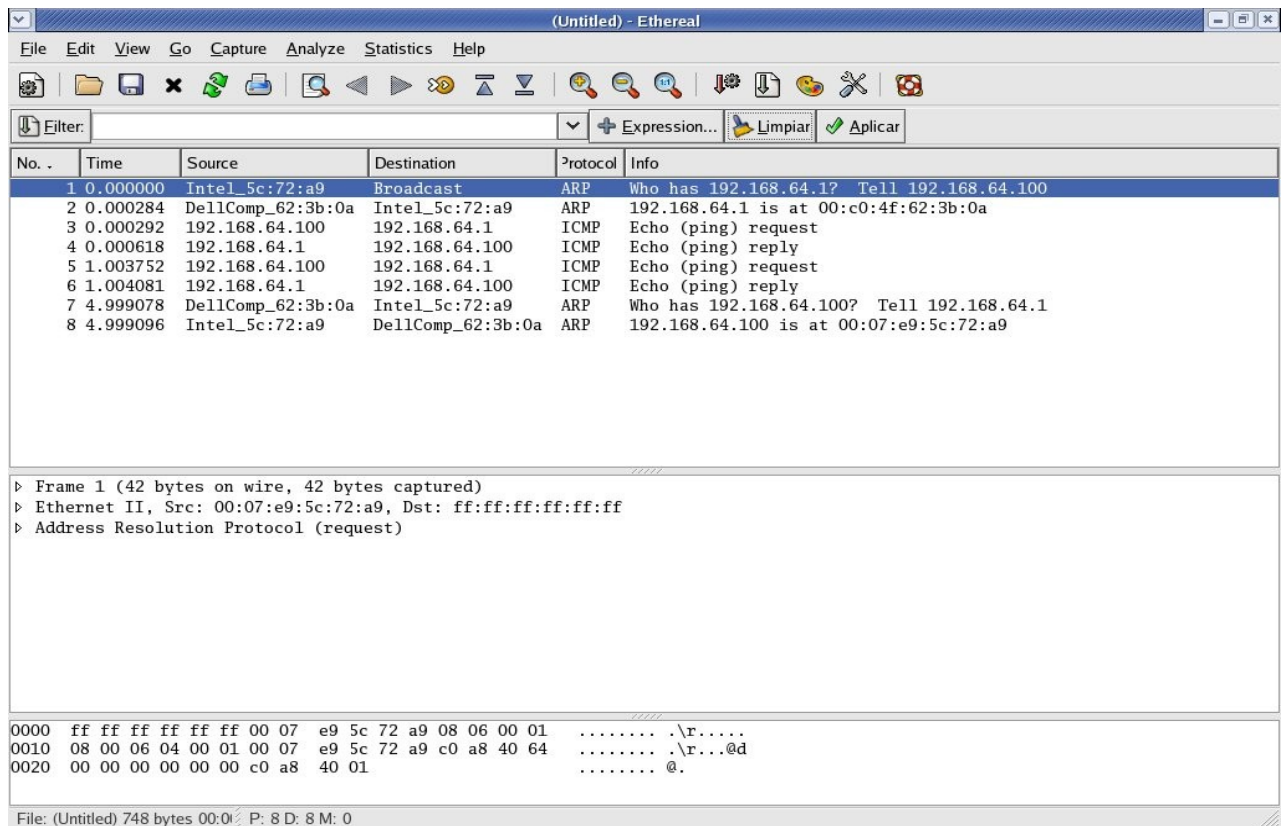
Komando hori ARP taula atzitu eta kudeatzeko erabiltzen da. Gogoan izan taula hori *cache* bat dela, non helbide fisiko eta IP helbideak gordetzen diren Ethernet sareetan. Haren izena taula osatzeko eta mantentzeko erabiltzen den protokolutik hartzen du. *Cache* bat denez, taula behin-behinekoa da: sarrerak iraungitzen dira erabiltzen ez badira. Normalean, iraungitze-epea 2 minutukoa da.

Informazio gehiago eskuratu behar duzunean: egin *man arp*.

### Wireshark

Protokolo-analizatzaile edo *sniffer* bat da. Sare-interfazeek (txartelek) jasotzen eta bidaltzen duten trafikoa gorde eta pantailaratzen du, erabiltzaileak erazagututako trafikoa atzemateko iragazkien (*Capture filter*) arabera. Nahitaezkoa da sare-interfazea modu ‘promiskuoan’ egotea, hau da, saretik datozen trama guztiak jaso behar ditu, eta, horretarako, *root* moduan egikaritu behar da, ***sudo*** erabiliz (oro har, sare-txartel batek sistema eragileari makinarako diren tramak soilik pasatzen dizkio). Analizatzailea erabiltzaile mailan exekutatzen den softwarea da, *kernel*aren zatia den trama-iragazkiarekin komunikatuz. Iragazki horrek sare-txartelaren *driver* edo kontrolatzailearekin komunikatzen da, txartelaren bidez jaso edo igortzen den trama bakoitzaren kopia lortzeko. Analizatzaileak iragazkian finkatutako baldintzak betetzen dituzten tramak soilik jasoko ditu (helbide jakin batetik datozenak, protokolo zehatz baten tramak, eta abar).

*Wireshark*ek trafikoa harrapatzeko iragazkiak definitzeko sintaxiari buruzko informazioa hemen duzu: <http://wiki.wireshark.org/CaptureFilters> edo bestela [http://www.openmaniak.com/wireshark\\_filters.php](http://www.openmaniak.com/wireshark_filters.php).



### 1 irudia: *Wireshark* trama-jasotzea.

*Wireshark*ek ingurune grafikoa eskaintzen du, eta, hala, bere erabilera errazagoa egiten du beste analizatzaile batzuen aldean (adibidez tcpdump). Harrapaketa bat abiatzen denean, zabalduko leihoan, iragazkiak harrapatutako ikus dezakegu, denbora errealean trafikoa. Trafiko hori lasai aztertzeke, ordea, harrapaketa gelditu eta atzemandako trafikoa araka dezakegu pantailan bertan. Harrapatutakoa fitxategi batean gordetzea ere badago, eta, gero, bigarren motako iragazkiekin aztertzea (*Display filter*). Guk, ordea, soilik trafikoa atzemateko iragazkiak erabiliko ditugu.

*Wireshark* exekutatzeko, terminal bat ireki, eta ***sudo -b wireshark*** idatzi; 1. irudiaren antzeko leihoa azalduko zaizu.

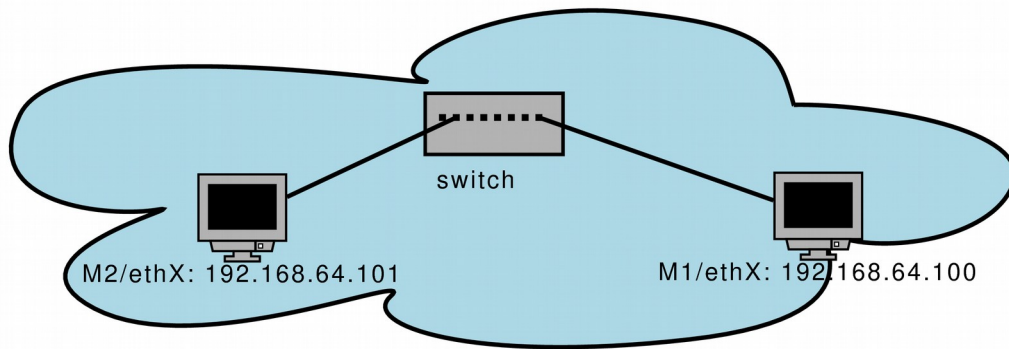
Irudian, iragazkirik gabeko trama-eskuratze bat egin da. Jasotako trafikoa ARP eta ICMP da. Leihoak hiru zati ditu. Lehenengoan, jasotako tramen laburpena dugu (trama bat lerroko). Bigarrean, lehenengo leihoan aukeratutako tramaren xehetasunak ikus ditzakegu. Azkenik, hirugarrenean, tramaren edukia ikus daiteke hamaseitarrean eta ASCII formatuan.

*Aholkua: denbora sobera baduzu (bestela, etxean egin), man **wireshark** exekutatu eta aztertu jasotako informazioa. Wiresharki buruzko dokumentazioa [www.wireshark.org](http://www.wireshark.org) webgunean ere aurkituko duzu.*

### Sare simple baten ezarpena

Esperimentuekin hasteko, sare simple bat ezarriko dugu, izar bakar batek osatua. 2. irudian duzu sare-eskema.





## 2. irudia: sare-eskema minimoa.

Sarea osatzeko honako urrats hauei jarraitu M1n eta M2n:

1. Gelditu *network-manager* zerbitzua: **`sudo service network-manager stop`**.
2. Deskonektatu sare-kablea makinatik, eta utzi askatutako muturra mahaian dauden gakoetako batean
3. Makinaren sare-interfazea birkonfiguratu *ifconfig* erabiliz, irudiko helbidea esleituz makina bakoitzari:  
*ifconfig interfazearen\_izena helbidea/aurrezenbakiaren\_luzera up*
4. Egiaztatu interfazeen konfigurazioa ondo egin dela, horretarako **`ifconfig`** komandoa berriz erabiliz.
5. Aukeratu mahai gainean duzuen konmutagailuetako bat, eta PIZTU ORAIN. Hartu sare-kable normaletako bat (ez hartu gurutzatua!) eta konektatu zure makina piztu duzun konmutadoreko aho batera. Ziurtatu aho horri dagokion leda piztu egin dela konektatutakoan, eta kolore gorritik berdera igaro dela.
6. Egiaztatu ea sarea badabilela. Horretarako, *ping* egin M1etik M2ra edo alderantziz. Zein IP helbide erabili behar dituzu orain M1 eta M2 identifikatzeko?

## 3. ariketa: arpekin eta Wiresharkekin trebatzea

1. Ireki terminal-leiho bat M1 makinan. Kontsulta ezazu arp taula, terminal horretan **`'arp -n'`** komandoa exekutatu. Ba al dago sarrerarik taulan? Sarreraren bat balego, arp komandoaren `-d` aukera erabili taula husteko. Oharra: `-d` aukeraren erabilera kontsultatu eskuliburuan (man arp).
2. Exekutatu orain wireshark lehenengo terminalean, ARP edo ICMP edukia duten tramak atzemateko konfiguratu (*capture/options* lehoian<sup>6</sup> **`arp or icmp`**<sup>7</sup> filtroa ezarri), eta abiatu ('start' botoia sakatu). Bigarren leihoan, berriz, *ping* bat exekutatu ondoko makinara, trama bakarra bidaliz (`-c` aukera). *Wireshark* trafikorik jasotzen ez duenean (segundo batzuk), gelditu eskuratzea. Ordoren, arp taula berriz kontsultatu. Zer sarrera daude orain?
3. *Wireshark*ek eskaintzen duen informazioa aztertu, honako galdera hauei erantzuteko:
  - Aukeratu eta aztertu ARP edukia daraman trametako bat: zein protokolo erabiltzen da TCP/IP arkitekturaren maila bakoitzean? Zein mailataraino ailegatu zara? Hartu orain ICMP trama bat eta galdera berdeei erantzun.

<sup>6</sup> Lubuntu bada zure sistema, *Wireshark*en bertsioak lehoi nagusian bertan du filtroak definitzeko laukia, eta ez 'Capture/options' aukera hartuta irekitzen den lehoian.

<sup>7</sup> Adi, minuskulak erabili.

- Erantzun al dio ondoko makinak *ping* komandoari? Nola daki makina horrek zein IP helbideri itzuli behar zion ICMP *echo reply* paketea? Nola lortu du ondoko makinak gure makinaren helbide fisikoa? Zertarako behar zuen gure helbide fisikoa?

## CISCO 2811 bideratzailerako sarrera.

CISCO 2811 bideratzaile gisa funtzionatzen duen konputagailu berezia da eta sistema eragile propioa du, *Internetwork Operation System* (IOS). Bideratzailearen kudeaketa kontsola edo sarearen bidez egin daiteke, *telnet* izeneko programa edo arakatzailer bat erabiliz. Lehenengo aldiz konektatzean, kontsola bidez besterik ezin dugu egin, interfazeek inolako konfiguraziorik ez dutelako eta ondorioz ezinezkoa da sarearen bidez konektatzea. Gainera, arazoak agertzen direnean, bideratzailea kontrolatzeko erarik aproposena da kontsolarena, sare-erabilerarengatik sor daitezkeen arazoak edo interferentziak ekiditen direlako. Guk EL makinan abiatutako kontsola baten bidez kontrolatuko dugu CISCO bideratzailea.

Kontsola bidez konektatzeko, bi gauza behar ditugu:

1. Konputagailu bat, serie-portua libre duena, eta eta terminal emuladore bat instalatuta duena. Gure konputagailua EL izango da, eta *kermit* programa erabiliko dugu emuladore gisa.
2. Kable bat, konputagailua eta bideratzailea fisikoki konektatzeko. Hori izango da hasieran aipatutako kable urdina, DB-9 konektorea (serie-portua) eta RJ-45 konektorea (bideratzailearen kontsola-portua) dituen.

Kontsola bidezko konexioa ezartzeko, honako hau egin beharra dago:

1. Kablea ondo konektatu: bideratzailean '*console*' konexiora (urdina), eta konputagailuan serie-portuan.
2. Ireki terminala konputagailuan, eta *kermit* programa exekutatu (*kermit* idatziz). *Prompta* azalduko zaizu:

```
/root/) C-Kermit>
```

3. Aukeratu erabiliko duzun serie-portua:

```
(/root/) C-Kermit> set line /dev/ttyS0
```

4. Telefono-linea erabiliko ez dugunez, eramailearen detekzioa desgaitu:

```
(/root/) C-Kermit> set carrier-watch off
```

1. Bideratzailearekin konexioa ireki:

```
(/root/) C-Kermit> connect
```

2. *Return* sakatu eta zure erabiltzailea (*root*) eta pasahitza (*enable*) eskatuko dizkizu. Ondoren *prompta* agertuko zaizu:

```
CISCO#
```

## CISCOren IOSa

IOSaren testu-komandoen interfazearen sintaxia nahiko erraza da, baina horren erabilera zaila egiten da ehunka komando daudelako (eta komando bakoitzeko aukera anitz). Linuxen aldean, IOSak lan modu pila bat ditu (Linuxen bi, *sudo* eta arrunta), eta, modu bakoitzean, komando-multzo bat dugu. Modu batetik bestera pasatzeko, komando bereziak erabiltzen dira, eta, laguntza gisa, *promptak* esaten digu momentu bakoitzean zein modutan gauden. Honako hauek dira ohiko lan moduak eta bakoitzari dagokion *prompta*:

- Erabiltzaile modua: CISCO>

Ez dugu erabiliko, ezta, normalean, ikusiko ere.

- Modu pribilegiatua: `CISCO#`

Normalean, modu horretan sartuko gara zuzenean bideratzailea piztean.

- Konfigurazio orokorra modua: `CISCO(config)#`

Modu horretan egiten dira makina osoari dagozkion konfigurazioak.

- Konfigurazio espezifikotarako moduak. Asko dira (17 baino gehiago), eta IOSren bertsioaren arabekoak. Gure laborategietan erabiliko dugun ia bakarra interfaze konfigurazio modua da. Honako hau da haren *prompta*: `CISCO(config-if)#`

Horrela, interfaze bati bakarrik dagozkion konfigurazioak egiten dira.

Ezin da edozein lan modutatik beste edozeinetara zuzenean pasatu. Zenbait ariketa egin ahala ikusiko ditugu lan moduen arteko ibilbideak eta oinarritzko komandoak.

*Aholkua: IOSen erabilera hobeto ezagutzeko (CLI-Command Line Interface), ikusi haren dokumentazioa [www.cisco.com/en/US/docs/ios/preface/usingios.html](http://www.cisco.com/en/US/docs/ios/preface/usingios.html) url-an. Zure etxeko konputagailuan instala dezakezu emuladore bat, doakoa, praktikatzeko: <http://www.gns3.com/>*

#### 4. ariketa: IOSa eta interfazeen konfigurazioa CISCOn

1. ORAIN PIZTU bi bideratzaileak, eta ireki kotsola bat ELn, EC kontrolatzeko (ikusirik aurreko orria).

2. Ikusi zein den duzun *prompta* CISCO makinan. Zein lan modutan zaude? Ez bazaude modu pribilegiatua, teklatu:

```
CISCO> root
```

Eta eman pasahitza.

3. Probatu nola erabiltzen den on-line laguntza IOSen: **help** teklatu eta erantzuna aztertu.

4. Ikusi bideratzailean interfaze-konfigurazioa, **sh ip interface brief** exekutatu. Zenbat interfaze ditu bideratzaileak? Zein izen erabiltzen dira? Zein daude aktibatuta (up) eta zein ez? Orain, egin **sh interfaces** eta erantzun honako galdera hauei, aktibatuta dauden interfazei buruzkoak: zein IP helbideak dauzkate esleituta? Zein formatutan ematen dira IP helbideen maskarak? Ikusi ematen diren helbide fisikoen formatua, zer desberdintasun dago Linuxen arp komandoak erabiltzen duen formatuaren aldean?

5. Erabiltzen ari zaren kotsolaren konfigurazioa ikusteko, **sh line 0** egin. Bilatu 'timeouts idle EXEC' parametroaren balioa. Ziur asko, 5 minutukoa izango da. Horrela uzten baduzu, gogaitu egingo zaitu laborategietan, CISCO kotsolan 5 minutuz jarraian lan egiten ez baduzu saioa etengo baitu eta berriz abiatu beharko baituzu. Segituan ikusiko dugu nola desgaitu jardura ezarako denboragailu hori.

6. Konfigurazio orokorra modura pasa, **configure terminal** exekutatu. Ikusi *prompta* aldatu dela. Lan modu horretan gaudela CISCOren beste portaera gogaikarri bat desgaituko dugu: komando bat gaizki teklatzen dugun bakoitzean sistema ez blokeatzeko tarte batean, honako hau egikaritu:

```
CISCO (config)# no ip domain-lookup
```

Hurrengo laborategietan, gogoratu gauza bera egitea IOS saio bat abiatzen duzun bakoitzean.

7. Jardura ezarako denboragailua desgaitzeko, kotsolaren konfiguraziorako lan modu espezifikora aldatu behar da. Horretarako, egin **line console 0**, eta *prompta* aldatuko zaizu. Orain, egin:

CISCO (config-line)# **no exec-timeout**

8. Atera kontsola konfiguratze modutik. Bi eratara egin dezakezu:

- a) **exit** tekleatuz, konfigurazio orokorra modura bueltatuko zara.
- b) **end** tekleatuz, modu pribilegiatura itzuliko zara.

Lehena hartuko dugu:

CISCO (config-line)# **exit**

CISCO (config)#

9. Orain, interfazeen konfigurazioa aztertuko dugu. Ondo ikasi hau, laborategi guztietan hainbat aldiz egin beharko baituzu. Edozein interfazeren konfigurazioa aldatzeko, interfaze horren konfigurazioaren lan modu espezifikora igaro behar dugu, **interface interfazearen\_izena** tekleatuz (*prompta* aldatuko da). Aldatu FastEthernet0/0 interfazea konfiguratze modura.

10. 192.168.64.11/24 helbidea esleitu FastEthernet0/0 interfazeari. Horretarako, honako komando hauek exekutatu behar dira:

- IP helbidea esleitzeko:

**ip address ip\_helbidea maskara\_formatua\_dezimalean**

- Interfazea gaitzeko:

**no shutdown**

- Atera interfazea konfiguratze modutik eta grabatu egindakoa:

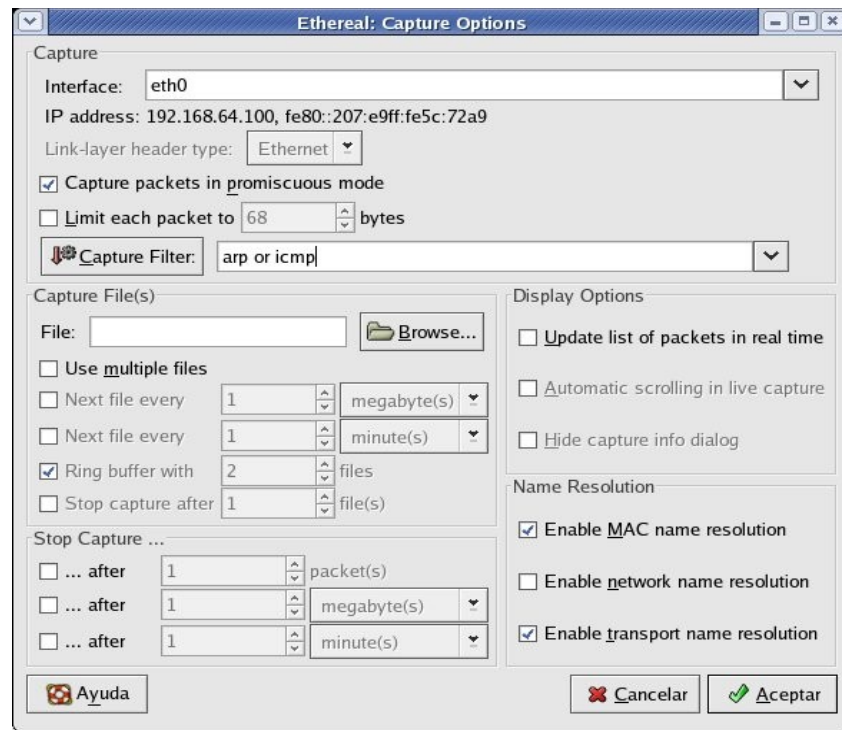
**end**

11. Orain *ping* bat egiten bada erabiltzaile makina baten eta 192.168.64.11 helbidearen artean, ez du funtzionatuko, oraindik ez dugulako interfaze hori fisikoki sarera konektatu. Egoera berean egongo ginateke sare-kablea gaizki balego, muturren bat deskonektatuta egonez gero, edota konektoreen bat puskatuta. Alegia, konexio fisikoa ibiliko ez balitz. Egikaritu **sh ip interface brief** komandoa, konekta ezazu FastEthernet0/0 konmutagailura kable normal bat erabiliz, exekutatu berriz **sh ip interface brief**, eta ikus ezazu zer aldatu den.

12. Ikusi ea M1 eta M2 makinak atzigarri dauden bideratzailetik. Horretarako, *ping* erabili bideratzailean, makina horien kontra. Zenbat oihartzun bidali eta jaso dira *ping* bakoitzean? Kontrola al dezakezu, Linuxen egiten den moduan, zenbat oihartzun bidaltzen diren?

### 5. ariketa: IP helbide bikoiztuak

1. **EL**ren interfazeak desgaitu. Horretarako, **ifconfig eth0 0.0.0.0** eta **ifconfig eth1 0.0.0.0** egin.
2. EL gehitu eraiki dugun sareari, EL/eth0 interfazea konmutagailura konektatuz. Konfiguratu eta aktibatu interfaze hori 192.168.64.11/24 (ikus 2. ariketa) helbidea erabiliz. EL/eth0 eta EC/FastEthernet0/0k IP helbide bera dutela ohartu.
3. Egiaztatu M1en ARP taula hutsik dagoela. Bestela, `arp -d` erabili husteko.
4. *Wireshark* exekutatu, M1 eta ELn, iragazki bat definituz, ARP eta ICMP trafikoa eskuratzeko. Horretarako, nahikoa da `arp or icmp` idaztea *Capture Options* leihoan, irudian azaltzen den bezala.



### 3. irudia: Iragazki simple bat definitu *Wiresharken*.

5. Egin ping 192.168.64.11 -c 1 M1etik. Harrapaketa gelditu eta aztertu jasotako trafikoa. Zenbat makinak erantzun diote M1ek egindako ARP eskaerari? Begiratu haien helbide fisikoak. Zeinek erantzun du lehen? Zein helbide fisiko dagokio 192.168.64.11 helbideari M1en taulan?
6. Hustu ezazu M1en ARP taula. Berrabiatu *wireshark* harrapaketa M1n eta ELn. Exekutatu orain, ECTik, ping 192.168.64.100. Erantzun al die M1ek ECK bidalitako oihartzun eskaerei? *Wireshark* gelditu eta aztertu jasotako tramak. Lehen emandako erantzun bera emango zenuke? *Wiresharken* ikusi bezala, M1ek erantzun du. Baina nork jaso ditu horren ICMP reply mezuak? Azal ezazu honen zergatia.

*Laborategitik joan aurretik, **GOGORATU**:*

- *Gorde erabilitako sare kable guztiak beren poltsan.*
- *Itzali makina guztiak: M1, M2, Linux bideratzailea, Cisco bideratzailea, eta konmutadoreak.*
- *Hurrengo laborategietara enuntziatu hau eta hartutako apunteak ekarri behar dituzu.*

## 2. laborategirako teoria: Datagramak birbidaltzea

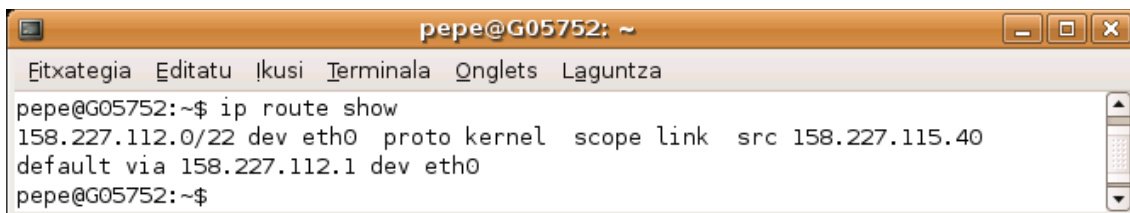
### Birbidaltze-taulak (*forwarding table*)

IP entitatearen lana datagramak bideratzea da. Horretarako **birbidaltze-taula**<sup>8</sup> erabiliko du. birbidaltze-taulako lerro bakoitza bide bat da (*route*). Honako informazio hau izango dugu, gutxienez, bide bakoitzerako:

- Sare-aurrezenbakia. Hau da taulan bilatzeko gako nagusia. Helbide sorta bat da (helbide bakarra izatea ere posible da, 32 maskara erabiliz), bide honetatik atzigarriak ditugun helbideak biltzen dituen. Datagrama bat bideratzean, IP entitateak bilatuko du bere taulan zein helbide sortari dagokion datagramak daraman helburu-helbidea, eta taulako lerro horretan aurkituko duen informazioa erabiliko du datagrama bideratzeko.
- Hurrengo urratsa. Datagramak bere bidean bisitatu behar duen sarearteko hurrengo bideratzailearen IP helbidea da. Gure konputagailua eta helburukoa sare berean badaude, ez dago hurrengo urratsarik bide honetan.
- Interfazea. Makinak duen interfazeen artean, nondik transmititu behar den datagrama. Taulako zutabe honek IP entitateari adieraziko dio ea zein sarbide entitateri eman behar dion datagrama.

IP inplementazioaren arabera, informazio gehiago egon daiteke (eta egoten da) birbidaltze-tauletan, baina hauek dira daturik garrantzitsuenak. Helburu batera iristeko bide bat baino gehiago daudenean, erabilgarria da bide bakoitzari balio bat esleitzen dion beste parametro bat izatea taulan. Hori da metrikarena:

- Metrika. Helburura iristeko kostua. Bideratzaileek metrika eremu hau erabiltzen dute taulan agertzen diren aukeren artean bat hartzeko. Normalean, bidean zeharkatu beharko den bideratzaile-kopurua (ingelesez, *hop*) adierazten du metrikak, baina beste irizpideak erabiltzea ere badago.



```

pepe@G05752: ~
Fitxategia Editatu Ikusi Terminala Ongletas Laguntza
pepe@G05752:~$ ip route show
158.227.112.0/22 dev eth0 proto kernel scope link src 158.227.115.40
default via 158.227.112.1 dev eth0
pepe@G05752:~$

```

### 2.1 irudia: birbidaltze-taula xume bat, erabiltzaile baten konputagailu batena (eta ez bideratzaile batena).

2.1 irudian Linux sistema baten birbidaltze-taula ikus daiteke, *ip route* komandoaren bidez lortuta<sup>9</sup>. Irudiko taula interfaze bakarra duen makinaren bi bideko taula tipikoa da. Taulako

<sup>8</sup> Taula hau izendatzeko adostasunik ez dago Interneten. Testu askotan (ikusi RFC 1812),

**birbidaltze-taula** deitzen zaio, (*forwarding table* edo FIB-*Forwarding Information Base*). Beste askotan, aldiz, bideratze-taula terminoa erabiltzen da (*routing table*, ikusi RFC 4271).

<sup>9</sup> Badago beste komando batzuekin informazio bera lortzea, adibidez, *route* edo *netstat* komandoekin, baina beste aukera horiek baztertzen ari dira berriagoa den *ip* komandoaren mesederako.



lehenengo lerroan agertzen da lehenengo bidea, 158.227.112.0/22 helbideetara doana, taula duen konputagailuko sare berean dauden helburuetara joateko bidea, alegia. Bertako saretik atera behar ez denez, ez da agertzen hurrengo urratsik, eta zuzenean `eth0` interfazetik birbidaliko dira datagramak. Bigarren lerroa besterik ezeko bidea da (*default* ingelesez), hau da, beste edozein tokitara joateko bidea. Hor bai agertzen dela hurrengo urratsa zein den (`via 158.227.112.1`), erabili behar den interfazeaz gain. Erabiltzaile baten konputagailua denez, interfaze bakarra du, `eth0` izenekoa, eta hortik igorri behar dira, halabeharrez, datagrama guztiak.

### ***Birbidaltze-taulen erabilera***

IP entitate batek datagrama bat bidali (edo bideratzaileen kasuan, birbidali) behar duenean, honako urrats hauek ematen ditu datagramari dagozkion bidea birbidaltze-taulan bilatzeko<sup>10</sup>:

1. *Basic match* araua: Taulako bide bakoitzean, egiaztatu ea bat datorren datagramaren helburuko helbidea bideko helburu-helbidearekin. Bat datozen bideek balizko bideen multzoa osatzen dute.
2. *Longest match* araua: Balizko bideen artean, aukeratu maskara luzeena dutenak. Horiek dira gure datagramari gehien dagozkion bideak.
3. *Best metric* araua: Aurreko urratsean aukeratutako bideen artean, metrika hoberena dutenak hautatu.
4. *Vendor policy* araua: Oraindik bide bat baino gehiago baldin badago balizko bideen multzoan, kudeatzaileak definitutako berezko irizpideak erabili (horrelako irizpideak badaude) beraien artean aukeratzeko.
5. 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:

<i>Destination</i>	<i>Next hop</i>	<i>Metric</i>	<i>Interface</i>
155.233.0.0/16	191.166.12.1	3	Geth0
155.233.16.0/20	191.166.12.2	4	Geth0
155.233.18.0/23	180.96.138.2	4	sdh0
155.233.18.64/26	191.166.12.1	3	Geth0
155.233.18.64/26	191.166.14.3	1	FastEth0

**2.1 taula:** 155.233.18.78 helbidearekin bat datozen birbidaltze-taulako bideak.

Bigarren urratsa betez gero, 2.1 taulako azkeneko bi bide besterik ez dugu izango. Hirugarren urratsean horietako bat bakarrik aukeratuko dugu, datagrama `FastEth0` interfazetik bidaliko duena. Laugarren eta bostgarren urratsak ez ditugu bete behar izango.

### ***Helbiderik gabeko interfazeak***

Batzutan, konputagailu batetik bestera joateko ez da erabiltzen sare kommutatu bat, baizik eta konexio zuzen bat. Horrelako konexioak erabiltzen dira, askotan, bideratzaileen artean. Adibidez, bi sare lotzen dituzten bi bideratzaileak zuntz optiko baten bidez lotuko dira askotan. Kasu berean daude sare telefonikoaren bidez konektatutako konputagailuak (PPP loturak, alegia), zuntz baten lambdaz (edo kanala) egindako konexioak, edo zirkuitu birtual baten bidezko konexioak (adibidez,

<sup>10</sup> Algoritmo hau ez dago estandarizatuta era formalean. RFC 1812 agirian deskribatzen da, baina agiri berak algoritmo hau 'Interneten folklorearen zati bat' dela adierazten du.

ATM eta FR konexioak). Kasu horietan guztietan egoera berezi bat sortzen da birbidaltze-taula betetzean. Azter dezagun arazoa eta bere irtenbidea.

Hasiera batean, konputagailu baten interfaze bakoitzari esleitu behar zaio IP helbide bat. IP helbide hori interfazearen bidez atzitzen den sareari dagokion helbide sortatik erauzitako helbide bat izango da. Baina konexio zuzenen kasuan ez dago horrelako sarerik, linea bat besterik ez baitugu. Badago linea hori minisare bat bezela hartzea, muturreko bi konputagailuak besterik ez duena, eta sare aurrezenbaki bat esleitzea lineari. Baina hori IP helbideak xahutzea litzateke, eta, horregatik, helbiderik gabeko lineen kontzeptua sortu dute (*unnumbered lines*). Horrelako linea bati ez zaio inongo sare-aurrezenbakirik esleitzen, eta, ondorioz, linearekin lotuta dauden sare-interfazeek ere ez dute IP helbiderik.

Helbiderik gabeko interfaze hauek zenbait arazo bereziak sortzen dituzte. Horietako bat datagrama baten bidean zein den hurrengo urratsa adierazten duen birbidaltze-taulako parametroaren balioa da. Egoera normal batean, hau da, bere IP helbidea duen interfazearen kasuan, konexioaren beste muturrean dagoen konputagailuaren birbidaltze-taulan agertuko litzatekeen hurrengo urratseko IP helbidea, interfazearena litzateke. Konexio zuzenen kasuan, ordea, interfazeak ez du IP helbiderik eta konexioak ez du aurrezenbakirik esleituta. Horrela izanik, zein IP helbidea ipini behar dugu birbidaltze-taulako 'hurrengo urratsa' eremu horretan? Egia esan, arazoa hutsa da, ez baitago horren IP helbidearen inongo beharrik, interfaze horretatik bidaltzen den guztia toki berera joaten delako (konexioaren beste muturrean dagoen makinara, alegia). Baina birbidaltze-taulan zerbait jarri behar denez, zenbait trikimailu asmatu dira. Akaso gehien erabiltzen dena helbiderik gabeko interfazea duen konputagailuaren beste IP helbideren bat (konputagailu batek beti behar du IP helbide bat gutxienez) ipintzea da. Hainbat interfazeetarako erabiltzen den helbide horri *router-id* deitzen zaio testu batzuetan (RFC 1812 agirian, adibidez).

### ***Bide-elkarketa***

Taulen kudeaketa ez da arazo bakarra bideratze-taulen tamaina handiegia suertatzen denean. Gainera, bideratzailearen lana asko mantsotu daiteke: datagrama bakoitzaren helburuko helbidea taulako bide guztiekin alderatu behar dela gogoratu. Taulak oso handiak direnean, bideraketa luzatzen da, eta, horrekin batera, bere helburura ailegatzeko datagramak hartuko duen denbora. Gainera, datagrama bakoitza prozesatzeko denbora luzea denez, bideratzaileen ilaretan pilatuko dira datagramak bere txandaren zain, kongestioa sortuz. Kongestioa larria denean, okerre gertatzen da: heldu berriko datagramak baztertuak izango dira beraientzako tokirik ez badago bideratzailearen ilaretan. Horregatik guztiaengatik taulen tamaina ahal den txikiena mantendu behar da. Horretarako oinarrizkoa da maskaren erabilera ahalbidetzen duen bide-elkarketa.

Bideak elkartzeko asko gutxitu daiteke bideratze-taulen tamaina. Baina askotan bideratzaile baten bidez atzigarriak ditugun sare guztiak ezin dira elkartu bide bakar batean.

## 2. laborategirako galdetegia

1. Idatzi behar den Linux komandoa `vm0` izeneko interfazea desgaitzeko.
2. Zein dira gure laborategiko EL makinek integratuta daukaten sare-txartelen helbide fisikoetako lehenengo 6 byteak?
3. Idatzi laborategiko M1 makinaren interfazea konfiguratzeko behar den komandoa (ez erabili ip komandoa)
4. Laborategiko interfazeak konfiguratuta dauzkazula, idatzi behar den komandoa M2 makinari *ping* bat egiteko, beste edozein Linux makinatatik.
5. Linux sistema batean zaudela, idatzi komandoa birbidaltze-taula ikusteko.
6. Lubuntu makina batean birbidaltzeko gaitasuna aktibatuta dagoen ala ez ikusteko behar den komandoa idatzi (cat komandoa erabili).
7. Lubuntu makina baten birbidaltzeko gaitasuna aktibatzeko komandoa idatzi.
8. Birbidaltze-taula batean irtenbidea (lehenetsitako bidea) 192.168.1.1 ezartzeko behar den Linux komandoa idatzi.
9. Idatz ezazu behar den IOS komandoa birbidaltze-taularen edukia kontsultatzeko.
10. Idatzi behar den IOS komandoa, 192.168.32.0/24 sarera joateko 192.168.64.1 bideratzailea erabiltzeko.
11. IOS sistema baten birbidaltze-taulatik 192.168.32.0/24 sarera doan bidea ezabatzeko komandoa idatzi.
12. IOS sistema baten birbidaltze-taulan 192.168.1.1 irtenbidea grabatzeko behar den komandoa idatzi.
13. IOS sistema baten birbidaltzeko gaitasuna aktibatzeko behar den komandoa idatzi.

## 2. laborategia: Birbidaltzea konfiguratzeko

Helburuak:

1. IP datagramen birbidaltze-prozesua errepetatzea.
2. Bideratzaileak nola konfiguratu diren ikastea (bide estatikoak), Linux eta CISCO inguruneetan.

Denbora: 2 ordu 25 minutu

Lan-metodologia:

1. Dokumentazioa irakurri, eta bete galdetegi *moodlen*.
1. Laborategian, ariketak egin, gidoian agertu ahala, eta behar dituzun apunteak hartu.
2. Erabili dituzun makinak itzali eta utzi lanpostua aurkitu duzun bezala. Ahaztu gabe, fakultateko sare-kableak konektatu berri.

### Bibliografia:

- IOS komandoak: [www.cisco.com/en/US/docs/ios/preface/usingios.html](http://www.cisco.com/en/US/docs/ios/preface/usingios.html).
- IOS etxean praktikatzeko, GNS3 simulagailua erabili: <http://www.gns3.com/>.

### Birbidaltze-taulak eta IP konfigurazioa

IP erabiltzen duten makina guztiek behar dute birbidaltze-taula bat, bai bideratzaileek, baita erabiltzaileen makinek ere. Berez, birbidaltze-taula ondo osatzea behar-beharrezkoa da makina sarean ibili ahal izateko. Halaber, edozein makinaren IP konfigurazioa osatzeko, honako bi urrats hauek bete behar dira:

1. Interfazeak konfiguratu. Hori aurreko laborategian ikasi duzu.
2. Birbidaltze-taula osatu. Hori laborategi honetan ikasiko duzu.

Bideratzaileen kasuan, hirugarren urratsa ere gehitu behar da:

3. Birbidaltzeko ahalmena gaitu. Hori ere laborategi honetan ikasiko duzu.

Bi erako sarrerak egoten dira birbidaltze-taula batean:

- Zuzenean lotuta ditugun sareetara joateko bideak.

Sarrera horiek sistemak berak gehitzen ditu, interfaze bati IP helbidea esleitzen diogunean.

- Beste bide guztiak.

Gutxienez, besterik ezeko bidea edo sareko irtenbidea izaten da (ingelesez, *default*, gazteleraz *puerta de enlace*). Beste bide horiek eskuz sartu behar dira, edo, bestela, automatikoki ere sar daitezke. Laborategi honetan, eskuz egingo dugu. Automatikoki egitean, desberdina da erabiltzaileen makinaren kasua eta bideratzaileena. Erabiltzaileen makinaren kasuan, DHCP erabiltzen da konfigurazio automatikoa egiteko (hurrengo laborategian landuko dugu aukera hori). Bideratzaileen kasuan, bideratze-protokoloak erabiltzen dira birbidaltze-tauletako beste bideak automatikoki osatzeko.

## Birbidaltze-taulekin lan egitea Linuxen

Honako hauek dira erabiltzen diren komando nagusiak<sup>11</sup>:

- `netstat`

Hori birbidaltze-taula kontsultatzeko erabiliko dugu, **`netstat -rn`** eginez.

- `route`

Birbidaltze-taulan bide berriak sartu behar baditugu edo bideak ezabatzeko erabiliko dugu. Honako hau dugu bide bat sartzeko komandoa:

**`route add -net Helburuko_ip_sorta gw Hurrengo_bideratzailearen_IP`**

Adibidez: **`route add -net 180.132.45.0/24 gw 158.192.56.1`**

Besterik ezeko bidea sartzeko berezia da:

**`route add default gw irtenbidearen_IP`**

Dagoen bide bat ezabatu nahi badugu:

**`route del -net Helburuko_ip_sorta`**

Askoz aukera gehiago ditu `route` komandoak. Gehiago jakin nahiz gero, edo zalantzak izanez gero, kontsultatu sistemaren laguntza, **`man route`** eginez.

- Gauza berak egin daitezke `ip` komandoa erabiliz:

Taula kontsultatzeko: **`ip route sh`**

Bide bat gehitzeko: **`ip route add -net Helburuko_ip_sorta via Hurrengo_bideratzailearen_IP`**

Irtenbidea sartzeko: **`ip route add default via Irtenbidearen_IP`**

Bide bat ezabatzeko: **`ip route del -net Helburuko_ip_sorta`**

## Birbidaltzeko ahalmena gaitzea Linuxen

`Kernel`aren `ip_forward` parametroari '1' balioa eman behar zaio. Hori egiteko, bi era posible ditugu, besteak beste:

- Zuzenean parametro hori gordetzen duen fitxategian idatziz:

**`echo 1 > /proc/sys/net/IPv4/ip_forward`**

- `Kernel`aren parametroak aldatzeko `sysctl` tresna erabili:

**`sysctl -w net.IPv4.ip_forward=1`**

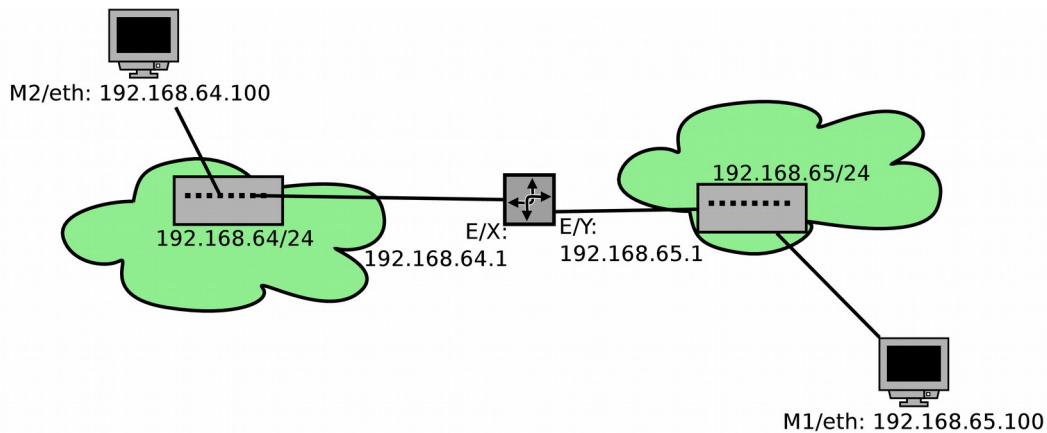
Aukera bi horiek abiatu dugun saiorako besterik ez dute balio. Hau da, makina berriz abiatzean, `kernel`erako grabatuta dauden parametroak kargatuko dira. Abiatzeko parametro horiek aldatzeko `/etc/sysctl.conf` fitxategia aldatu behar da. Ez dugu hori egingo laborategi hauetan.

## Sare-topologia

Laborategi honetan, sare bana osatuko dugu mahaian dugun konmutagailu bakoitza erabiliz. Gero, bi sare horiek elkartuko ditugu bideratzaile bat erabiliz, 1. irudian azaltzen den bezala<sup>12</sup>.

<sup>11</sup> Adi: horiek ez dira modu bakarrak lan hauek egiteko, beste ere asko badaude.

<sup>12</sup> Oharra: benetako interfazeen izenak ez dira izango irudian agertzen direnak, baizik sistema bakoitzak esleitutakoak.



**1 irudia : ariketetarako sarea. E bideratzailea EL izango da 1. eta 2. ariketan, eta EC izango da 3. ariketan.**

### 1. ariketa: sarearen ezarpen fisikoa

1. Sarea fisikoki eraiki. Horretarako:

- Kendu M1 eta M2 konputagailuetatik unibertsitateko sare-kablea, alde batera utzi, eta PIZTU BI MAKINAK. M1 eta M2n desgaitu *network-managerra* (**`sudo service network-manager stop`**). Interfaze birtualak badaude gaituta, desgaitu (**`ifconfig interfazearen_izena down`**).
- Birkonfiguratu M1 eta M2 makinaren interfazeak, 1. irudian finkatutakoaren arabera (ikusi 1. laborategia zalantzak badituzu).
- PIZTU MAHAIKO BI KOMMUTAGAILU. M1 konmutagailu batera konektatu, eta M2 beste konmutagailura, kable normalak erabiliz (ez gurutzatua!!). Ziurtatu dagozkien *ledak* berdez gelditzen direla.
- PIZTU EL makina. *Network managera* abiatuta balu, geldiarazi (exekutatu **`sudo service network-manager status`** eta ikus erantzuna). Kontsultatu interfazeen egoera, eta ez badaude gaituta, gaitu **`ifconfig interfazearen_izena up`** eginez. Ziurtatu zein den `eth0` txartela eta zein `eth1`<sup>13</sup>.
- Aztertu ELren birbidaltzeko taula. Orain, ELren interfazeetako bati 192.168.64.1 helbidea esleitu, eta M2 konektatu duzun konmutagailu berari lotu interfaze hori (adi zein den EL makinaren `eth0` eta zein `eth1`!!), kable normal bat erabiliz (ez gurutzatua!!).
- Berrikusi ELren birbidaltze-aula. Zein bide agertu da?
- *Ping* egin ELtik M2ra, eta, erantzunik ez badago, berrikusi egindakoa eta **ez jarraitu *ping* hau ibili arte**.
- EL makinaren beste interfazeari 192.168.65.1 helbidea esleitu eta interfaze horri dagokion sare-txartela M1 konputagailuarekin lotuta dagoen konmutagailuarekin konektatu, beste kable normal bat erabiliz (ez gurutzatua!!).
- Berrikusi ELren birbidaltze-aula. Zein bide agertu da oraingo honetan?
- Egin *ping* ELtik M1era. Ez badabil, berrikusi egindakoa eta **ez jarraitu *ping* hori ibili arte**.

<sup>13</sup> Gure laborategiko makina hauetan, integratuta dagoen txartelaren helbide fisikoa beti hasten da 00:0c:f1 segidarekin.



2. Egiaztatu ELren bideratze-ahalmena aktibatuta dagoela, /proc/sys/net/IPv4/ip\_forward fitxategiaren edukia aztertuz (adibidez, cat komandoa erabiliz). Aktibatuta ez balego, gaitu ezazu. Ping bat egin M1etik M2ra. Zergatik jasotzen duzu errorea? Erantzuna ez baduzu ikusten ere, segi aurrera.
3. Idatzi paper batean M1 eta M2 makinek behar dituzten birbidaltze-taulak IP konfigurazioa osatuta izateko. Zure aurreko taldearekin alderatu idatzitakoa. Aurreko taldearekin kontsultatuta ere ez baduzu ulertzen zeinek izan behar duen birbidaltze-taulen edukiak, kontsulta egin irakasleari. Zure taulak ondo daudela ziurtatu duzunean, osatu M1 eta M2 makinetan birbidaltze-taulak. Ping bat egin M1etik M2ra, eta alderantzizkoa. Baten bat ez badabil, berrikusi egindakoa eta **ez jarraitu ping horiek ibili arte**.
4. Demagun switch bakoitzarekin gure bi makinaz gain beste makina batzuk konektatuta daudela. Aldatuko al zenituzke M1, M2 eta ELren birbidaltze-taulak? Zein helbideratze-tartetan egon beharko lirakeke switchetara konektatutako makinak? Erantzunak ez badituzu topatzen, kontsultatu irakaslearekin.
5. Gure laborategiko sarea isolatuta dago. Baina demagun ELk hirugarren interfazea baduela, eth2 izenekoa, interfaze hori 158.227.112.0/20 sarera lotuta daukala, eta sare horren irtenbidea 158.227.112.1 dela. Osatu EL makinaren birbidaltze-taula paper batean eta irakasleari erakutsi.

## 2. ariketa: bideratzaile baten funtzionamenduaren analisia

1. Idatzi paper batean sarean dauden lau interfazeen helbide fisikoak (#M1/eth0, #M2/eth0, #EL/eth0, #EL/eth1).
2. Wireshark exekutatu M1n eta M2n, ICMP trafikoa soilik hartuz.
3. M2tik M1era ping bat egin (bakar bat, -c aukera erabiliz), eta trama-eskuratzea eten bi trama atzeman eta gero.
4. Aztertu jasotako tramak. Zein dira, jasotako trama bakoitzarentzat jatorri eta helburu helbide fisikoak? Azaldu nola lortu duen IP entitate bakoitzak bidalitako tramen IP helbidea (jatorrizkoa eta helburukoa).
5. Makina desberdinen artean, 30 oihartzun eskatzen duen ping bat exekutatu (-c aukera). Idatzi makina batetik bestera joan-etorria egiteko behar duten bataz besteko denbora, geroko emaitzekin alderatzeko.

### Birbidaltzearen konfigurazioa IOS sisteman

- Taularen edukia ikusteko, lan modu pribilegiatuko **sh** komandoa erabili: **sh ip route**
- Taula osoa ezabatzeko, lan modu pribilegiatuan: **clear ip route \***
- Birbidaltze-taulan bide berriak sartzeko, konfigurazio orokorreko lan moduan sartu behar da, eta hor ip komandoa erabili. Bide berri bat sartzeko:

**ip route aurrezenbakia Maskara [Hurrengo\\_bideratzailearen](#)\_@IP**

Adi, helbide sortak azaltzeko sistema zaharra erabiltzen da, maskararen bidez. Taulan dagoen bide bat ezabatzeko, 'no' aukera erabiltzen da:

**no ip route aurrezenbakia maskara**

Besterik ezeko bidea ezartzeko, 0.0.0.0 da aurrezenbakia eta maskara.

- Birbidaltzeko gaitasuna abiatzeko, konfigurazio orokorreko lan moduan: **ip routing**

<b>3. ariketa: Bide estatikoen konfigurazioa CISCO erabiliz</b>
-----------------------------------------------------------------

Oraingoan, ELren ordeztu, EC erabiliko dugu sarean eta 2.5 ariketako neurketa errepikatuko dugu. Urratsak honako hauek dira:

1. EL deskonektatu konmutagailuetatik.
2. EC PIZTU eta ireki kotsola bat ELn EC kontrolatzeko (ikus aurreko laborategiko dokumentazioa).
3. ECren interfazeak birkonfiguratu 1. irudiaren arabera. Aztertu ECren birbidaltze-taula, eta egiaztatu espero duzun bezala dagoela. Zergatik ez diozu inongo sarrerarik gehitu behar?
4. EC bideratzailearen birbidaltzeko ahalmena gaitu.
5. Egiaztatu, *ping* baten bidez, M1en eta M2ren artean konexioa dagoela. Ez badabil, berrikusi egindakoa eta **ez jarraitu *ping* hori ibili arte**.
6. Errepikatu 2.5 ariketa, eta konparatu lortutako denborak.

*Laborategitik joan aurretik, **GOGORATU**:*

- *Gorde erabilitako sare kable guztiak beren poltsan.*
- *Itzali makina guztiak: M1, M2, Linux bideratzailea, Cisco bideratzailea, eta bi konmutadoreak.*
- *Hurrengo laborategietara, enuntziatu hau eta hartutako apunteak ekarri behar dituzu.*

### **3. laborategirako teoria: DHCP**

Konputagailu bat TCP/IP sare batean konektatzeko bere IP maila konfiguratu behar dugu. Konfigurazio horren atal nagusiak sarearekiko konexioa gauzatuko duen sare-interfazeari IP helbide bat esleitzea eta konputagailuaren bideratze-taula abiatzea dira. Erabiltzaileen konputagailuen kasuan, lan horiek eskuz edo automatikoki, konfiguraziorako zerbitzari bat erabiliz, egin daitezke. Konputagailu asko dituzten sareen kudeaketa lana asko errazten du konfigurazio automatikoak, eta berdina gertatzen da konputagailuak sarritan konektatzen eta deskonektatzen direnean sarera, gero eta hedatuagoak dauden WiFi sare lokaletan gertatzen den moduan. Erabiltzaileen konputagailuen konfigurazio automatikoa ahalbidetzeko erabiltzen da DHCP protokoloa (bideratzaileentzako ez da erabiltzen).

Beste alde batetik, Interneten erabilitako IP helbideen kopurua murrizteko asmoz RFC 1918 agirian definitutako helbide pribatuen erabilera bultzatu da. Horren ondorioz, datagramak garraiatzen dituzten helbideak dinamikoki aldatu behar dira, Internet publikoan helbide pribatuko helburua duten datagramak (bideraezinak direnak) ez txertatzeko. Hori NAT izeneko teknika erabiliz lortzen da.

#### **DHCP protokoloa**

Sare konfigurazioa automatikoki egiteko bezero-zerbitzaria eredua jarraitzen da. Hau da, badago konfigurazioa egiten duen zerbitzari bat, eta zerbitzari horri eskatu behar dizkiote erabiltzaileen konputagailuek (bezeroek) bere konfiguraziorako datuak. Bezero eta zerbitzarien arteko komunikaziorako protokolo bat behar da; hori da DHCP (RFC 2131).

DHCP zerbitzuak IP helbide sorta baten kudeaketa dinamikoa ahalbidetzen du. Hau da, interfaze batek jasoko duen IP helbidea estatikoa (beti berdina) edo dinamikoa (aldakorra) izan daiteke. Esleipen dinamikoa erabilgarria da, adibidez, gure erakundeak kontrolatzen duen IP helbide sorta sarean dauden konputagailu kopurua baino txikiagoa denean, baina konputagailu guztiak ez badaude aldi berean konektatuta. Kasu horretan, konputagailu bat konektatzen denean IP helbide bat mailegatzen dio DHCP zerbitzariak. Deskonektatzen denean, erabilitako IP helbide hori askatuko da, eta beste konputagailu bati esleitu dakioke. Hori da ISP-ek egiten dutena IP dinamikoa bat ematen digutenean. Horrela, ez dugu behar IP helbide bat sarean egon daitekeen konputagailu bakoitzeko.

DHCP izan da IP helbideen eskasiari aurre egiteko tresna bat, baina bere erabilera bultzatu duen beste arrazoi bat informatika higikorren etorrera izan da. Gero eta maizago ikusten ditugu bere konputagailu eramangarria toki batetik bestera besapean daramatenak. Ikasle batek etxean erabiltzen duen makina bera eraman dezake ikastetxera, eta bieran Internetetikiko konexioa beharko du. Gune bakoitzeko sare konfigurazioa eskuz egitea ez da egokia, ezta, askotan, bideragarria ere. Behin behineko erabiltzaile asko duten sareen baldintzak idealak dira DHCP erabiltzeko: konfigurazio lanak maiz egin behar dira, konputagailuak etengabe konektatzen eta deskonektatzen direlako, eta benetan behar den IP helbide kopurua sareko erabiltzaile kopurua baino askoz txikiagoa da.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x2f5ff241
2	0.200606	192.168.61.1	192.168.61.10	DHCP	DHCP Offer - Transaction ID 0x2f5ff241
3	0.200815	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x2f5ff241
4	0.207829	192.168.61.1	192.168.61.10	DHCP	DHCP ACK - Transaction ID 0x2f5ff241
5	141.454221	192.168.61.10	192.168.61.1	DHCP	DHCP Request - Transaction ID 0x2f5ff241
6	141.460351	192.168.61.1	192.168.61.10	DHCP	DHCP ACK - Transaction ID 0x2f5ff241

Frame 1 (342 bytes on wire (342 bytes captured) on interface 0:00:00:00:00:00)

Ethernet II, Src: 00:07:e9:5c:72:a9, Dst: ff:ff:ff:ff:ff:ff

Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

Bootstrap Protocol

0000 ff ff ff ff ff ff 00 07 e9 5c 72 a9 08 00 45 10 ..... \r...E.

0010 01 48 00 00 00 00 10 11 a9 96 00 00 00 00 ff ff ..H.....

0020 ff ff 00 44 00 43 01 34 08 ec 01 01 06 00 2f 5f ...D.C.4 ...../\_

0030 f2 41 00 00 00 00 00 00 00 00 00 00 00 00 00 ..A.....

0040 00 00 00 00 00 00 00 07 e9 5c 72 a9 00 00 00 00 ..\n.....

File: (Untitled) 21: P: 6 D: 6 M: 0

### 3.1 irudia: DHCP elkarrekintza, sniffer batek hartutako traza batean.

#### Oinarrizko iharduera

DHCP konfigurazioa egiteko urratsak ondoko hauek dira:

- 1) Aurkitu DHCP zerbitzaria. Horretarako, bezeroak *DHCP discover* mezu bat bidaltzen du, UDP segmentu batean sartuta (ikusi irudiko 1. bidalketa). UDP segmentua IP datagrama batean sartu behar da, baina, zein IP helbideak, jatorrizkoa eta helburukoa, izango ditu datagrama horrek, bidaltzen duenak ez badu IP helbiderik esleituta oraindik, eta datagramaren helburuaren DHCP zerbitzariaren IP helbidea ez badu ezagutzen? Jatorrizko helbide bezala 0.0.0.0 jarriko du bezeroak, eta helburuko IP helbiderako difusio mugatuko helbide berezia erabiliko du (255.255.255.255). Helburuko helbide hori erabiltzeak erabilitako sareak difusiorako ahalmena duela suposatzen du. Gaur egun sare-txartelean Ethernet teknologia erabiltzea ia unibertsala denez (erabiltzaileen konputagailuetan, behintzat), protokoloak ezartzen duen baldintza honek ez du inor baztertzen. Datagrama difusiorako helbide fisikoa izango duen trama batean (FF-FF-FF-FF-FF-FF helbidea, Etherneten kasuan) sartu eta bidaliko da. Trama hori sareko segmentu berean dauden konputagailu guztiek jasoko dute, eta, horien artean, DHCP zerbitzariak.
- 2) DHCP zerbitzariak eskainiko dio helbide bat bezeroari, *DHCP offer* mezu bat bidaliz. Hori da 2.16 irudiko 2. bidalketa. Protokoloak DHCP zerbitzari bat baino gehiago sare berean egotea onartzen duenez, agian zerbitzari batek baino gehiagok erantzungo diote bezeroak bidalitako *discover* mezuari. Hala bada, bezeroak aukeratuko du zein zerbitzari erabili. Erantzun hauek IP helbiderik ez duen konputagailuari helarazteko, *discover* mezuak ekarri duen jatorrizko helbide fisikoa erabiliko da. DHCP *offer* mezua UDP segmentu batean sartuko da, segmentu hori IP datagrama batean, eta datagrama hori bezeroaren helbide fisikora bidalitako trama batean.
- 3) Bezeroak eskainitako helbideen artean bat aukeratuko du, eta dagokion zerbitzariari eskainitako helbidea esleitzeko eskatuko du, *DHCP request* mezu bat bidaliz. Eskaera hori eramango duen datagramaren jatorrizko IP helbidea 0.0.0.0 izango da, bezeroak ez baitu oraindik inongo IP helbiderik esleituta. Ikusi 2.16 irudiko hirugarren lerroa.

- 4) DHCP zerbitzariak helbidea esleituko dio bezeroari, DHCP *ACK* mezu baten bidez (irudiko 4. lerroa). Hemendik aurrera, eta zerbitzariak ezarritako epean, bezeroak badu esleitutako IP helbidea erabiltzea.

Egindako esleipena ez da betirako, iraungitze-epea baitu. Epe hori baino luzerago erabili nahi badu bezeroak 'bere' IP helbidea, zerbitzariari eskatu behar dio esleipen hori luzatzea. Horretarako beste DHCP *request* mezua bidaliko dio. Luzapena DHCP *ACK* mezu baten bidez emango du zerbitzariak. Irudiko 5. eta 6. bidalketetan horrelako berritzea egiten da. Ohartu irudiko ezkerreko zutabeaz, *time* izenekoak. Hor ikus daiteke egindako bi DHCP eragiketen artean emandako denbora. Hasierako 4 bidalketa, konfigurazioari dagozkionak, oso epe laburrean daude eginda (0'207 segundotan). Hurrengo bidalketa egin arte, berritzeari ekin diona, 141 segundo igaro dira: epe hori zen emandako konfigurazioa erabiltzeko muga.

DHCP zerbitzari batek IP helbideaz gain beste sare konfiguraziorako parametroak ere eman diezazkioke bezeroari. Horien artean ohikoena sareko atebidearen IP helbidea izaten da. Datu horrekin, eta esleitutako IP helbidearekin, bezeroak bere bideratze-taula eraiki ahal izango du.

### 3. laborategirako galdetegia

1. Zein interfazea aukeratu behar da *Wireshark*en, makina baten interfaze guztietan nahi badugu trafikoa zelatatzea.
2. TCP/IP arkitekturako zein mailatan kokatzen da DHCP protokoloa?
3. Zein garraio-mailako protokoloa erabiltzen dute DHCP bezeroek eta zerbitzariak beren mezuak trukatzeko?
4. Demagun CISCO bideratzaile bat konfiguratzeko ari zarela, eta FastEthernet0/0 izeneko interfazearen konfiguraziorako lan moduan zaudela. Bideratzaile hori DHCP 192.168.100.1 helbideko zerbitzariaren DHCP *relay* bilakatzeko behar den komandoa idatzi.
5. Erabili `ps` eta `grep` komandoak ea gure makinan '*server*' izena duen prozesuren bat bizirik dagoen.
6. Enuntziatuko 1. irudiko eskeman agertzen diren EC bideratzailearen interfazeen izenak erabiliz, esan zein interfaze konfiguratu beharko dugun 4. ariketan EC makina DHCP *relay* bilakatzeko.



### 3. laborategia: DHCP

Helburuak:

1. DHCPri buruzko ezagutza zabaldu eta sendotzea.
2. Linux ingurune batean, DHCP zerbitzariak eta bezeroak konfiguratzen ikastea.
3. CISCO ingurune batean, DHCP *proxy* bat konfiguratzen ikastea.
4. Sare-interfazeen oinarritzko konfigurazioa eta birbidaltze-taulak (Linux eta CISCO) berrikustea.
5. Sare-ekipoak muntatzen eta konfiguratzen trebatzea.
6. Sare-monitorizaziorako tresnak erabiltzen trebatzea.

Denbora: 2 ordu eta 25 minutu

Lan-metodologia:

1. Ondo errepasatu nola konfiguratzen den IPa Linux eta IOS makinetan.
2. Dokumentazioa irakurri, eta bete galdetegia *moodlen*.
3. Laborategian, ariketak egin, gidoian agertu ahala, eta behar dituzun apunteak hartu.
4. Erabili dituzun makinak itzali eta utzi lanpostua aurkitu duzun bezala. Ahaztu gabe, fakultateko sare-kableak konektatu berri.

**OHARRA: EZ PIZTU ORAINDIK ERABILTZAILE-MAKINAK**

#### DHCP protokoloa

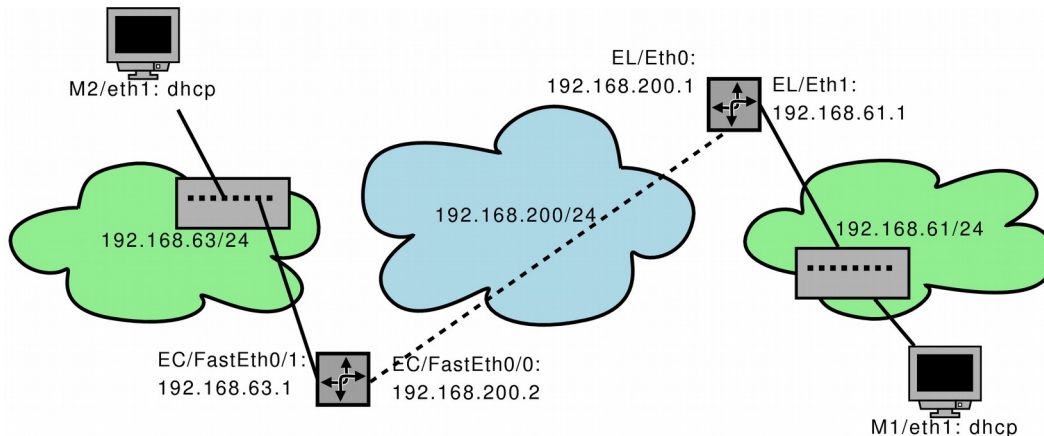
Protokolo hori erabiltzaile makinen IP parametro batzuk dinamikoki konfiguratzeko erabiltzen da. Gutxienez, IP helbidea, aurrezenbakia, eta irtenbidea eman behar zaizkio makina bati bere IP konfigurazioa osatzeko, baina, normalean, bere sareko DNS zerbitzaria zein den ere ematen zaio. DHCPk bezero/zerbitzari-ereduari jarraitzen dio: bezeroek (aplikazio mailan, berez) eskaerak luzatzen dizkiote zerbitzariari DHCP protokoloa erabiliz, eta zerbitzariak erantzuten die eskatutako konfigurazio-parametroak bidaliz. Bezeroek eta zerbitzariak UDP erabiltzen dute DHCP mezuak bidaltzeko. RFC 2131-ak azaltzen du protokolo osoa.

#### Sare-topologia

Erabiliko dugun sare-topologia 1. irudian dagoena da. Bideratzaileen IP konfigurazioa eskuz egingo dugu, baina M1 eta M2 makinen IP konfigurazioa DHCP bidez egingo da. Irudian ikus daitekeenez, laborategi honetan hiru sare eraikiko ditugu:

- 192.168.61.0/24 sarean, M1 makina eta EL bideratzailea daude. Azken horretan exekutatuko da DHCP zerbitzaria
- 192.168.63.0/24 sarean, M2 eta EC ditugu. M2k ere ELn dagoen DHCP zerbitzua erabiliko du.
- 192.168.200.0/24 sarean bi bideratzaile daude. Sare hori gauzatzeko ez dugu hirugarren konmutagailu bat mahai gainean, eta, horregatik, kable gurutzatu batekin lotuko ditugu

zuzenean EC eta EL bideratzaileak. Baina, praktikan, konmutagailu bat balitz bezala konfiguratu eta erabiliko dugu lotura zuzen hori.



1. irudia: laborategiko sare-topologia.

### 1. ariketa: Bideratzaileak abiatzea

1. EC eta EL piztu, eta EL makinaren interfazeak FISIKOKI identifikatu <sup>14</sup>.
2. Ondokoa egikaritu EL makinan: **`rm /etc/dhcp/labo3.conf`**
3. ELtik kontsola bidezko konexioa ireki ECKekin, kermi erabiliz (ikusi 1. laborategia).
4. Kable normalak erabiliz, lotu bideratzaileak konmutagailuekin, eta kable gurutzatua erabili bi bideratzaile zuzenean lotzeko, irudian azaltzen den bezala.
5. EL eta EC bideratzaileen interfazeak birkonfiguratu 1. irudiaren arabera. Begiratu beren birbidaltze-taulak: txartelei dagozkien bi bide zuzenek besterik ez dute agertu behar.
6. Bideratzaile bakoitzaren birbidaltze-taula osatu, zuzenean lotuta ez daukan sarera joateko bide bat gehituz. Birbidaltzeko ahalmena gaitu bi bideratzaileetan. Egiaztatu birbidaltze-taulen edukia bi bideratzaileetan. Espero duzuna ez bada, edo ulertzen ez duzun sarreraren bat agertzen bada, **ez segi aurrera taula konpondu arte**.
7. *Ping* bat egin ELtik ECKo interfaze bakoitzari. Erantzunik jasotzen ez baduzu, berrikusi orain arte egindakoa.
8. Idem ECKtik ELko bi interfazeetara. Baten bat ez badabil, berrikusi egindakoa, *ping* guztiak ibili arte.

## DHCP zerbitzari baten konfigurazioa eta abiatzea Ubuntu sisteman

`dhcpd` programak Linuxeko DHCP zerbitzaria abiatzen du (informazioa on-line eskuliburuan). Zerbitzaria exekutatzean, hark konfigurazioa kargatuko du `/etc/dhcp/dhcpd.conf` fitxategitik, guk beste konfigurazio-fitxategirik adierazten ez badiogu. Fitxategi horren sintaxia oso konplexua izan daiteke DHCP zerbitzuaren funtzionalitate guztiak erabili nahiz gero. Guk oinarriko konfigurazio bat egingo dugu, non:

- Hasieran ematen diren parametro orokor batzuk. Guk bat besterik ez dugu definituko, DNS eguneraketa (desgaituko dugu).

<sup>14</sup> Oinarri-plakan dagoenaren helbide fisikoa 00:0c:f1-rekin hasten da.

- Gero, zerbitzariak kudeatzen duen IP helbide sorta bakoitzeko konfigurazioa egiten den. Gure kasuan, bi sorta kudeatu behar dira, 192.168.61/24 eta 192.168.63/24.
- ELren konfigurazioan, gainera, erazagutu behar da 192.168.200/24 sorta, nahiz eta horren kudeaketa zerbitzariak ez egin, baina zerbitzariak sorta horretan duen interfazetik DHCP eskaerak onartu ahal izateko erazagutu behar da sorta hori.

Konfigurazio-fitxategia honela geldituko da:

```
##### Parametro orokorrak

# Parametro bakarra definituko dugu: ez egin DNS eguneraketarik
ddns-update-style none;

##### Ondoan, kudeatutako helbide sorten konfigurazioak.

# Lehenengo sorta, 192.168.61/24

subnet 192.168.61.0 netmask 255.255.255.0 {

    # --- Sare horren atebidea:
    option routers                192.168.61.1;

    # --- Sarean esleituko den helbide-tartea
    range 192.168.61.2 192.168.61.10;

    # --- Esleipenen iraungitze-epea
    max-lease-time 10;
    default-lease-time 10;
}

# Bigarren sorta, 192.168.63/24
subnet 192.168.63.0 netmask 255.255.255.0 {

    # --- Sare horren atebidea:
    option routers                192.168.63.1;

    # --- Sarean esleituko den helbide-tartea
    range 192.168.63.2 192.168.63.10;

    # --- Esleipenen iraungitze-epea
    max-lease-time 10;
    default-lease-time 10;
}

# Zerbitzariaren 192.168.200.2 interfazetik DHCP mezuak jaso ahal izateko
# erazagupena:

subnet 192.168.200.0 netmask 255.255.255.0 {}
```

Zerbitzariak egindako esleipenak /var/lib/dhcp/dhcpd.leases fitxategian gordetzen ditu.

## **2. ariketa: DHCP zerbitzariaren konfigurazioa eta abiatzea ELn**

1. /etc/dhcp/lab03.conf fitxategia sortu (nahi duzun editorea erabiliz), eta bete lehen azaldutako konfigurazioarekin. **Ez ahaztu fitxategi hori ezabatzea laborategitik atera baino lehen.**

2. Terminal bat ireki ELn, eta abiatu DHCP zerbitzaria **`dhcpd -f -cf /etc/dhcp/labo3.conf`** exekutatu. Ez kasu egin agertuko zaizun 'ERROR PID ...' mezuari.

OHARRA: Hobe duzu zerbitzaria abiatuz gero, hura ez gelditzea. Ezergatik gelditu behar baduzu CTRL-C erabiliz, jakin ezazu ez dela guztiz hiltzen horrela. Ondorioz, zerbitzaria berriz abiatu baino lehenago, lehen utzi duzun zombi-prozesua hil beharko duzu 'kill' komandoa erabiliz (ez badakizu nola egin, galdetu irakasleari).

`dhcpd` komandoari buruzko informazio gehiago nahiz gero, aztertu on-line eskuliburua laborategira joan aurretik: **`man dhcpd`**; **`man dhcpd.conf`**; **`man dhcp-options`**; **`man dhcpd.leases`**;

### 3. ariketa: DHCP-ren funtzionamenduaren analisia

1. Abiatu M1 konputagailua, **inongo sareri lotu gabe**<sup>15</sup>. Abiatuta dagoela, konektatu kable normal batekin, 1. irudian agertzen den moduan. Interfaze birtualak desgaitu (**`ifconfig interfaze_izena down`**) eta *network manager* abiatuta ez dagoela egiaztatu. Abiatuta balego, gelditu.
2. Egiaztatu birbidaltze-taula hutsik dagoela, **`netstat -rn`** egikaritzuz. Hutsik ez balego, hustu.
3. Exekutatu *Wireshark* M1en<sup>16</sup>, DHCP trafikoa hartzeko edozein interfazetan (any interfazea aukeratu). Horretarako behar den `capture` filtroan, DHCPk erabiltzen dituen portuak azaldu (bat bezeroentzat eta bestea zerbitzariarentzat): `port bootpc` or `port bootps`.
4. Beste terminal batetik, abiatu DHCP bezeroa zure interfazean M1en<sup>17</sup>:  
**`dhclient -d interfazearen_izena`**
5. Bezeroaren jarduera zelatatu *wireshark*aren leihoan, eta 6 trama atzematen dituenean<sup>18</sup>, *Wireshark* gelditu<sup>19</sup> eta gorde pantailan agertzen dena (hurrengo ariketan ere beharko duzu). Jasotako informazioa aztertu, eta erantzun honako galdera hauei:
  - Aztertu lehenengo trama, eta esan zein protokolo erabiltzen den arkitekturako maila bakoitzean. Oharra: DHCP protokoloa identifikatzeko, beraren aurrekaria izan zenaren izena erabiltzen da: *bootstrap protocol*. Zein protokolo erabiltzen du DHCP zerbitzariak garraiorako? Eman arrazoiren bat protokolo hori erabili behar izateko.
  - Atzeman diren 6 trama horietan, bi DHCP eragiketa egin dira: esleipen bat eta berritze bat. Paper batean idatzi horietako eragiketa bakoitzean izandako DHCP mezu-trukea, mezu bakoitzaren DHCP mota eta jatorrizko eta helburuko IP helbideak identifikatu.
  - Zein IP helbide esleitu zaio M1en interfazeari (**`ifconfig`** erabili egiaztatzeko)? Aztertu ELn `/var/lib/dhcp/dhcpd.leases` fitxategia, egiaztatzeko ikusitakoa bat datorren fitxategiaren edukiarekin. Zein sarrera agertu dira M1en birbidaltze-taulan?
  - Nola da posible M1ek DHCP zerbitzariarekin komunikatu ahal izatea IP helbiderik gabe eta birbidaltze-taula hutsik izanik?

<sup>15</sup> UPV/EHUko sarera lotuta abiatzen baduzu, unibertsitateko DHCP konfigurazioa abiatuko da, eta ezingo dituzu laborategiko ariketak ondo egin.

<sup>16</sup> Gogoratu, `sudo` moduan, ehu erabiltzaile gisa sartu bazara.

<sup>17</sup> Gero gelditzeko, CTRL-C sakatu.

<sup>18</sup> Zer edo zergatik esperimendua errepikatu behar baduzu, hurrengo egikaritzapenetan 4 trama baino ez duzu jasoko. Hasierako DISCOVER eta OFFER mezuak ez dira bidaliko. Hasierako egoera berreskuratzeko, DHCP bezeroaren *cache*a ezabatu behar duzu: `echo "" > /var/lib/dhcp/dhclient.leases`

<sup>19</sup> Aholkua: gorde jasotakoa fitxategi batean, etxera eramanez ahal izateko idatzitako dokumentazioarekin batera. Horrela, edozein momentutan berriz analiza dezakezu.

6. Errepikatu ariketa honen 1-5 atalak M2 makinan. Zergatik ez du M2k bere IP helbidea lortzen, nahiz eta zerbitzaria konfiguratuta egon 192.168.63.0/24 sarean dauden makinei IP helbideak esleitzeko? Ariketa hau bukatzen duzunean, amaitu M2n abiatutako dhcp bezeroa.

## Proxy DHCP

Aurreko ariketako 6. atalean agertzen den arazoa konpontzeko, *Proxy DHCP* zerbitzari bat erabil daiteke. (edo *DHCP relay agent*). *Proxya* atzigarri egongo da bezeroentzat, eta haien eskaerak jaso eta zerbitzarirantz bidaliko dira. Era berean, zerbitzariaren erantzunak jaso eta bezeroenganantz birbidaliko ditu. Gure laborategian, CISCO (EC) bideratzaileak *proxy DHCP* prena egingo du, 192.168.63.0/24 sarean dauden makinetarako.

## Proxy DHCP baten konfigurazioa IOSen

Egin behar den gutxienezkoa honako hau da:

- Bezeroek egindako DHCP eskaerak jasoko dituen interfazea *relay* gisa konfiguratu.
- Interfaze horretan, konfiguratu zein helbidetara (DHCP zerbitzariarena, alegia) birbidali behar diren eskaera horiek.

Aurreko biak ***ip helper-address*** komandoarekin egiten dira. Ondoko ariketan egingo dugu.

### 4. ariketa: Proxy DHCP (relay) baten funtzionamenduaren analisisia

1. Ziurtatu DHCP bezerorik ez dagoela abiatuta M2 makinan. Horretarako, begiratu ea 'dhcp' hitzak bere izenean duen prozesuren bat bizirik dagoen makina horretan, ***ps*** komandoa erabiliz: ***ps -fea | grep dhcp***. Baten bat balego, hil: ***sudo kill -9 prozesuaren\_zenbakia***.
2. Konfiguratu EC *proxy DHCP* bezala, ELn bidez zerbitzua eman ez 192.168.63.0/24 sareari. Horretarako komandoak honako hauek dira<sup>20 21</sup>:

```
CISCO(config)# interface
eskaerak_jasoko_dituen_interfazearen_izena
CISCO(config-if)# ip helper-address
DHCP_zerbitzariaren_helbidea
CISCO(config-if)# end
```

3. *Wireshark* exekutatu M2n eta EL/eth0n, eta DHCP trafikoa jaso. Aurreko ariketan definitutako iragazki bera erabil dezakezu.
4. DHCP bezeroa abiatu M2n, M1en egin zenuen bezala.
5. Eten *Wireshark* 4 trama jaso ondoren. Egiaztatu, ***ifconfig*** erabiliz, M2/eth0-k IP helbide bat duela. Egiaztatu ere M2ren birbidaltze-taula ondo bete dela.
6. Erantzun honako galdera hauei, eskuratutako tramak aztertuz:
  - Aldatu al ditu DHCP *proxy*ak birbidalitako DHCP komando edo erantzunak?
  - Aldatu al ditu DHCP *proxy*ak birbidalitako datagramen IP goiburukoak?
  - Alderatu M2k eta M1ek jasotako DHCP erantzunak. Zein da aldea?

<sup>20</sup>dhcrelay erabiliz gauza bera egin dezakegu Linuxen.

<sup>21</sup> Informazio gehiago: [https://www.cisco.com/en/US/docs/ios/12\\_4t/ip\\_addr/configuration/guide/htdhcpre.html](https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html)

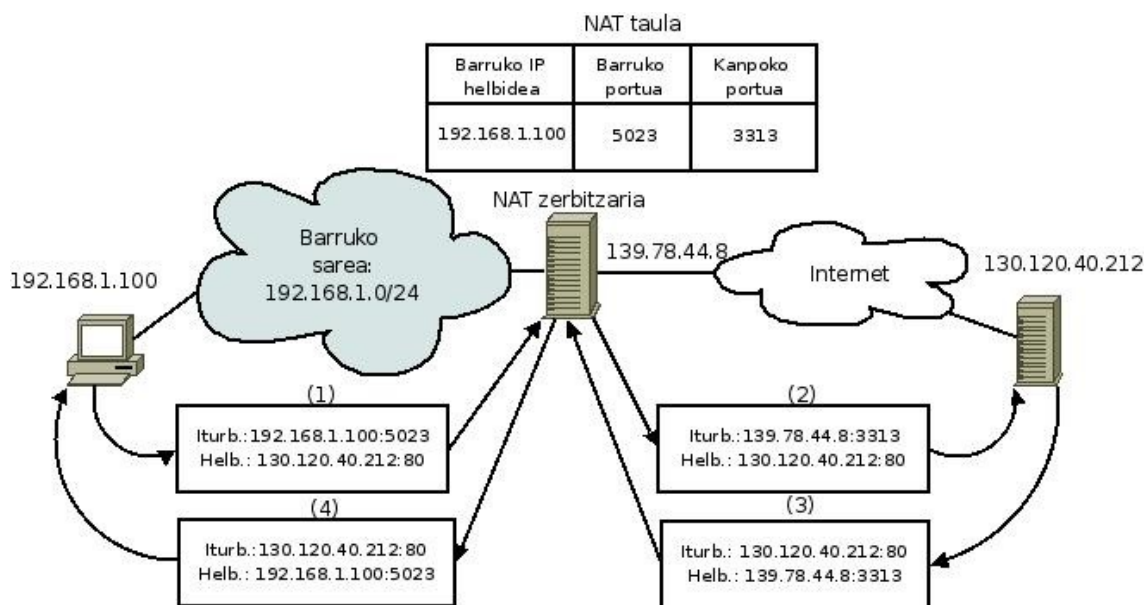
- Nola jakin dezake DHCP zerbitzariak (ELk) zein saretan dagoen DHCP request eskaera bidaltzen dion bezeroa? Nahiz eta gure sarean urrutiko sare bakarra egon, kontuan izan egoera erreal batean urrutiko zenbait sare egon daitezkeela ELn kontrolpean, eta eskaera guztiak interfaze beretik jasoko direla.

***GOGORATU: /etc/dhcp/labo3.conf fitxategia ezabatu laborategia utzi baino lehen.***



## 4. laborategirako teoria: NAT

NAT (*Network Address Translation*, RFC 2663/3022) helbide-itzulpen sistema bat da, baina ez ARP bezalakoa, IP helbide eta helbide fisikoen arteko itzulpena egiteko, baizik eta IP helbide pribatu eta publikoen artekoa. Ikusi barruko komunikazioetarako ez direla behar urriak eta ordaintzekoak diren IP helbide publikoak, nahikoa baita RFC 1918-k erabilpen pribaturako gordetzen dituen helbide sortak erabiltzea. Baina, beste alde batetik, helbide pribatu horiek Interneten dauden konputagailuekin komunikatzeko ez dute balio. NAT-ek testuinguru bakoitzean helbide mota desberdina erabiltzea ahalbidetzen du, hau da, bertako komunikazioetarako helbide pribatuak erabiltzen dituzte konputagailuek, eta Interneten ibiltzeko, publikoak. Bere abantaila erabiltako IP publiko kopuruan datza: nahikoa da helbide publiko bakarra sare oso bat Interneten ordezkatzeko.



4.1 irudia: NAT zerbitzua.

NAT-en funtzionamendua 4.1 irudian adierazten da. Hor bertako sare bat agertzen da, 192.168.1.0/24 helbide pribatuen sorta erabiltzen duena. Sare horren Internetetarako atebidean NAT zerbitzari bat dago kokatuta, saretik ateratzen diren edo sarera sartzen diren datagrama guztiak zerbitzari hori zeharkatu behar dutela ziurtatuz. Zerbitzariak helbide publiko bat (139.78.44.8) erabiltzen du bere Internetetarako konexioan, eta helbide pribatu bat barrurako konexioan (irudian ez da agertzen). Ikus dezagun zerbitzari horren lana urratsez urrats:

- (1) Barruko sareko konputagailu batek bidaltzen du datagrama bat kanpora, 130.120.40.212 IP helbidera. Gogoratu 1. ikasgaian ikusi genuela garraio mailak (TCP/UDP protokoloak erabiltzen dituenak) identifikatuko duela zein den, helburuko konputagailuan egikaritzen ari diren aplikazioen artean, datagramak daraman informazioaren helburua. Identifikazio hori hurrengo kapituluan sakonago aztertuko dugun portu zenbakiak egiten du (1. kapituluko 1.1 taulan ere aurkituko dituzu portuak). Irudiko lehenengo bidalketa 80 portura doa, web zerbitzariak erabiltzen dutena. NAT-ek portuekin lan egiten duenez (bere erabilera nagusian, behintzat), portuen kontu hau aurreratu behar izan dugu orain.

- (2) Datagrama horrek NAT zerbitzaritik igaro behar du kanpora ateratzeko. Kanpora birbidali baino lehenago, datagramaren jatorrizko helbidea ordezkatzeko du NAT zerbitzariak, helburua den web zerbitzariak erantzuna inori eman ahal izateko (helbide pribatu bati ezin zaio erantzun, bideratzaileek ez dutelako prozesatuko). Jatorrizko helbide pribatu bakoitza beste helbide publiko batekin ordezkatzeko badu NAT zerbitzariak, oinarrizko NAT (*Basic NAT*) dugu. Baina, kasu gehienetan, jatorrizko IP helbide publiko bera esleitzen zaie kanpora doazen datagrama guztiei, NAT zerbitzariaren kanpoko IP helbidea, hain zuzen. Honi **NAPT** (*Network Address and Port Translation*) edo **IP estalketa** (*IP masquerading*) deitzen zaio, barruko sare osoa NAT zerbitzariaren IP publikoak ezkututzen baitu. Baina, nola bereiztuko du NAT zerbitzariak nori dagokion Internetetik datorren datagrama bat, sareko konputagailu guztiek erabili badute jatorrizko IP helbide publiko bera kanpora bidali dituzten datagrama guztietan? Irakurleak asmatuko duenez, horretarako erabiltzen da portua. Kanpora bidalitako datagrametan, jatorrizko IP helbidea ez ezik, jatorrizko portua ere ordezkatzeko du NAT zerbitzariak, irudiko (2) datagraman agertzen den moduan: jatorrizko 5023 portuaren ordeza, 3313 ipini du NAT zerbitzariak. Egindako bidalketari dagokion erantzuna gero identifikatzeko, eta kontrako ordezkapena egin ahal izateko, [barruko helbidea + jatorrizko portua, esleitutako portua] bikotea gordeko du NAT zerbitzariak bere itzulpen taulan. Irudian, 192.168.1.100:5023 bikotea 3313 portuarekin lotuta agertzen da itzulpen taulan.
- (3) Bidalitako datagramaren erantzuna NAT zerbitzariari helduko zaio, bere kanpoko IP helbideari bidalita izango baita.
- (4) NAT zerbitzariak bere taula erabiliko du kontrako itzulpena egiteko: helburuko portuaren arabera, benetako helburuko IP helbidea eta portua eskuratuko ditu, eta datagrama barruko sarean birbidaltzeko balio horiek erabiliko ditu.

NAT teknologia IP helbideen eskasiari aurre egiteko sortu zen, baina segurtasuna ere bere bultzatzailea izan du, NAT zerbitzari batek barruko sarea ezkutatzeko baitu. Oso ohikoa da NAT eta DHCP batera erabiltzea, sareko atebidea den bideratzailean bi zerbitzariak kokatuta.

## 4. laborategirako galdetegia

1. Laborategi honetan eraiki beharko dugun sarean, zein da M1 lotuta daukan sarearen helbidea?
2. Laborategi honetan eraiki beharko dugun sarean, zein da M2 makina lotzen duen sarearen helbidea?
3. Kontuan hartuta 1. irudian eta 1. ariketan deskribatutako sare-konfigurazioa, zein izango da EC bideratzailearen birbidaltze-taulako besterik ezeko bidea (*default*)? Eman haren IP helbidea.
4. Kontuan hartuta 1. irudian eta 1. ariketan deskribatutako sare-konfigurazioa, zein izango da EL bideratzailearen birbidaltze-taulako besterik ezeko bidea (*default*)?
5. Kontuan hartuta 1. irudian eta 1. ariketan deskribatutako sare-konfigurazioa, zein izango da M1 makinaren birbidaltze-taulako besterik ezeko bidea (*default*)?
6. Kontuan hartuta 1. irudian eta 1. ariketan deskribatutako sare-konfigurazioa, zein izango da M2 makinaren birbidaltze-taulako besterik ezeko bidea (*default*)?
7. EC bideratzailea NAT zerbitzari gisa konfiguratzen badugu irudiko sarean, zein interfazeri dagokio '*inside*' izaera? Idatzi haren izena, irudian agertzen den bezala.
8. EC bideratzailea NAT zerbitzari gisa konfiguratzen badugu irudiko sarean, zein interfazeri dagokio '*outside*' izaera? Idatzi haren izena, irudian agertzen den bezala.
9. Suposa dezagun EC bideratzailearen NAT konfigurazioan nahasi zarela, eta '*inside*' moduan jarri duzula behar ez zen interfazea. Zein komandoa egikarituko duzu interfaze horren konfigurazio moduan egindakoa desegiteko?
10. Suposa dezagun EL konfiguratuta nahi duzula IP *masquerading* egiteko M1en sarerako. Zein izango da *iptables* komandoaren '--to' parametroari eman beharko diozun IP helbidea?
11. Suposa dezagun EL konfiguratuta nahi duzula IP *masquerading* egiteko M1en sarerako. Zein izango da *iptables* komandoaren '-s' parametroari eman beharko diozun balioa?

## 4. laborategia: NAT/NAPT

### Helburuak:

1. NAT/NAPT teknikak ezagutzea, baita bere konfigurazioa ere, Linux eta CISCO makinetan.
2. Sare-ekipoak muntatzen eta konfiguratzeko trebatzea.
3. Sare-monitorizazioarako tresnak erabiltzen trebatzea.

Denbora: 2 ordu eta 25 minutu

### Lan-metodologia:

1. Ondo errepetatu nola konfiguratzeko den IPa Linux eta IOS makinetan.
2. Dokumentazioa irakurri, eta bete galdetegi *moodlen*.
3. Laborategian, ariketak egin, gidoian agertu ahala, eta behar dituzun apunteak hartu.
4. Erabili dituzun makinak itzali eta utzi lanpostua aurkitu duzun bezala. Ahaztu gabe, fakultateko sare-kableak konektatu berri.

### Bibliografia:

- Cisco NAT: <http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/4606-8.html>

### NAT/NAPT itzulpena (*Network Address/Port Translation*)

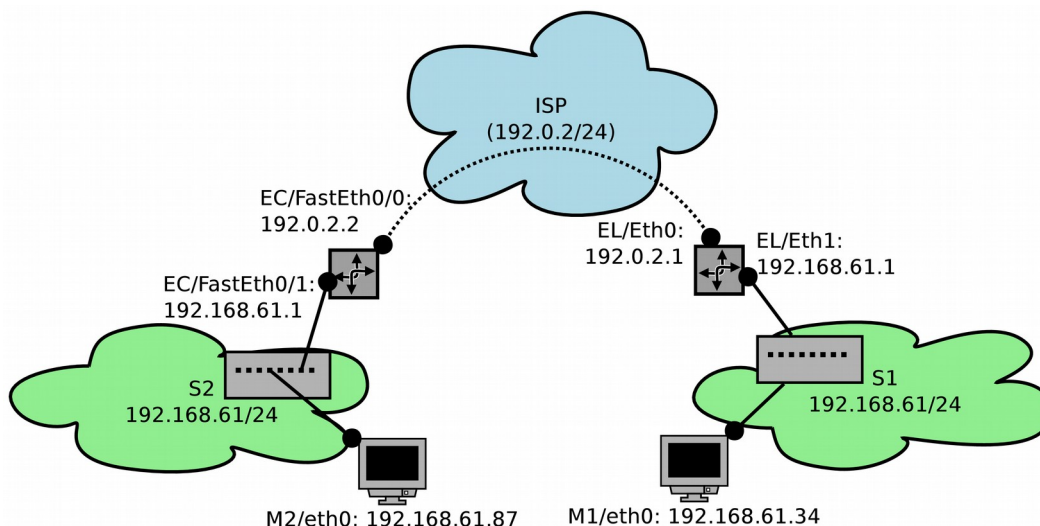
Gogoratu sare publikoko bideratzaileek ez dituztela IP helbide pribatuak zuzendurik dauden datagramak birbidaltzen. Horrek suposatzen du RFC 1918 helbideak erabiltzen dituzten makinak Internetetik isolatuta daudela. Arazoa larria izan daiteke, kontuan hartuta dagoeneko ez dela gelditzen IPv4 helbide publikorik esleitu gabe. Egoera konpontzeko, NAT zerbitzariak erabiltzen dira. Sare pribatu batean dauden makinak IP helbideak (RFC 1918 helbideak, alegia) helbide publikoekin ordezkatzen ditu NAT zerbitzariak Internetera doazen edo Internetetik datozen datagrametan (normalean, portuak ere ordezkatzen dira; horregatik, zehatzagoa litzateke NAPT deitzea). Normalean, Internetekin lotura egiten duen bideratzaileak egiten du NAT zerbitzariaren lana.

Bi NAT mota nagusi daude: estatikoa eta dinamikoa. NAT estatikoan, zerbitzarian, NAT taula bat bete behar da, adieraziz zein helbide publiko esleitzen zaion helbide pribatu bakoitzari. Ikus daitekeenez, era hori erabiliz ez dugu helbide publikorik aurrezten. Bigarren ariketan aztertuko dugu NAT estatikoa. NAT dinamikoa erabiliz, IP helbide publiko multzo bat kudeatzen da, eta horiek dinamikoki lotzen dira helbide pribatuak. NAT dinamikokoaren konfigurazio gehienetan, helbide publiko bakarra erabiltzen da (*IP masquerading*). Hori da 3. ariketan ikusiko dugun kasua.

### Sare-topologia

Laborategi honetan ezarriko dugun sare-topologia aurreko laborategiko bera da, baina sareen eta makinak IP helbide esleipena desberdina izango dugu (ikus 1. irudia). Aurreko laborategian bezala,

**puntu-lerroak kable gurutzatu baten erabilera adierazten du.** Kable horrekin, sare publiko bat simulatu dugu. Puntu beltz bakoitza IP interfaze bat da.



### 1. irudia: laborategiko sare-topologia.

Irudian ikusten denez, laborategi honetan hiru sare ditugu, baina **horietako bik, S1 eta S2 sareek, IP helbide bera dute**. Are gehiago, EC/FastEth0/1 eta EL/eth1 interfazeek ere helbide bera dute (192.168.61.1). Hori posible da 192.168.61.0/24 helbideratze-tartea RFC 1918an helbide pribatu gisa definituta dagoelako. Ikusiko dugun bezala, NATek ahalbidetzen du M1 eta M2 makinaren arteko komunikazioa, makinaren helbide pribatu horiek publikoekin ordezkatzeko baitituzte beren arteko komunikazioetan. ELk eta ECk NAT zerbitzariarenak egingo dute beren sare pribaturako, lehenengoak NAT dinamikoa gisa eta bigarrenak, berriz, NAT estatikoa gisa.

Hirugarren sareak ISP baten lana egingo du, eta suposatuko dugu S1 eta S2 sareek ISP horren bidez dutela beren Internetarako sarbidea (goranzko bidea). Egiaztatu behar genuke ISP horren sargune batera (edo PoP: *Point of Presence*), baina, horretarako, hirugarren bideratzaile bat behar genuke mahai gainean. Beraz, zuzenean konektatuko ditugu bi makina horiek, eta, gure esperimentuetarako, nahikoa izango da. Hori bai, ohartu ELren besterik ezeko bidea EC izango dela, eta kontrakoa: ECren irtenbiderako EL hartuko dugu.

### 1. ariketa: sare fisikoaren ezarpena

1. Abiatu EL eta EC. ELtik kontsola ireki ECrekin, *kermi* erabiliz (ikusi 1. laborategia). Egiaztatu zein txartel den EL/eth0 eta zein den EL/eth1. **Ez egin aurrera honetan seguru egon arte.**
2. Bi *switch*ak piztu, eta ELrekin eta ECrekin lotu 1. irudiari jarraituz. Gero, EL eta EC elkarren artean lotu, kable gurutzatua erabiliz.
3. **Interfazeak konfigurat**u ELn eta ECn, irudian dagoen bezala. Bi bideratzaileen **birbidaltze-*taulak osatu***, bietan besterik ezeko bideak gehituz, bat besteari irteera izan dadin. Hau da, ELn bide lehenetsia EC izango da eta alderantziz (bata besteari ISPa balitz bezala).
4. **Birbidaltzea gaitu ELn eta ECn<sup>22</sup>**. Egin *ping* ECtik EL/eth0ra. Ez badabil, berrikusi egindakoa, **pina ibili arte**. Nahasten bazara, eta EL/Eth0ri ordezkatu, EL/Eth1i egiten badiozu *ping*, zer gertatuko da? Errorea jasoko al duzu?
5. Egin *ping* ELtik EC/FastEthernet0/0ra. Ez badabil, berrikusi orain arte egindakoa, eta **ez egin aurrera ping hori ondo ibili arte**. Nahasten bazara, eta EC/FastEthernet0/0ri ordezkatu, EC/FastEthernet0/1i egiten badiozu *ping*, zer gertatuko da? Errorea jasoko al duzu?

6. Piztu M1 eta M2, EHUKo sareari lotuta izan gabe, ehu erabiltzailea gisa sartu, eta **network-managerra gelditu** bietan. Egiaztatu beren birbidaltze-taulak hutsik daudela. Baten bat ez badago hutsik, ondokoa egikaritzuz hustu: **ip route flush table main**.
7. M1en eta M2ren **interfazeak konfiguratu**, irudian azaltzen diren IP helbideak ezarri. Bi makinaren **birbidaltze-taulak osatu**, beren sareetatik ateratzeko besterik ezeko bideak gehituz.
8. Egin ezazu *ping* M1etik ELra (bi interfazeetara), eta M2tik ECra (bi interfazeetara). Hauetariko *pingen* batean errorea jasoz gero, aurreko pausoak berrikusi eta zuzenketak egin (**ez jarraitu ping horiek guztiak ondo jaso arte**).
9. Egin *ping* M1etik EC/FastEthernet0/0ra. Zergatik ez duzu erantzunik jaso? Bidali al du ECk erantzuna? Ez badakizu zer erantzun, abiatu *wireshark* M2n, konfiguratu haren *capture* iragazkia ICMP trafikoa harrapatzeko, eta errepikatu M1>EC/FastEthernet0/0 egindako *pinga*. Ikusten al duzu orain zer gertatu den<sup>23</sup>? Zer gertatuko da M2tik EL/eth0 interfazera egiten badugu *ping*? Eta M2—>EL/Eth1 *ping* egiten badugu?

## NAT zerbitzari estatiko baten konfigurazioa IOSen

IOSen hizkeran, sare pribatuari *inside* (barrukoa) deitzen zaio, eta publikoari *outside* (kanpokoa). CISCO bideratzailean itzulpen estatikoak konfiguratzeko honako bi pauso hauek bete behar dira:

1. Adierazi zein interfaze dauden konektaturik sare pribatura eta zein sare publikora. Horretarako, dagokion interfaze-konfigurazio lan moduan definitu interfazea pribatua ala publikoa den, honela (**ez egikaritu orain, baizik eta dagokion ariketa egitean**):

```
CISCO(config-if)# ip nat inside
```

```
CISCO(config-if)# ip nat outside
```

Gogoan izan interfazearen konfigurazio modutik ondo irten behar duzula aldaketak gordeta gera daitezen:

```
CISCO(config-if)# exit
```

```
CISCO#
```

2. Gehitu sarrera bat NAT taulan, kanpora irtengo den helbide pribatu bakoitzeko. Horretarako, konfigurazio global moduan, idatzi beharko duzu, NAT taulan sartu beharreko sarrera bakoitzeko (**ez egikaritu orain, baizik eta dagokion ariketa egitean**):

```
CISCO(config)# ip nat inside source static IPhelb1 IPhelb2
```

Aurreko komandoaren bidez, *IPhelb1* helbide pribatua, *IPhelb2* helbide publikoarekin lotzen dugu.

Egindako esleipenak ikusi ahal izateko, honako komando hau erabil dezakezu:

```
CISCO# show ip nat translations
```

Komando horrek erakutsitako taulako zutabeek honako hau esan nahi dute:

- *Inside local*: barruko makinak esleituta duen IP helbidea. Hau izango da, gure kasuan, RFC1918 helbide bat.
- *Inside global*: barruko makinak kanpora joateko erabiltzen duen IP helbidea. Helbide horrek ordezkatzeko du '*inside local*' zutabearen agertzen dena, datagrama kanpora joaterakoan.

---

<sup>23</sup> Benetako egoera batean, hau da, S1 eta S2 sareak benetako ISP bati lotuta baleude, M1>EC/FastEthernet0/0 egindako *pingaren* bistako emaitza laborategi honetan lortutako bera litzateke, hau da, ez genuke jasoko inongo erantzunik. Hala ere, sarean gertatutakoa desberdina litzateke, ISP baten bideratzaileek ez baitute birbidaltzen helbide pribatu bat daraman datagramarik.



- ## 2. ariketa: NAT zerbitzariaren konfigurazioa eta abiatzea ECn

- Laborategirako Eskuliburua*



**iptables**

*Netfilter* konfiguratzeko eta kudeatzeko aplikazioa da. Horren erabilera nahiko konplexua izan daiteke; horregatik, ohikoa da on-line eskuliburua erabili behar izatea, aukera bereziak edota xehetasunak kontsultatzeko. Honako hau da haren sintaxia:

**iptables [-t taularen\_izena] komandoa kate\_izena 1. parametroa 1. argumentua N. parametroa N. argumentua**

-t parametroarekin zein taularekin lan egin behar duzun azaltzen da. filter da taula lehenetsiaren izena. Beste aukerak, gogoan izan, nat eta mangle dira. NAT taula maneiatzeko erabiltzen diren iptables dei guztiek horrela dute hasiera:

**iptables -t nat**

Komandorik erabilienak -A (gehitu arau bat kate batera), -D (kendu arau bat kate batetik), -F (ezabatu kate bateko arau guztiak) eta -L (kate baten arauak erakutsi) dira. Parametroak eta argumentuak komandoaren arabera aldatzen dira.

Honako hauek dira NAT taularekin lotutako erabileraren adibide batzuk:

- NAT edukia ikusi:

**iptables -t nat -L** (bere egikaripenak segundo batzuk har ditzake).

- NAT taulako, POSTROUTING katearen n. sarrera ezabatzeko:

**iptables -t nat -D POSTROUTING n**

- Taulako sarrera guztiak ezabatzeko:

**iptables -t nat -F**

- Aurrezenbakia/luzera sareko helbide guztiak IPhelb helbidearekin lotzeko:

**iptables -t nat -A POSTROUTING -j SNAT --to IPhelb -s aurrezenbakia/luzera**

**3. ariketa: IP estaltzea Linuxen**

1. ELn NAT taula aldatu, M1en sare-kide direnen helbide guztiak ordezkatzeko EL/eth0 interfazearen helbide publikoarekin.
2. Kontsultatu NAT taula, aurrekoa ondo egin duzula egiaztatzeko.
3. *Wireshark* exekutatu M1 eta EL makinetan, telnet trafikoa harrapatzeko (*capture* iragazkia definitzeko: port 23)<sup>25</sup>.
4. Egin *telnet* EC/FastEth0ra M1etik (**telnet @helbidea**). ECk konexioa ukatuz erantzuten duenean, *wireshark* eten. Trama horiek aztertu, eta ikusi nola lotu diren portuak eta helbideak, ondoko taula betez. Jarri lerro bat M1etik ECra doan lehen datagramari (SYN datagrama) dagokion informazioarekin, eta beste bat, ECtik M1era doan lehenengo datagramari (RST/ datagrama) dagokionarekin.

<sup>25</sup> Adi:Lubuntun instalatuta dagoen *Wireshark*en bertsioan, interfaze bakoitzeko definitu behar dira iragazkiak; ez dago iragazki bakarra 'Capture/options' leihoan.

192.0.2.0/24 sarea(ELn atzemandu)		192.168.61.0/24 sarea (M1en atzemandu)	
Iturburu IPa: portua	Helburu IPa: portua	Iturburu IPa : portua	Helburu IPa: portua

- Exekutatu *Wireshark* M1, M2, eta EL/eth0 konputagailuetan, *ping* trafikoa jasoz (iragazkia: 2.2 ariketarena).
- Bidali *ping* bat M1etik M2ra, eta eten *Wireshark* erantzuna jaso eta gero. Zein IP helbideri egin behar izan diozu *ping*? Aztarnen arabera, ondoko taula bete, lerro bat oihartzun-eskaerarako eta beste bat oihartzun erantzunerako erabiliz:

<b>192.168.61.0/24 (M2) sarea</b>		<b>192.0.2.0/24 sarea</b>		<b>192.168.61.0/24 (M1) sarea</b>	
Iturburu IP-a	Helburu IP-a	Iturburu IP-a	Helburu IP-a	Iturburu IP-a	Helburu IP-a

- Azaldutako NAPT teknika ikus dezakezu 3.3 ariketan. Baina *ping* kasuan, igorritako ICMP mezua IP datagrametan zuzenean sartzen direnez, ez dira portuak erabiltzen. Hala ere, aurreko ariketan ikusi duzun bezala, ELk lortu du *ping*ak eragindako erantzuna behar zaion makinari helaraztea. Aztertu *wireshark*ek jasotako informazioa, ea ikusten duzun moduren bat ELk jasotako *echo reply* mezua M1erako dela asmatzeko.

## 5. laborategirako teoria: Ipv6

XX. mendeko 90. hamarkadaren hasieran hasi ziren IPv4 protokoloaren ordezkoa sortzeko ekimenak. Horren ondorioa da IPv6.

### ***Zergatik IPv6***

80. hamarkadaren bukaera aldean, une hori arte ia unibertsitateen mundura soilik mugatuta zegoen Internetek, bere komertzializazioari eta zabaltzeari ekin zion. Erakunde askok Internetera konektatu zituzten beraien sareak, A/B/C klaseetan egituratutako IP helbideak horretarako erabiliz. Interneten hazkundeak era esponentziala hartu zuen, eta hazkunde hori asetzeko IP helbideen ahalmenak kezka sortu zuen. Interneten ezaugarri teknikoak definitzen dituen IETF erakundeak (*Internet Engineering Task Force*) IP helbideratze sistemarekin lotutako ondoko arazo hauek identifikatu zituen 1992. urtean (RFC 4632):

- 1) B klaseko helbideen agorpenaren arriskua. Bere sarea Interneten sartu nahi zuten erakunde gehien-gehienek B klaseko helbide sorta eskatzen zuten, A eta C klaseen tamaina guztiz desegokia baita sare gehienerako.
- 2) Interneteko ardatz sareko bideratze-taulen gehiegizko hazkundea, garaiko hardwareak eta softwareak kudeatu zezakeen tamaina gainditzeko mehatxua sortuz. Tamaina horrek ondoko bi arazo sortzen ditu: taulen eguneraketa oztopatzen du, eta kongestioak sortarazten ditu. Alde batetik, bideratzaileek trukatu behar duten informazio kopurua ikaragarria denez, bideratzaileek denbora gehiago eman behar dute trukaketa horiek egiten datagramak bideratzen baino. Beste alde batetik, datagrama bakoitza prozesatzeko taularen bide guztiak miatu behar direnez (maskara luzeenaren araua erabiltzearen), datagrama bakoitzaren prozesatzeko denbora luzatzen da, horrekin batera prozesatzeko zain dauden datagrama-ilarak handituz. Ilara horien gehienezko luzera gaindituta, kongestioa dugu.
- 3) IPv4 helbide guztien agorpena.

Argi zegoen lehenengo bi arazoak kritikoak bihurtuko zirela 93-95. urtetarako. Irtenbide azkar baten bila, CIDR helbideratze sistema berria definitu zuten 1993. urtean. CIDR-ek helbideen egitura klaseetatik askatu zuen, askoz eraginkorragoa den helbideen esleipena ahalbidetuz, eta bideratze-taulen hazkundea moteldu zuen, bide-elkarketaren bitartez. Honek guztiak hasierako bi arazoez sortzen zuten larrialdia gainditzeko balio zuen, baina hirugarren arazoa, IP helbide guztien agorpena alegia, konpontzeke gelditzen zen oraindik. Irtenbide bakarra IP helbideen bit kopurua handitzea zen, eta horretarako nahitaezkoa zen IP-ren bertsio berri bat definitzea. Horra hor IPv6.

### ***Zertan da hobe IPv6?***

Bere hasierako eta helburu nagusia IP helbide kopurua handitzea izan arren, hori ez da IPv6-ak ekartzen duen hobespen bakarra. Ondoko hauek dira protokolo berriaren hobespen nagusiak:

- IP helbide kopurua ikaragarria da:  $2^{128}$ . Kopuru horrekin badago  $7 \times 10^{23}$  helbide esleitzea Lurreko metro karratu bakoitzean (itsasoak barne); badirudi nahikoa dela.
- Interneten ardatz sareko bideratze-taulak txikiak izango dira. Hori bermatzeko ondoko baldintzak ezarri dira:
  - IPv6 helbideak zenbaki telefonikoak bezala egituratzen dira, bideratzeko informazio topologikoa aurrezenbakian sartuz. Hau da, helbideko aurrezenbakiak identifikatutako interfazeraino heltzeko bidea adierazten du. Ikusi IPv4-ren maskarekiko aldea: maskarak

bidea aurkitzeko informazioa ematen du, baina ez du adierazten zein den helbidea identifikatzen duen konputagailuraino heltzeko bide hori.

- Aurrekoa ahalbidetzeko, IPv6 helbideak ez dira *esleitzen*, *uzten* baizik. Hau da, gure sarea Internetera konektatzen dugunean, gure ISPak utziko dizkigu horretarako beharko ditugun IPv6 helbideak. Helbide horien aurrezenbakia hornitzaile horrekin egongo da lotuta, bide elkarketaren optimizazioa ahalbidetuz: hornitzaile baten bidez Interneten sartzen diren sare guztien helbideak bide bakar batean elkartu ahal izango dira tauletan. Internet hornitzaileaz aldatzen badugu, IPv6 helbideak horrekin batera aldatu beharko dugu, tauletan zuloak ez sortarazteko. Sareen IP birzenbakitze hori era automatikoa egiten da. Honek DNS-renganako eragina ere izango du, helbidea aldatu arren, konputagailuaren izenak ez baitu aldatu behar.
- IPv6 goiburukoaren egiturak bideratzaileek egin behar duten datagrama bakoitzaren prozesamendua dezente arintzen du, ondokoengatik:
  - IPv4 datagramak prozesatzeko, bideratzaileek aztertu behar dute lehenago non bukatzen den goiburukoa (goiburukoaren hasieran aurkituko duten *goiburukoaren luzera* eremua begiratzuz), bere luzera aldarokorra baita. IPv6 bertsioan ez dute hori egin behar: datagrama guztien goiburukoek luzera bera dute (40 byte).
  - Bideratzaileetan ez dago datagramak zatitzerik. Zatiketak IPv4 goiburukoa konplexuagoa egiten du (3 eremu sartu behar dira zatiketak egiteko eta datagramak berreraikitze) eta, berriro ere, bideratzaileen lana zailtzen du. IPv6-an, datagrama bat handiegia baldin bada bideratzaileak baztertuko du, eta datagramaren igorleari kontrol-mezu bat bidaliko dio (ICMPv6 protokoloaren bidez) horren berri emanez. Igorleak berak jatorrizko datagraman sartu nahi zuen informazioa datagrama txikiagoetan banatu eta bidali beharko du.
  - Bideratzaileek ez dute inongo errore-kontrolik egin behar. Lehenago ikusi dugunez, IPv4k goiburukoan egiten duen errore-kontrolak ez du asko balio eta, gainera, bideratzaile bakoitzean datagramaren goiburukoa berregitera behartzen du (gogoan izan TTL aldatzen dela bideratzaile bakoitzean eta, beraz, errore-kontrolaren eremua birkalkulatu egin behar dela).

## IPv6 helbideak

IPv6 helbideratze sistema RFC 4291 agirian dago deskribatuta. IPv6 helbideak interfazeak edo interfaze sortak identifikatzeko 128 bit osatutako identifikadoreak dira. Bit horien barneko egitura helbide motaren arabera da.

### IPv6 helbide motak

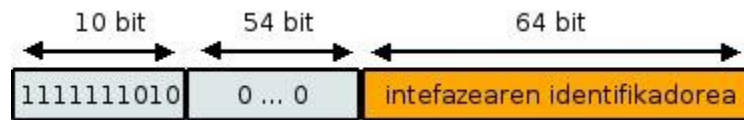
Ondoko hiru IPv6 helbide motak daude:

- Unicast helbideak, edo helburu bakarreko helbideak. Interfaze bakar bat identifikatzen dute<sup>26</sup>. Ondoko bi azpimota aurkituko dugu unicast helbideetan:
  - Bertako unicast helbideak (*Link-Local unicast*): Bere izenak adierazten duen bezala, helbide hauek esanahi lokala besterik ez dute. IPv4 helbide pribatuak bezala, bideratzaileek ez dituzte prozesatzen IPv6 bertako unicast helbideak. Beraz, zuzenean

---

26 Badago salbuespen bat, RFC 4291 agirian definituta.

lotuta dauden beste interfazeekin komunikatzeko balio dute soilik (interfazearen DHCP bidezko konfigurazioan, adibidez). Bere formatua ondoko hau da:



### 5.1 irudia: IPv6 bertako unicast helbideen egitura.

- Unicast helbide globalak (*Global unicast*): IPv4 helbide publikoen baliokideak dira helbide hauek, hau da, interfazeek behar dituzten helbideak Interneten bidezko komunikazioak egin nahi badituzte. Datagramaren helbururaino heltzeko bideratzaileraren bat baldin badago, helbide mota hau behar da helburuko interfazea identifikatzeko. IPv4-n bezala, helbidearen bitak bi zatitan daude egituratuta: hasierakoek, 'aurrezenbakia' izendatuta, sarea identifikatzen dute, eta besteek interfazea identifikatzen dute. Maskarak zehazten du zenbat bitek osatzen duten aurrezenbakia.

RFC 4291 argitaratu baino lehen (2006ko otsaila) bazegoen hirugarren azpimota bat unicast helbideetarako (*site-local unicast* izenekoa) baina dagoeneko baztertuta dago.

- Multicast helbideak, edo taldeko helbideak. Interfaze asko identifikatzen dute. Multicast helbide batera datagrama bat bidaltzen denean, datagrama horren kopia bana helbideak identifikatutako interfaze guztiei eman behar zaie.
- Anycast helbideak. Hauek ere interfaze asko identifikatzen dute, baina horietako bakar bati emango zaio anycast helbide batera bidalitako datagramaren kopia bat.

Interfaze batek behar du, gutxienez, bertako unicast helbide bat. Horrez gain, helbide gehiago ere izan dezake interfazeak, edozein motatakoak (unicast, multicast, anycast).

Ikusi difusio helbiderik (broadcast) ez dagoela IPv6 bertsioan, bere eginkizuna taldeko helbideek betetzen baitute. Etorkizunean helbide mota edo azpimota gehiago definitzea badago.

Ondoko bi helbide bereziak definitu dira:

- Zehaztu gabeko helbidea: 128 bitak zerokoak dira. Helbide hau ez zaio esleitu behar inongo interfaze bati, helbiderik ez dagoela adierazten baitu, hain zuzen ere. Bere erabilera tipikoa DHCP bidezko konfigurazioa egiteko da. Ezin da erabili helburuko helbide gisa. Bideratzaileek ez dituzte birbidaltzen jatorrizko helbidean zehaztu gabekoa daramaten datagramak.
- *Loopback* helbidea: Hasierako 127 bitak zerokoak eta azkenekoa batekoa duen helbidea dugu hau. *Loopback* izeneko interfazea birtuala da, ez fisikoa. Bere buruari datagramak bidaltzeko erabiltzen dute makinek interfaze hori. Ezin zaio inongo interfaze fisikori *loopback* helbidea esleitu, eta ezin dira makinatik kanpora bidali helbide hau daramaten datagramak (ez jatorrizko helbide gisa, ezta helburukoa ere).

IPv6 helbide motak helbidearen hasierako bitek adierazten dute, ondoko taulan agertzen denaren arabera:

<i>Helbide mota</i>	<i>Hasierako bitak</i>
Zehaztu gabekoa	000...0 (128 bitak)
Loopback	000...1 (128 bitak)
Multicast	11111111
Bertako unicast	1111111010
Unicast globala	beste guztiak

**5.1 taula:** IPv6 helbide moten identifikazioa

Anycast helbideak ez dira agertzen goiko taulan unicast helbideen espaziotik hartzen direlako (bertakoak edota globalak), eta ezin dira sintaktikoki bereiztu.

### *IPv6 helbideen idazkera*

Helbide baten 128 digitu bitarrak idaztea ez da batere eroso. Horregatik, IPv4 helbideen 32 bitekin egiten den bezala, IPv6-an ere beste notazio bat, idazteko eta ulertzeko errazagoa, definitu da. Notazio horretan hiru modu daude IPv6 helbideak idazteko:

- Oinarrizko modua: Helbidearen 128 bitak 16 biteko 8 taldetan banatzen dira, eta talde bakoitza notazio hamaseitarrean idazten da. Sortzen diren 8 zenbaki hamaseitarrak, bakoitza 4 digituk osaturik, ':' karakterekin banatzen dira. Adibideak:

- ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

- 2001:0DB8:0000:0000:0008:0800:200C:417A

Beste notazioetan bezala, hamaseitarrean ere ez dira normalean ezkerreko zeroak idazten. Horregatik bigarren adibidea arrotza da. Normalean, ondoko beste era honetan idatziko dugu helbide hori:

- 2001:DB8:0:0:8:800:200C:417A

- Modu trinkotua: Askotan topatuko dugu zeroak osatutako segida luzeak dituzten IPv6 helbideak. Segida horiek ':' karaktere bikotearekin ordeztu daitezke. Anbiguotasunak ekiditeko, behin bakarrik ager daiteke ':' karaktere bikotea helbide batean. Adibideak:

<i>Oinarrizko modua</i>	<i>Trinkotua</i>
2001:DB8:0:0:8:800:200C:417A	2001:DB8::8:800:200C:417A
FF01:0:0:0:0:0:0:101	FF01::101
0:0:0:0:0:0:0:1 ( <i>loopback</i> helbidea)	::1
0:0:0:0:0:0:0:0 ( <i>zehaztu gabeko</i> helbidea)	::

- IPv4 eta IPv6 bertsioen arteko trantsizioan zehar, bi helbideratze sistemak elkar biziko dira. Epe horretarako IPv4 helbideak IPv6 helbideetan mapeatzeko espazioa gorde da, eta notazio bat ere definitu da horretarako (*IPv4-mapped IPv6 address* izenekoa). Mapeatze hori egiteko gordetako IPv6 helbide sorta unicast helbide globalen azpitalde bat da, hasierako 80 bitak zeroak eta hurrengo 16ak batekoak dituen. Gelditzen diren azkeneko 32 bitak IPv4 helbidea adierazteko erabiltzen dira. Mapeatze honetarako definitutako notazioan, helbidearen aurreneko 96 bit lehenago definitu dugun era hamaseitarrean idazten

dira (normalean trinkotuta), eta azkeneko 32ak, aldiz, IPv4 era hamartar puntudunean. Beraz, horrelako helbide misto baten itxura ondoko adibideetakoa da:

<i>Oinarrizko modua</i>	<i>Trinkotua</i>
0:0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38
0:0:0:0:0:FFFF:158.227.112.1	::FFFF:158.227.112.1

RFC 4291 argitaratu baino lehen, bazegoen beste era bat IPv4 helbideak IPv6 helbideetan integratzeko (*IPv4-compatible IPv6 address* izenekoa), baina dagoeneko baztertuta dago.

Unicast global edo anycast helbide baten aurrezenbakiaren luzera IPv4-ren era berean adierazten da, hau da, ondokoa:

IPv6\_helbidea/aurrezenbakiaren\_luzera

non

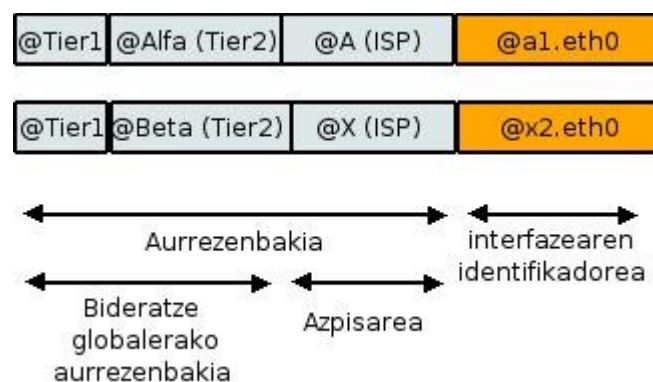
- IPv6\_helbidea aurreko edozein notaziotan idatz daiteke. Helbide osoa izan daiteke edo aurrezenbakia bakarrik. Bigarren kasu honetan idatzitakoa sare baten helbidea izango da.
- Aurrezenbakiaren\_luzera hasierako zenbat bitek osatzen duten aurrezenbakia adierazten duen zenbaki hamartarra da.

Adibideak:

2001:0DB8:0:CD30:123:4567:89AB:CDEF/64	Interfaze baten helbidea, aurrezenbakia adierazita
2001:0DB8:0:CD30::/64	Aurreko interfazearen sarearen helbidea
2001:0DB8:0:CD30::/60	Aurreko sarea barne hartzen duen beste sare baten helbidea

### Unicast helbide globalak

Unicast helbide globalen sarearen identifikadoreak barneko egitura hierarkikoa du. Zenbait eremuk osatuko dute identifikadore hori, eta horietako eremu bakoitzak Interneten barruti topologiko bat zehazten du. Adibide gisa, har dezagun 2.13 irudiko a1 eta x2 konputagailuen bi interfazen helbidea, a1.eth0 eta x2.eth0 izenekoak. Beraien unicast helbide globalen egitura ondoko irudian agertzen dena izango da:



### 5.2 irudia: IPv6 unicast helbide globalen aurrezenbakiaren barneko egitura hierarkikoa (RFC 3587).



Zenbat eremuk osatuko duten helbidearen aurrezenbakia ez dago finkaturik, baina ondoko bi dira gutxienez: bideratze globalerako aurrezenbakia (*global routing prefix*) aurreneko  $n$  bit dira, eta hurrengo  $m$  bitek azpisarearen identifikadorea osatzen dute (*subnet ID*). Aurrezenbakiaren bi eremu hauek azpieremutan egituratzen dira, hauek ere era hierarkikoan. Bideratze globalerako aurrezenbakiaren egitura RIR-ek (gogoratu, *Regional Internet Register*) eta ISP-ek definitzen dute. Azpisarearen egitura sare bakoitzaren kudeatzaileek definituko dute.

Aurreko irudian, @A eta @X dira azpisareen identifikadoreak. Interneten hierarkia topologikoaren goialdean dauden interfazeen helbideek eremu gutxiago izango dute aurrezenbakian, eta hierarkia horren behealdean daudenek, gehiago. Erabiltzaileen konputagailuek ez dute ezagutu behar beren interfazeen helbideen aurrezenbakiaren barneko egitura, hori bideratzeko informazioa baita. Nahikoa dute interfazearen identifikadorearen eta sarearen identifikadorearen arteko muga non dagoen jakitea. Bideratzaileen kasua desberdina da. Datagramak bideratu behar dituztenez, aurrezenbakiaren barneko egitura ezagutu eta erabili behar dute. Hala ere, bideratzaile guztiek ez dute ezagutu behar aurrezenbakiaren eremu guztiak. Datagrama bideratzeko zenbat aurrezenbakiko eremu ezagutu beharko dituen bideratzaileak, bideratzaile horrek sarean duen kokapenaren arabera izango da.

Aurrezenbakiaren luzera 64 bit da, hasierako 3 bit 000 direnean ez ezik. Hiru zerokoekin hasten diren helbide globalen barneko egiturarako ez dago inongo mugarik definituta. Helbide berezi horiek erabiltzen dira, oraingoz, IPv4 helbideak IPv6 helbideetan mapeatzeko (ikus gorago). Erabilpen gehiago definitu daitezke etorkizunean.

### ***Interfazearen identifikadorea***

Unicast helbideen (globalenak eta bertakoenak) interfazearen identifikadorea azkeneko 64 bitek osatzen dute, oraintxe aipatu dugun salbuespenean ez ezik. Interfaze baten identifikadoreak bakarria izan behar du aurrezenbaki bera duten interfazeen artean. Beraz, nodo baten interfaze desberdinek interfazearen identifikadore bera izan dezakete, beti ere sare desberdin batera lotuta baldin badago nodoaren interfaze horietako bakoitza. Kasu horretan bi interfazeen IPv6 helbideak aurrezenbakiak bereiztuko ditu.

Normalean, interfazearen identifikadorearen bitak sare-txartelaren helbide fisikotik abiatuta definitzen dira. Helbide fisiko bakoitzeko definitu behar da IPv6 interfazearen identifikadorea sortzeko prozedura. Ethernet helbideentzako, adibidez, RFC 2464 agiriak zehazten du prozedura hori.

### ***Anycast helbideak***

Anycast helbide batera doan datagrama bat helbide hori duen gertuen dagoen interfazera eramango dute bideratzaileak. Gaur arte ondoko bi erako erabilerak definitu dira anycast helbide hauentzako:

- Zerbitzu bat ematen duten zerbitzari guztiak identifikatzea. Horrela eginez, gertuen dugun zerbitzariak erantzun digu zerbitzu horri eskaera bat bidaltzen diogunean.
- Bideratzaile talde bat identifikatzea. Adibidez, ISP baterako sarrera diren bideratzaile guztiak identifikatuz, ISP horien bezeroek ez dute ISP-aren bideratzaile konkretu bat aukeratu behar. Era berean, sare baten bideratzaile guztiek konpartitu dezakete anycast helbidea.

Izan ere, azken erabilera horretarako anycast helbide bat dago aurredefinituta: azpisare baten bideratzaileen anycast helbidea (*subnet-router anycast address*) onartu behar dute sare baten

bideratzaile guztiek. Helbide hori sare helbidea bera da, hau da, sarearen identifikazioaren eskuinean dituen bit guztiak (interfazearenak barne) zerokoak dituen helbidea.

### ***Helbide helburuanitzak (multicast)***

IPv6 helbide helburuanitz batek interfaze talde bat identifikatzen du. Interfaze bera hainbat multicast taldetan egon daiteke. Multicast helbide batera igorritako datagramaren kopia bana eraman behar diote bideratzaileek taldeko interfaze bakoitzari. Beste alde batetik, ez dago multicast helbide bat agertzea datagrama baten jatorrizko helbidearen eremuan.



### **5.3 irudia: IPv6 multicast helbideen egitura.**

Goiko irudian adierazten den moduan, helbide helburuanitz guztiak FF digituz hasten dira. Geroko ikur-bitek ea helbidea aldi baterakoa (hau da, dinamikoki esleituta taldeari) edo betirakoa den bereizten dute, besteak beste. Betirako multicast helbideak IANAK gordetako helbide berezi batzuk dira. Adibide batzuk ondoko taulan dituzu:

<b><i>Helbidea</i></b>	<b><i>Identifikatutako taldea</i></b>
FF02::1	Sare segmentu baten nodo guztiak
FF02::2	Sare segmentu baten bideratzaile guztiak
FF05::2	Sare baten bideratzaile guztiak
FF0E::101	Internet osoan dauden NTP zerbitzari guztiak

### **5.2 taula: Gordetako IPv6 helbide helburuanitz batzuk.**

Taldearen identifikadorearen aurrean dauden 4 bitek multicast helbideak zein barruti topologikoan balio duen adierazten dute. Bit horiek erabiliz, IPv4 helbideen difusiorako eta difusio mugaturako helbideetaz gain, beste barruti desberdinetarako ere difusio helbideak definitu daitezke. Hau da, topologiaren hierarkia bakoitzeko azpisarerako definitu ditzakegu difusio helbideak. Horren adibidea 5.2 taulako bigarren eta hirugarren lerroak dira.

### ***Nodo baten helbideak eta multihoming***

IPv6 nodo batek ezagutu beharko ditu bere burua identifikatzen dituen helbide guztiak, interfazei dagozkienak eta aurredefinituta daudenak. Nodo hori erabiltzailearen konputagailu bat baldin bada (hau da, ez da bideratzaile bat), ondoko hauek dira 'bere' IPv6 helbideak:

- Bere interfaze bakoitzaren bertako unicast helbidea.
- Bere interfazeetan konfiguratutako beste edozein unicast (adibidez, globalak) eta anycast helbideak.
- Loopback helbidea.

- Gordeta dauden 'nodo guztietarako' multicast helbideak: nodo baten interfaze guztiak identifikatzen dituen (FF01::1) eta sare segmentu baten nodo guztiak identifikatzen dituen (FF02::1).
- Bere unicast eta anycast helbide bakoitzetik sortzen den multicast helbide berezi bat, *Solicited-node multicast* izeneko. Helbide hori autokonfigurazioan erabiltzen da.
- Nodoa taldekidea duten multicast talde guztien helbideak.

Bideratzaileen kasuan, aurrekoei ondoko hauek gehitu behar zaizkie:

- Bideratzaileari lotutako sare bakoitzeko, sare horren bideratzaileen anycast helbidea.
- Gordeta dauden 'bideratzaile guztietarako' multicast helbideak: bideratzailea sareekin lotzen duten interfaze guztiak identifikatzen dituen (FF01::2), sare segmentu baten bideratzaile guztiak identifikatzen dituen (FF02::2), eta sare baten bideratzaile guztiak identifikatzen dituen (FF05::2).

Gogoratu gero eta arruntagoa dela sare batek goranzko konexio ugari edukitzeak (*multihoming*). Kasu horretan, sare horren nodoek unicast helbide global ugari izango dituzte, bakoitza aurrezenbakia desberdinekin. Honek arazo berriak sortzen dizkigu datagrama bat bidaltzean:

- Alde batetik, zein jatorrizko helbidea emango diogu igorri behar dugun datagrama bati, interfazeak helbide global bat baino gehiago baldin badu? Kontuan hartu behar da aukeratuko dugun helbide horrek definituko duela zein izango den datagramaren erantzunak jarraituko duen bidea guregana itzultzeko.
- Beste alde batetik, datagramaren helburua ere sare multikonektatu batean baldin badago, zein helbidea grabatu behar dugu datagramaren helburuko helbidearen eremuan?

Aukeraketa horiek egiteko algoritmoak proposatu dira dagoeneko (RFC 3484). Hala ere, sare multikonektatuena arazo irekia da Interneten. IPv6 sareetan arazoa bideratzeko lantaldea badago Interneten (ikusi <http://www.ietf.org/html.charters/shim6-charter.html>).

<i>Helbidearen idazkera</i>	<i>Helbide mota</i>
::/128	Zehaztu gabeko helbidea
::1/128	Loopback
FFxx:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh	Multicast
FE80::hhhh:hhhh:hhhh:hhhh/64	Bertako unicast
::FFFF:d.d.d.d	IPv4-mapeatutakoak
Beste guztiak*/64	Unicast globalak

(\*) Hasierako hiru bit 000 direnak ez ezik.

**5.3 taula:** IPv6 helbideen laburpena. 'h' karaktereak edozein 4 bit biltzen dituen digitu hamaseitarra adierazten du. 'x' karaktereak aurredefinituta dauden 4 bit biltzen dituen digitu hamaseitarra adierazten du. 'd' karaktereak 8 bit biltzen dituen digitu hamartarra adierazten du.

## 5. laborategirako galdetegia

1. Zein konfigurazio global mota erabiliko dugu laborategian?
2. Zein makinatan egikaritu beharko duzu radvd programa? (idatzi haren izena 1. irudian agertzen den bezala).
3. Laborategian eraikiko dugun sarean, zein da EC bideratzailea eta M2 elkartzen dituen sareko IPv6 helbide sorta globala?
4. Laborategian eraikiko dugun sarean, zein da EL bideratzailea eta M1 elkartzen dituen sareko IPv6 helbide sorta globala?
5. Zein da IPv6 helbide lokalen helbide sorta?
6. Demagun 1 irudiko M1/eth0 interfazearen bertako *unicast* helbidea fe80::baca:3aff:fe7c:aaa6/64 dela. Idatz ezazu helbide horretara EL makinatik *ping* bat egiteko behar den komandoa. Demagun eth0 dela IPv6 sarean konektatuta dagoen ELren interfazea.
7. Egin *ping* bat 2000::baca:3aff:fe7c:aaa6 helbidera EL makinatik.
8. Idatzi zure Linux makinaren IPv6 itzulpen-taula ikusteko komandoa.
9. Idatzi zure Linux makinaren IPv6 birbidaltze-taula ikusteko komandoa.

## 5. laborategia: IPv6

### Helburuak:

1. IPv6 inguruko zenbait kontzeptu argitzea.
2. IPv6 interfazeen eta bideratzaileen oinarrizko konfigurazioa ezagutzea Linux eta CISCO testuinguruan.

### Lan-metodologia:

1. Dokumentazioa irakurri, eta bete *moodle*ko galdetegia. Ez segi aurrera galdetegiko galdera guztiei zuzen erantzun arte.
2. Laborategian, ariketak egin eta dokumentatu (hau da, zure apunteak sortu).
3. Konputagailuaren konfigurazioa zegoen bezala utzi, eta makina itzali.

### Bibliografia

- <http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO>
- <https://wiki.ubuntu.com/IPv6>
- <http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/hints-daemons-radvd.html>
- [http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/12\\_4/IPv6\\_12\\_4\\_book.html](http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/12_4/IPv6_12_4_book.html)
- <http://wiki.wireshark.org/IPv6>

### Deskribapen laburra

Laborategi honetan, honako hauek egingo ditugu:

1. IPv6 interfazeen konfigurazio lokala.
2. Irtenbideak zuzendutako autokonfigurazioa abiatu (*stateless*).
3. Bi IPv6 irla komunikatu IPv4 sarean zehar, eskuzko tunel bat erabiliz.

Erabilitako IPv6 helbide globalak adibideetarako eta dokumentaziorako gordetakoak dira (RFC 3849).

### IPv6 konfigurazioa

IPv6 sare baten konfigurazioan, bi alde bereizi behar dira: konfigurazio lokala, gure sare fisikoan IPv6 trafikoa trukatu ahal izateko, eta konfigurazio globala, beste sareekin komunikatu ahal izateko.

Konfigurazio lokala guztiz automatikoa izaten da<sup>27</sup>: interfaze bakoitzari IPv6 bertako *unicast* helbide bat esleitzen dio sistemak, bere helbide fisikotik abiatuta. Birbidaltze-taulan ere, konexio zuzenak sartzen ditu sistemak, bana interfaze bakoitzeko, eta denak helburu berekoak: helbide lokalak (fe80::/64 sorta). Horregatik, bertako *unicast* helbide bati *ping6* egiten zaionean, adierazi behar da zein interfazetatik nahi dugun bidalketa egitea.

---

<sup>27</sup> Konfigurazio automatiko hori abiatzeko, kableak konektatuta egon behar du Linux sistemetan. CISCon, gaituta egon behar du v6-k interfaze horretan.

Konfigurazio globala ere automatikoa izaten da<sup>28</sup>, batez ere erabiltzaileen konputagailuetan. Bi era daude konfigurazio hori egiteko: gure sarea IPv6 munduarekin lotzen duen bideratzaileak (hau da, gure irtenbideak) zuzenduta (*stateless autoconfiguration*) edo DHCPv6 zerbitzari bat erabilita (*stateful autoconfiguration*). Laborategian, lehenengo aukera erabiliko dugu, hau da, gure sare lokaleko irtenbideak zuzendutakoa.

### ***Neighbor Discovery Protocol (RFC 4861)***

IPv4 munduan dugun ARP protokoloaren eta taularen funtzioa *Network Discovery Protocol* izenekoak betetzen du IPv6 munduan, baita beste lan batzuk ere: irtenbidea aurkitzeko, autokonfigurazioa egiteko, helbide bikoiztuta atzemateko (*Duplicated Address Detection*) eta abar. Horretarako, honako ICMPv6 mezu hauek erabiltzen ditu:

- *Router Solicitation*
- *Router Advertisement*
- *Neighbor Solicitation*
- *Neighbor Advertisement*

Hauetako mezuren bat atzemango dugu laborategian. Zehazki, *Neighbor Solicitation* erabilera ikusiko dugu helbide bikoiztua atzemateko, interfaze baten autokonfigurazioan.

### **Irtenbideak zuzendutako autokonfigurazio globala (*stateless*, RFC 4862)**

Gure sareko irtenbideak *Router Advertisement* prozesua egikaritu beharko du. Prozesu horrek aldiro bidaltzen ditu sare-iragarpenak gure IPv6 sare fisikoan, non adierazten duen zein den sareri dagokion IPv6 aurrezenbaki globala. Sareko konputagailuek, iragarpen horiek jasota, beren interfazeak autokonfiguratu dituzte, jasotako aurrezenbakia eta interfazearen helbide fisikotik abiatuta.

### ***Linuxen***

*Router Advertisement* prozesuaren inplementazioa Linuxen *radvd* programa da. Haren konfigurazioa `/etc/radvd.conf` fitxategian gordetzen da. Fitxategi horretan, iragarri behar den sareko aurrezenbakia adierazi behar da gutxienez. Honako hau duzu horren konfigurazio minimoaren adibidea:

```
interface ethX
{
    AdvSendAdvert on;
    prefix @v6_sorta_globala/aurrezenbakiaren_luzera
    {
    };
};
```

Adibide honetan, `ethX` da gure IPv6 sare lokalari lotuta dagoen bideratzailearen interfazea. Hortik iragarriko da definitutako aurrezenbakia. Aurrezenbaki hori gure ISPak eman behar digu. Gure

---

28 Eskuz egitea ere badago, baina ez da ohikoa, batez ere *hostetan*.

laborategiko bideratzaileen kasuan ez dago horrelako ISPrik, eta, beraz, guk aukeratutako aurrezenbaki global bat hartu behar dugu. Ariketetan hartutakoa RFC3849 agirian dokumentaziorako gordetzen den 2001:db8::/32 sortatik ateratako helbide bat da.

Fitxategi horri buruzko informazio gehiago behar izanez gero, **man radvd.conf** egin.

## CISCO

Bideratzailean IPv6 birbidaltzea gaitzen dugunean, automatikoki hasiko da *Router Advertisement* mezuak zabaltzen bere sarean.

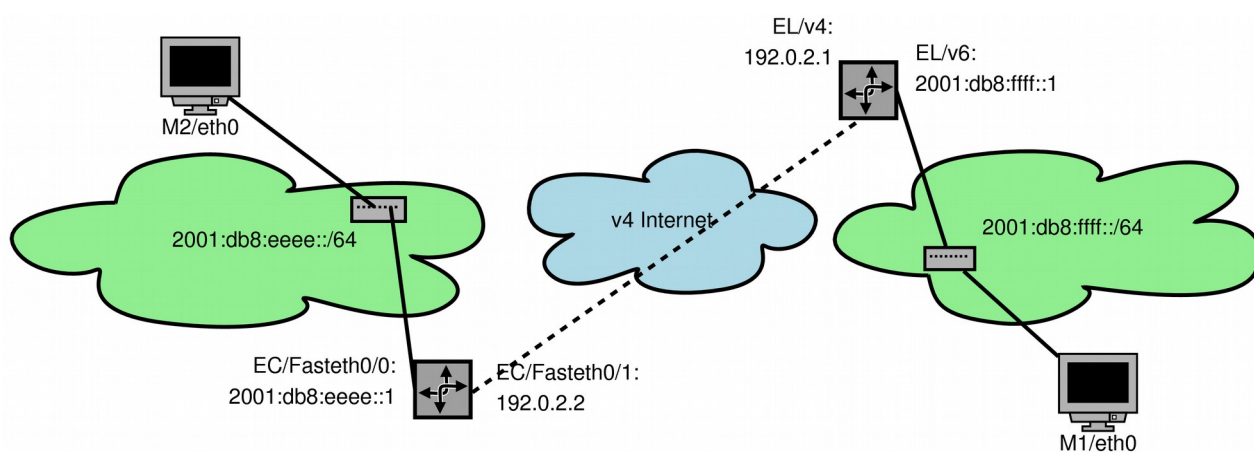
## Sare-topologia

Ezarriko dugun sare-topologia, 1. irudian azaltzen dena izango da. Kontuz Lubuntu bideratzaileen interfazeen izenekin: irudian eta testuan agertzen direnak (EL/v4 eta EL/v6) ez dira zure konputagailuetan erabiliko diren izenak (eth0 eta eth1). Aurreko laborategietan bezala, puntu-lerroak kable gurutzatu bat erabiltzen ari dela adierazten du.

Irudian ikusten denez, laborategi honetan, hiru sare ditugu:

- Bideratzaileak eta eramangarriak biltzen dituzten bi sareak. IPv6 sare hutsak dira.
- Bideratzaileak elkartzen dituen 'sarea'<sup>29</sup>. IPv4 sare bat da. Laborategi honetan, Internet balitz bezala har dezakegu sasisare hori.

Ohartu irudian ez direla adierazten eramangarrien interfazeen helbideak: **IPv6-n hainbat helbide izango dituzte interfazeek**, bertakoa eta globala, gutxienez. Biak sortuko dira automatikoki, eta, beraz, ezin diegu inongo helbiderik esleitu eramangarriei irudian. Bideratzaileen kasua desberdina da: sare-helbidea maiz esleitzen da eskuz, DHCPv6-PD (*Prefix Delegation*) erabiliz automatikoki egitea badago ere. Gure kasuan, aurrezenbakia esleitu beharko liguken ISPrik ez dagoenez, eskuz konfiguratuko ditugu bideratzaileen IPv6 interfazeen *unicast* helbide globalak, eta horiek dira irudian agertzen direnak.



1. irudia: laborategiko sare-topologia.

## Linux komandoak

Ariketak egiteko, honako tresna hauek erabiliko ditugu <sup>30</sup>:

<sup>29</sup> Fisikoki ez dago sarerik, baizik eta kable gurutzatua.

<sup>30</sup> Oharra: tresna horiei buruzko informazio gehiago behar izanez gero, erabili *man* komandoa.



- Interfazei IPv6 helbideak eskuz esleitzeko:

**ip** komandoa. Formatua:

**ip -6 addr add** helbidea/aurrezenbakiaren\_luzera **dev** interf\_izena

Adibidez: **ip -6 addr add 2001:ffff:f::1/64 dev eth0**

Esleitutako helbidea aldatu behar bada, lehenago ezabatu dagoena ('add' ordez, 'del' erabili), eta beste bat esleitu.

- Interfazeen konfigurazioa ikusteko:

**ifconfig** komandoa (aurreko laborategietan bezala) edo **ip** komandoa. Formatuak, **ip** erabiliz:

**ip -6 addr** → interfaze guztien IPv6 konfigurazioa

**ip -6 addr sh dev int\_izena** → interfaze jakin batena

- Birbidaltze-taulekin lan egiteko: **ip** edo **route** komandoak. Formatuak:

**ip -6 r** → Taula ikusteko.

**route -A inet6 | grep eth** → Idem, baina ethernet motako interfazeak soilik.

**ip -6 r sh dev int\_izena** → Interfaze bati dagozkion bideak besterik ez ikusteko.

**ip -6 r flush dev int\_izena** → Interfaze bati dagozkion bideak ezabatzeko.

**ip -6 r add IPv6\_helburua dev int\_izena** → Bide bat sartu birbidaltze-taulan.

- Itzulpen-taula ikusteko (bizilagunen taula, edo *neighbour table*):

**ip -6 neigh sh**

- Irtenbideak zuzendutako konfigurazio automatikorako: **radvd** programa. Aurrerago erakutsiko dugu hura nola erabili.

- Konputagailuen arteko konektibitatea egiaztatzeko: **ping6** programa. Betiko **ping** programaren funtzionamendu bera du **ping6** programak; hau da, ICMPv6 echo request bidaltzen du eta ICMPv6 echo reply jasotzea espero du. Hala ere, haren erabilera desberdina da, bereizi behar baita helbide globalei edo lokalei egiten zaien **pinga**. Helbide lokalei egiten zaienean, adierazi behar da zein interfazetatik bidali behar den echo-request, interfaze guztiak daudelako helbideratze-espazio berean (espazio lokalean, alegia, fe80::/64). Honako hauek dira **ping6** egiteko erabilerak:

**ping6 helbide\_globala** → helbide global bati egiteko.

**ping6 IPv6bertako\_helbidea%int\_izena** → bertako helbide bati egiteko.

**ping6 -I int\_izena IPv6bertako\_helbidea** → Idem aurrekoa.

Sareko konputagailu guztiak identifikatzen dituen IPv6 *multicast* helbidera (ff02::1) **ping6** egiten badugu, azalduko zaigu zein beste IPv6 konputagailu dauden gure sarean.

## CISCO

Komando gehienak IPv4 konfiguraziorako erabiltzen diren berak dira, besteak beste, **IPv6**. Ariketetan ikusiko dugu hura nola erabiltzen den.

## 1. ariketa: IPv6 konfigurazio lokala

1. 2001:db8:ffff::/64 sarea eraikitzeke, piztu *switch*ak, M1 eta EL/ethX<sup>31</sup> konektatu *switch* batera, eta piztu EL. Ez piztu oraindik M1. EL/ethX (oinarri plakan dagoen txartela) izango da EL/v6.
2. Egiaztatu `/etc/radvd.conf` fitxategirik ez dagoela ELn. Baldin balego, ezabatu (**`rm /etc/radvd.conf`**).
3. ELn desgaitu *privacy extensions* aukera: **`echo 0 > /proc/sys/net/IPv6/conf/all/use_tempaddr`**.
4. ELren bi interfazeak gaitu (**`ifconfig int_izena up`**).
5. Aztertu ELren bi interfazeen v6 konfigurazioa<sup>32</sup>. Zein motatakoak dira v6 helbide horiek? Alderatu IPv6 helbideak eta interfazeen helbide fisikoak.
6. Aztertu IPv6 birbidaltze-taula. Zergatik uste duzu agertzen direla bi bide fe80::/64 helburura ailegatzeko?
7. Abiatu *wireshark* EL bideratzailean, **IPv6 interfazean soilik** icmpv6 trafikoa atzemateko (*capture* iragazkia: `icmp6`).
8. Orain, piztu M1, eta *Network Managerra* desgaitu makina horretan. Desgaitu interfaze birtualak M1en (`vmnet1` eta `vmnet8`), ez oztopatzeko. Desgaitu *privacy extensions* M1n: **`echo '0' > /proc/sys/net/IPv6/conf/eth0/use_tempaddr`**.
9. *Wiresharkek* ICMPv6-ko *Neighbor Solicitation* erako mezu bat atzematen duenean<sup>33</sup>, gelditu eta aztertu atzemandakoa. Aztertu eramangarriaren v6 interfazearen IPv6 konfigurazioa. Nork bidali du mezua? Zertarako, zure ustez?  
  
Zer edo zergatik esperimentu hau errepikatu behar baduzu, ez ibili eramangarria berriz itzaltzen eta pizten: nahikoa duzu eramangarria interfazea desgaitu (down) eta berriz gaitu (up), harrapaketa abiatuta duzula.
10. Egin **`ping6`** ELtik M1era. Adi egon: dokumentazio honetan, **`ping6`** komandoaren bi erabilera adierazten dira. Zein erabili behar duzu orain? Argi ikusten ez baduzu, errepasatu 4. urratsa.
11. Konektatu EC eta M2 beste *switch*era, eta biak piztu.
12. M2n egiteko: desgaitu *Network Managerra*, eta interfaze birtualak (`vmnet1` eta `vmnet8`), ez oztopatzeko, eta desgaitu *privacy extensions*.
13. ELn egiteko: ireki *kermit* saio bat ELtik EC kontrolatzeko.
14. ECn: FastEthernet0/0 interfazean IPv6 gaitu:  
`Cisco(config-if)# IPv6 enable`  
`Cisco(config-if)# exit`
15. EC-n: IPv6 birbidaltzea ere gaitu:  
`Cisco(config)# IPv6 unicast-routing`
16. ECn: Aztertu interfazearen v6 konfigurazioa eta v6 birbidaltze-taula:

31 EthX izan behar du ELren oinarri-plakan integratuta dagoen Ethernet interfazea, makina batzuetan, `eth0` izango da, eta beste batzuetan, `eth1`. Nahasten bazara, eta erantsitako sare-txartelaren bidez konektatzen baduzu EL *switch*arekin, oinarri-plakan dagoen interfazeak ez du autokofigurazio lokala burutuko, eta ariketaren enuntziatuan aurreikusten diren gertaerak ez dira gertatuko.

32 Interfazearen batek ez badu v6 konfiguraziorik, segur aski, nahasi egin zara eta ez duzu konektatu oinarri-plakan dagoen sare-txartela.

33 Ez badu ezer harrapatzen, ziurtatu v6 interfazean SOILIK ari zarela harrapatzen. Hala eta guztiz ere, ezer harrapatzen ez badu, desgaitu `eth0` eta gaitu berriz.

```
Cisco# sh IPv6 interface
```

```
Cisco# sh IPv6 route
```

17. *Ping* egin ECTik M2ra:

```
Cisco# ping ipv6
```

Eskatuko dizkizu *ping* egiteko parametroak, helburuko IPv6 helbideaz hasita. **Ez jarraitu *ping* horri ondo ibili arte.**

## 2. ariketa: sare lokaleko autokonfigurazioa (stateless)

1. Esleitu EL/v6 interfazeari irudiaren arabera dagokion IPv6 helbide globala:

```
ip -6 addr add helbide_globala dev ethX34
```

Eta errepikatu 1. ariketako 5. urratsa.

2. Berriro aztertu ELren IPv6 birbidaltze-aula. Zein bide berri agertu da?
3. M1etik saiatzen bazara *ping6* egiten EL/v6ri berriki esleitu diozun helbide globalari, zergatik ez duzu erantzuna jasoko? Laguntza: ateratzen al da ICMPv6 *echo request* mezua eramangarritik? Erantzuna ez badakizu, erabili *wireshark* IPv6 trafikoa atzemateko eta aztertu ea bidaltzen den ala ez.
4. EL bideratzailean: */etc/radvd.conf* fitxategia sortu<sup>35</sup> editore batekin (adibidez, *vi*, *nano*, *emacs* edo *pico*), eta behar den moduan konfiguratu radvd deabrua (ikusi 2. orrialdea).
5. Gaitu ELn IPv6 bideratzaile-lana:

```
echo 1 > /proc/sys/net/IPv6/conf/all/forwarding
```

6. Abiatu *wireshark* EL/v6 interfazean, v6 interfazean IPv6 trafikoa atzemateko iragazkiarekin.
7. Abiatu<sup>36</sup> radvd ELn: ***radvd start***.
8. Begiratu ea M1/eth0 interfazeak v6 helbide globala duen. Horrela denean, gelditu *wireshark* eta aztertu atzemandako trafikoa. Adieraz ezazu nola lortu duen eramangarriak helbide global hori.
9. Aztertu eramangarriaren v6 birbidaltze-aula. Zein bide berri agertu da? Nori dagokio bide horren hurrengo bideratzailearen helbidea? Aztertu *wiresharke* harrapatutakoa, ea helbide horren arrastoa aurkitzen duzun.
10. Egin berriro 3. urratsetako *ping6* hori. Ez badabil, errepasatu egindakoa, ibili arte.
11. Begiratu M1en itzulpen taula. Zenbat IPv6 helbide daude esleituta EL/v6 interfazeari? Zergatik?

## CISCOren konfigurazioa

1. ECn: esleitu FastEthernet0/0 interfazeari irudiaren arabera dagokion IPv6 helbidea:

```
Cisco(config-if)# IPv6 address IPv6_helbidea
```

```
Cisco(config-if)# exit
```

Berrikusi EC/FastEthernet0/0 interfazearen v6 konfigurazioa eta EC makinaren v6 birbidaltze-aula. Helbide globala esleituta, EC hasiko da irtenbidearena egiten, eta, beraz, *Router*

<sup>34</sup> Dagokiona idatzi: eth0, eth1, ...

<sup>35</sup> Gerta daiteke dagoeneko fitxategia sortua izatea; kasu horretan, egiaztatu haren edukia.

<sup>36</sup> Ezergatik gelditu behar baduzu, egin '*sudo killall radvd*'.

*Advertisement* mezuak igortzen. Hori jasota, M2k bere burua konfiguratuko du komunikazio globaletarako.

2. M2/eth0 interfazearen konfigurazioa aztertu, helbide globala hartu duela egiaztatzeko, eta IPv6 birbidaltze-aula berrikusi, bide globala ere sartu dela egiaztatzeko. Egin *ping6* M2tik ECko IPv6 helbide globalera, eta alderantzizkoa. Ez jarraitu bi *ping* horiek ibili arte.

### 3. ariketa: tunel bat sortu bi IPv6 sareen artean

1. EL/v4 eta EC/FastEthernet0/1 lotu kable gurutzatuaren bidez.
2. EL/v4 eta EC/FastEthernet0/1 interfazeak konfiguratu, irudian agertzen diren IPv4 helbideekin, eta gaitu IPv4 bideratzaile izaera bi makinetan. Egin *ping* arruntak (v4) batetik bestera. Ibiltzen ez badira, errepasatu egindakoa erantzunak jaso arte.

3. ELn: tunela sortu:

***ip tunnel add tunel\_izena mode sit remote beste\_sareko\_IPv4 local gure\_IPv4***

Non:

- *tunel\_izena*: nahi duzun izena, tunela identifikatzeko zure sisteman. Tunela interfaze birtual moduan kudeatuko du Ubuntu.
- *mode sit*: IPv6 datagramak IPv4 datagrametan sartuta ibiliko direla adierazteko.
- *beste\_IPv4*: Beste muturraren IPv4 helbidea, hau da, EC/FastEthernet0/1ena.
- *gure\_IPv4*: EL/v4ren IPv4 helbidea.

Aztertu tunelaren konfigurazioa, *ifconfig* erabiliz.

4. ELn: tunela gaitu:

***ip link set dev tunel\_izena up***

5. ELn, IPv6 birbidaltze-aulan gehitu bide bat beste IPv6 **sarera** joateko tunelaren bidez:

***ip -6 r add beste\_sareko\_IPv6 dev tunel\_izena***

6. ECn, tunela sortu:

- `Cisco(config)# interface tunnel zenbaki_bat`

Interfaze birtual bat sortzen du, tunelarena egiteko, eta interfaze hori konfiguratzeko moduan sartzen da. Tunelaren identifikadoreak zenbaki bat izan behar du.

- `Cisco(config-if)# IPv6 enable`

Interfaze horretan (tunela), IPv6 ahalmena gaitzen du. IPv6 bertako helbidea esleitzen dio automatikoki.

- `Cisco(config-if)# tunnel source interfazearen_izena_edo_IPv4_helbidea`

Tunelaren bertako muturra esleitzen du. Horren IPv4 helbidea ere erabil daiteke.

- `Cisco(config-if)# tunnel destination IPv4_helbidea`

Tunelaren urrutiko muturra identifikatzen du.

- `Cisco(config-if)# tunnel mode ipv6ip`

Tunel mota esleitzen du. Dauden beste motak ikusi nahi baduzu, egin **tunnel mode** ?

- Cisco(config-if) # **exit**

Tunelaren konfigurazioa grabatzen du.

7. ECn, IPv6 birbidaltze-taulan gehitu bide bat beste v6 **sarera** joateko:

Cisco(config) # **IPv6 route beste\_sareko\_IPv6 Tunnel tunelaren\_zenbakia**

8. Egiaztatu tunela badabilela:

- Egin *ping6* ELtik EC/FastEthernet0/0ra, eta kontrakoa. Ez badabil, errepasatu egindakoa eta **ez jarraitu ondo ibili arte**.
  - Egin *ping6* ELtik M2ra, eta kontrakoa. Ez badabil, errepasatu egindakoa eta **ez jarraitu ondo ibili arte**.
  - Egin *ping6* M1etik EC/FastEthernet0/0ra, eta kontrakoa. Ez badabil, errepasatu egindakoa eta **ez jarraitu ondo ibili arte**.
  - Egin *ping6* M1etik M2era, eta kontrakoa. Ez badabil, errepasatu egindakoa eta **ez jarraitu ondo ibili arte**.
9. Abiatu *wireshark* EL/v4 interfazean, iragazkirik gabe. Abiatu *wireshark* M2n ere bai, eta egin *ping6* eramangarri batetik bestera. Aztertu eta alderatu tunelaren barruan eta kanpoan atzemandako ICMP mezuak.

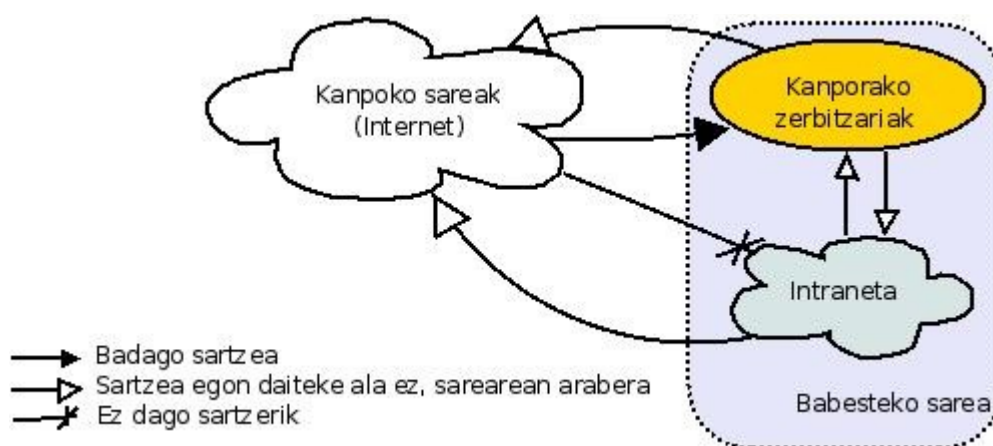
## SAIO-AMAIERA

Zure konputagailuak itzali eta laborategitik atera baino lehen, mesedez, honako hau bete:

- Zure saioko apunteak eta fitxategiak eraman eta ezabatu laborategiko makinetan.
- Ezabatu /etc/radvd.conf fitxategia:  
**rm /etc/radvd.conf**
- Itzali makina guztiak.
- Egiaztatu 6 kableak gorde dituzula beren poltsan.

## 6. laborategirako teoria: Suhesiak

Sare batean dauden konputagailuak ondoko bi taldetan banatu ditzakegu: kanpotik atzigarriak egon behar dutenak, eta egon behar ez dutenak. Lehenengo taldean egoten dira, adibidez, posta elektronikoa jaso behar dutenak, DNS jatorrizko zerbitzariak, edo kanporako web zerbitzariak. Bigarren taldekoak barruko zerbitzariak eta erabiltzaileen konputagailuak izaten dira. Bigarren talde honi *Intranet* izena ematen zaio<sup>37</sup>. Hiru mundu horien arteko atzigarritasuna 6.1 irudian duzu. Muga horiek zaintzeko teknikak osatzen dute sarrera kontrola. Hau da, sarrera kontrolak Internet eta gure konputagailu talde hauen arteko trafikoa baimenduta besterik ez dela zaindu behar du, baita gure bi konputagailu taldeen artekoa ere.



**6.1 irudia:** Gure sarerako atzigarritasuna. Babesteko sarea, normalean, gure sare pribatua da, eta, kasu horretan, kanpoko sareak Internet izango da. Hala ere, badago babestu behar den sarea gure sare pribatuko zati bat besterik ez izatea.

Sarrera kontrola irudiko mugetan kokatzen diren konputagailuek burutu behar dituzten ondoko bi zereginetan datza:

- Alde batetik, trafikoa miatu behar da, tartean trafiko maltzurra ez dela ezkututzen bermatzeko. Hau da, trafikoa iragazi egin behar da. Iragazketa lan hau **suhesiek**<sup>38</sup> (*firewall*) egiten dute.
- Beste alde batetik, urrutiko konputagailuak Intranetan sartu ahal izateko, egin beharko den urrutiko konexioa kautotu egin beharko da. Lan hori RAS zerbitzariak egiten dute (*Remote Access Server*). Zerbitzari hauek telefono bidezko konexioetarako asmatu ziren, baina gaur egun Internetetik datozen konexioetarako ere erabiltzen dira. Ohartu zaitez urrutiko konexio hauek 5.1 irudiko eskemarako salbuespentzat har daitezkeela.

Suhesiak eta RAS zerbitzariak lan horietarako espresuki jarritako makinak izan daitezke, baina, gaur egun, lan horiek sareen artean kokatzen diren bideratzaileek egiten dituzte normalean.

### Suhesiak

<sup>37</sup> Intranet bat, orokorrean, TCP/IP teknologia erabiltzen duen sare pribatu bat da. Hala ere, batzuek, barruko erabilerako soilik den web zerbitzaria deitzen dute Intranet.

<sup>38</sup> Euskaraz erabiltzen den *firewall* hitzaren beste itzulpena *suebaki* da.



Ingeleseko *firewall* terminoaren erabilera ez dago estandarizatua, hau da, errealitate desberdinak (eta, batzutan, oso desberdinak) izendatzeko erabiltzen da. Hemen erabiltzen dugun definizioa honako hau da: bi sareen arteko trafikoa halabeharrez zeharkatu behar duen makina bat da suhesia, eta makina horretan trafikoa aztertzen duen softwarea egikaritzen da.

Suhesiak sailkatzeko irizpide asko daude. Guk honako bi talde bereiztuko ditugu:

- **Pakete-iragazkiak.**

IP eta garraio mailako iragazketa lanak konbinatzen dituzte. IP mailako iragazketarako datagramaren iturburuko eta helburuko helbideak erabiltzen dira nagusiki. Horrela kontrolatu daiteke babestutako sareko zein konputagailuetarako sarrera gaituko den, baita ere zein konputagailuetarako trafikoa atera daitekeen gure saretik. Protokoloaren identifikadorea ere miatzen bada, badago konputagailu baterako trafikoa era zehatzagoan iragaztea. Adibidez, badago ICMP trafikoa blokeatzea, baina TCP eta UDP trafikoa onartzea.

Aurreko kontrolekin batera, badago garraio mailako kontrolak ezartzea, iragazketa are meheagoa egiteko. Garraio mailako iragazketa hori iturburuko eta helburuko portuen arabera egiten da, eta estatikoa ala dinamikoa izan daiteke. Estatikoa aplikazioei egindako portu esleipenean datza, hau da, portu erreserbatuen balioan. Gure sareko konputagailu baten aplikazio batzuk besterik ez izateko atzigarriak balio du, edo zein zerbitzuak eska daitezke gure sareko konputagailuetatik.

Garraio mailako iragazketa dinamikoari egoera-iragazketa ere deitzen zaio. Gure sareko bezeroek sortzen duten trafikoa kontrolatzeko balio du iragazketa honek. Egiten duena bezero bakoitzak ezartzen duen TCP konexioetan erabilitako portuen jarraipena da. Gogoratu bezeroek edozein portu, libreen artean, erabil dezaketela konexio bat ezartzean. Inongo jarraipenik egiten ez bada, gure bezeroen edozein portura igorritako trafikoa utzi beharko litzateke barrura igarotzen, eta edozein portutik bidalitakoa ateratzen utzi. Egoera-iragazkiak erabiltzen badira, ordea, TCP konexioetan erabiltzen ari diren portuetarako trafikoa soilik onartzen da barrura igarotzeko, eta portu horietatik bidalitakoa besterik ez da ateratzen utziko.

- **Aplikazioko proxiak eta pasabideak.**

Trafikoa aplikazio mailan aztertzen dutenak dira hauek. Azterketa hori aplikazio mailako goiburukoaren eremu batzuen balioaren arabera iragazketa hutsa baino gehiago izaten da. Komunikazioko bi muturretakoren bat ordezkatzan dute suhesi hauek: proxi izenekoek bezeroa eta zerbitzarien artean kokatzen dira, eta pasabideak bi zerbitzarien artean.

Proxiak kanpoan kokatutako zerbitzarietara bezeroek sortutako trafikoa bidean atzematen dute, eta ordezkatzan dute. Hau da, proxiak bezeroarena egingo du zerbitzariaren aurrean, eta zerbitzariarena bezeroaren aurrean (Hala ere, proxiaren lana ezkutua gelditzen da erabiltzailearentzat). Ez dute lan egiten aplikazio mailan bakarrik, TCP/IP goiko hiru mailetan baizik. Honako bi erako proxiak aurkituko ditugu:

- **Aplikazio batenak.** Kasu honetan proxiak aplikazio baten trafikoa besterik ez du atzematen. Oso erabiliak dira dagoneko ezagutzen ditugun web proxiak. Aurreko kapituluan proxi hauen cache lana ikusi dugu, baina, horrez gain, proxiaren bidez badago murritztea gure sareko zein konputagailuetatik atzitu daitekeen kanpoko zerbitzari edo weborri bat.
- **Orokorrak.** Hauek aplikazio askotako trafikoa (agian, aplikazio guztietakoa) atzematen dute. Atzemandako trafikoari ezarritako tratamenduak edozein aplikaziorako baliagarria



izan behar duenez, bere ahalmena mugatua da, aplikazio bakoitzak bere segurtasunerako berezko beharrak baititu. Izan ere, proxy hauek ez dute benetako iragazketa egiten aplikazio mailan (bai, ordea, iragaz dezakete IP eta garraio mailan), eta bere lana RAS (kautotzea) eta VPN zerbitzariarena (gero ikusiko dugunez, zifratzea) egitea da. Oso ezaguna eta erabilia den proxy orokorra SOCKS izeneko da. Internet estandar izateko proposatuta dagoena (RFC 1928). Esanguratsua da SOCKSen bertsio baten izena SOCKSVPN izatea.

Pasabideak proxyak bezalakoak dira, baina bi zerbitzarien arteko komunikazioetan, horietako bat ordezkatzan dute<sup>39</sup>. Bere erabileraren adibidea postarako pasabideak dira.

Bideratzaile/suhesiek sareko muga kokatzen direnez, IP/garraio/aplikazio iragazketaz gain honako lan hauek ere egin ditzakete (eta, askotan, egiten dituzte) gaur egun:

- DHCP/NAT zerbitzariarena. Ikusi NAT zerbitzari baten lana, azken finean, IP mailako proxy batena dela.
- RAS zerbitzaria. Hau da, urrutiko erabiltzaileen intranetarako sarrera kontrola egiten dute askotan suhesiek.
- VPN zerbitzaria. Gero ikusiko dugunez, honek gure intranetaren mugak gure sare fisikotik haratago hedatzen ditu.
- IDS zerbitzaria (*Intrusion Detection System*). Sistema hauek sarean dabilen trafikoa arakatzan dute, gure sarean baimenik gabeko sarrerak atzemateko nahian. Trafiko miaketa hori iragazketarekin oso erraz integratzen denez, ez da harrizkeoa makina berak bi lanak egitea.
- SNMP kudeaketarako agentea. SNMP protokoloan (*Simple Network Management Protocol*) oinarritutako sare-kudeaketarako aplikazioak erabiltzea ahalbidetzen du honek.

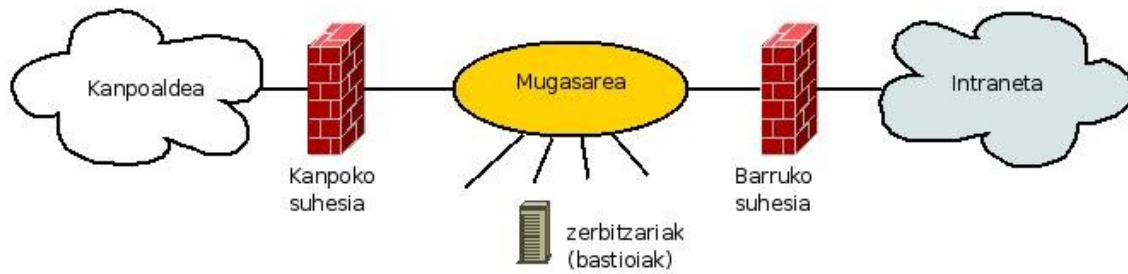
### ***Mugasareak***

Gure sarerako sarrera babesteko modurik xumeena gure sarea eta kanpoaldearen artean suhesi bat kokatzea da. Baina kanpotik atzigarriak diren zerbitzariak baditugu sarean, hori ez da nahikoa: horietako zerbitzari baten kontrako erasoren batek arrakasta lortzen badu, intraneta osoa dago arriskuan. Hortik dator 5.1 irudiko intraneta eta kanpoko zerbitzariak bilduko dituen sareak bereizteko ideia.

Mugasare bat babestu nahi dugun sarearen eta kanpoaldearen artean kokatzen den sare lokal bat da. Hau da, intraneta eta kanpoko sarearen (normalean, Internet) artean kokatuko dugun sare lokala. Sare lokal horretan, suhesiek babestuta, kanpotik atzigarriak egon behar duten konputagailuak soilik kokatu behar dira, 6.2 irudian agertzen den moduan. Bereizketa honi esker, intranetan sartzen den trafikoa kontrolatzea errazagoa izango da, baita mugasareko zerbitzari horiek babestea ere. Orain, kanpoko zerbitzarien kontrako eraso batek ez du zuzenean arriskuan jarriko intraneta. Beste alde batetik, gure intranetan sortutako erasoen kontrako babesa ere eskaintzen du mugasareak.

---

39 Berriz ere, termino honen erabilera estandarizatua ez dagoenez, 'pasabidea' hitza aurki dezakegu hemen definitu duguna ez diren kontzeptu edo teknikak izendatzeko.



## 6.2 irudia: mugasare arrunta.

Mugasarean kokatutako konputagailuetarako sarrera kontrola zerbitzari horietan bertan burutuko da, suhesiek sareko sarrera-irteerekin egiten duten modu berean. Izan ere, mugasareko zerbitzarietan kontrol hori egiten duen softwarea eta suhesietan egiten duena, baliokidea izaten da. Horregatik, zerbitzarietan instalatutako trafikoaren kontrolerako softwareari suhesi lokala deitzen zaio, eta horrelako softwarea erabiltzen duen zerbitzariari, gotorlekua (*bastion* ingelesez). Aipatzekoa da mugasareak deitzeko DMZ siglak ere erabiltzen direla maiz (*DeMilitarized Zone*).

Azpimarratu behar da mugasareak gure sarera sartzen den trafikoa kontrolatzeaz gain, gure saretik ateratzen dena behatzeko ere balio duela. Zonbi-konputagailuetaz egindako erasoen garrantzia handitzen den heinean, gure sarean sortutako segurtasun arazoei arretaren beharra ere handitu egin da.

Beste alde batetik, ohartu mugasareen erabilera ez dela gure sarea Internetetik isolatzea bakarrik. Gure sare barruan ere, azpisareen arteko mugasareak jartzea badago.

## 6. laborategirako galdetegia

1. Idatzi *iptables* komandoa iragazpen taula ikusteko Linuxen. Laguntza duzu Interneten (adibidez, <https://help.ubuntu.com/community/IptablesHowTo>) edo, bestela, '*man iptables*' Linux sistema batean.
2. Idatzi *iptables* komandoa iragazki taula osoa ezabatzeko.
3. Zein da gure makinak sortutako trafikoari aplikatzen zaion *iptables* katea? Kontuan izan letra handiekin idazten dela
4. Zein datagrama aplikatzen zaien *iptables*eko INPUT katea? Aukera ezazu bat:
  - a. Bere helburuko IP helbidea gure makinarena dutenei.
  - b. Gure makinara heltzen diren datagrama GUZTIEI, bai bere helburua gure makina direnei, baita gure makina zeharkatzen dutenei ere.
  - c. Bere iturburuko IP helbidea gure makinarena dutenei.
  - d. Gure makinatik ateratzen diren datagrama GUZTIEI, bai gure makinak sortutakoei, baita gure makinak birbidalitakoei ere.
5. Zein datagramari aplikatzen zaie *iptables*eko FORWARD katea? Aukeratu ezazu bat:
  - a. Gure makina zeharkatzen duten datagrama GUZTIEI.
  - b. Gure makinara heltzen diren datagrama GUZTIEI, bai beren helburua gure makina direnei, baita gure makina zeharkatzen dutenei ere.
  - c. Beren iturburuko IP helbidean gure makinaren helbidea dutenei.
  - d. Beren helburuko IP helbidean gure makinaren helbidea dutenei
6. Zein da gotorleku bat eta suhesi baten alde nagusietako bat? Aukeratu ezazu bat:
  - a. Gotorlekuak berari bidalitako trafikoa eta berak bidalitako trafikoa besterik ez du iragazten. Suhesiak, berriz, birbidaltzeko trafikoa ere iragazten du.
  - b. Gotorlekua *iptables*ekin konfiguratzeko da, eta suhesia, berriz, ACLkin.
  - c. Gotorlekuan, NAT taula konfiguratzeko da, eta suhesian, berriz, FILTER taula.
  - d. Gotorlekua Linux da eta Suhesia IOS da.

7. Zein lerro gehitu behar zaio 3.3 ariketan M2 makinaren birbidaltze-taulari? Aukeratu ezazu bat:
- a. *Default* bidea, 192.168.64.1 interfazetik.
  - b. 192.168.64.0/24 sarera joateko bidea, edo, bestela, *default*, edozein kasutan 192.168.65.100 bideratzailetik.
  - c. 192.168.64.0/24 sarera joateko bidea, edo, bestela, *default*, edozein kasutan 192.168.65.1 bideratzailetik.
  - d. Ez da ezer gehitu behar M2ren birbidaltze taulan.
  - e. 192.168.64.100 makinara joateko bidea, 192.168.65.1 bideratzailetik.
  - f. 192.168.65.100/24 sarera joateko bidea, 192.168.65.1 bideratzailetik.
  - g. 192.168.64.0/24 sarera joateko bidea, 192.168.64.1 bideratzailetik.
8. Zein sarrera gehitu behar da 3.3 ariketan EL makinaren birbidaltze-taulan, interfazeak konfiguratu eta gero? Aukeratu ezazu bat:
- a. 192.168.64.0/24 sarera joateko bidea, 192.168.64.1 bideratzailetik, eta 192.168.65.0/24 sarera joateko bidea, 192.168.65.1 bideratzailetik.
  - b. 192.168.64.100 makinara joateko bidea, 192.168.64.1 bideratzailetik, eta 192.168.65.100 makinara joateko bidea, 192.168.65.1 bideratzailetik.
  - c. *Default* bidea, 192.168.64.1 bideratzailetik, eta beste *default* bidea 192.168.65.1 bideratzailetik.
  - d. Ez da ezer gehitu behar birbidaltze-taulan.
9. Zein da besterik ezeko ekintza ACL zerrenda batean? Aukeratu ezazu bat:
- a. ACCEPT
  - b. in
  - c. any
  - d. permit
  - e. REJECT
  - f. FORWARD
  - g. DROP
  - h. deny
  - i. out
10. Idatzi IOSn komando bat, 110 izeneko ACL zerrenda batean arau bat gehitzeko, 192.168.64.1 helbidera doan trafiko guztia baztertzeko.
11. Idatzi IOS komandoa, 110 identifikadorea duen ACL zerrenda batean interfaze batetik heltzen den trafikoari aplikatzeko.

## 6. laborategia: Suhesiak

Helburuak:

1. Linux eta IOSen oinarritzko suhesi-konfigurazioak egiten ikastea.
2. Interfazeen eta bideratze estatikoaren oinarritzko konfigurazioen errepasoa, Linuxen eta IOSen.
3. Sare-ekipoen muntaia eta konfigurazioan trebatzea.

Lan-metodologia:

Laborategira joan baino lehen:

1. Dokumentazioa irakurri eta 1. ariketa egin.
2. *Moodle*ko galdetegia bete.

Laborategian bertan:

1. Ariketak egin, gidoian agertu ahala, eta erantzunak fitxategi batean idatzi eta gorde. Horrela, testuaz gain, pantaila desberdinen irudiak ere har ditzakezu zure apunteak osatzeko.
2. Makina itzali aurretik, eraman zurekin sortutako dokumentuaren kopia.
3. Erabili dituzun makinak itzali eta utzi lanpostua aurkitu duzun bezala.

Bibliografia

- Linuxeko suhesiak:  
<https://help.ubuntu.com/community/IptablesHowTo>  
*man iptables*
- IOSeko ACLei buruz:  
[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfaclds.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfaclds.html)  
<http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>

### Suhesiak Linuxen

4. laborategian, *netfilter* softwarea eta haren *iptables*<sup>40</sup> aplikazioa azaldu genituen. 4. laborategian, itzulpen-taula landu genuen (NAT), eta, laborategi honetan, iragazki-taula erabiliko dugu. Gogoratu *iptables* aplikazioaren sintaxi orokorra:

***iptables [-t taularen\_izena] komandoa kate\_izena 1. parametroa 1. argumentua N. parametroa N. argumentua***

*filter* da taula lehenetsia. Horregatik, -t aukera ez dugu erabiliko laborategi honetan.

Parametroak eta argumentuak erabileraren araberakoak dira. Xehetasunak kontsultatzeko, goian duzun bibliografia erabili (edo zure gustuko beste edozein).

---

40 Bertsio zaharra, *ipchains*, erabilgarri dago oraindik, sistema askotan.

Iragazki-taula (*filter* taula, alegia) hiru kateetan dago antolatutik: gure makinarentz zuzendurik datozen datagrama aplikatzen zaiena (*INPUT* katea), gure makinak sortzen dituen datagrama aplikatzen zaiena (*OUTPUT* katea), eta makina bideratzaile gisa lan egiteko konfiguratuta dagoenean, birbidalitako datagrama aplikatzen zaiena (*FORWARD* katea). Datagrama bakoitza, dagokion kateko arauekin alderatzen da, banan-banan. Datagramak arau baten baldintza betetzen badu, bi hauetako bat gertatuko da:

- Arau horren ekintzak datagramaren prozesamenduaren bukaera ekartzea. Hori da **ACCEPT** eta **DROP** ekintzen kasua, besteak beste. Lehenengoarekin datagrama onartuta izango da, hau da, bidalita (*OUTPUT* katea badagokio), jasota (*INPUT* katea badagokio) edo birbidalita (*FORWARD* katea badagokio). **DROP** ekintzaren kasuan, aldiz, datagrama baztertua izango da.
- Arau horren ekintzak datagramaren prozesamenduaren bukaera ez izatea. Horrela izanik, adierazitako ekintza bete eta gero, kateko hurrengo arauekin alderatuz jarraituko du datagramaren prozesamendua. Hori da **LOG** ekintzaren kasua, hurrengo ekintzan gertatuko grabatu nahi denean erabilia. Kasu horretarako, baldintza bera duten bi arau jarraian sartzen dira taulan: batetik, **LOG** ekintza duena, gertatuko erregistratzeko jartzen da, eta, bestetik, **ACCEPT**, **REJECT** edo **DROP** dena, ekintza betetzeko. Adibidez:

***iptables -A FORWARD -p tcp -j LOG --log-prefix "TCP trafikoa atzemanda eta baztertua"***

***iptables -A FORWARD -p tcp -j DROP***

Bi arauak jarraian grabatuta, lehenak birbidaltzekoa den tcp trafikoa atzematen du, eta horren berri grabatzen du sistemako *log* fitxategian<sup>41</sup> (bitakora, alegia), eta bigarrenak trafiko bera atzematen du, eta baztertzen du.

Datagrama kateko bukaeraraino ailegatzen bada, kate horren besterik ezeko ekintza egikarrituko da. Besterik ezeko ekintza hori **-P** komandoarekin (*policy*) defini daiteke, baina, definituta ez badago, ACCEPT egikarrituko da.

### ***1. ariketa: iptablesen erabilera***

#### **ARIKETA HAU EGIN BEHAR DA GALDETEGIA BETE BAINO LEHEN**

1. Kontsultatu (ikusi bibliografia) **eta ikasi** zer egiten duen hauetako egikaripen bakoitzak:

***iptables -F***

***iptables -L***

***iptables -A OUTPUT -p icmp -j ACCEPT***

***iptables -D INPUT 2***

***iptables -A INPUT -j LOG --log-prefix "Iragazkia INPUT:"***

***iptables -I INPUT 3 -j DROP***

***iptables -A FORWARD -p icmp -j ACCEPT***

***iptables -A FORWARD -d 158.227.112.1 -p tcp -dport 23 -j ACCEPT***

***iptables -A FORWARD -s 158.227.112.0/24 -j DROP***

***iptables -A FORWARD -p icmp -j ACCEPT --icmp-type echo-request***

<sup>41</sup> *Log*-mezuak, sistemaren *logen* konfigurazioan adierazten den lekuan gordeko dira. Gure makinak, *log*-mezuak */var/log/syslog* fitxategian gordetzeko daude konfiguratutik.

2. Zein da honakoko bi ekintza hauen arteko aldea?

***iptables -A OUTPUT -j DROP***

***iptables -A OUTPUT -j REJECT***

3. Zein eragina du honako arau hau azkena jartzeak bere katean?

`iptables -A {OUTPUT, INPUT, edo FORWARD} -j ACCEPT`

### 2. ariketa: gotorleku baten konfigurazioa Linuxen

1. Piztu M1 eta M2 makinak, UPV/EHUko sareari lotu gabe, eta *Network Manager*ra desgaitu. Sortu lab6 izeneko fitxategi bat M1en, eta hor idatzi M1 makinako *netfilter*a honako arautegi hau betetzeko behar diren komandoak:

- ICMP trafikoa onartu, barrurantz eta kanporantz.
- Beste edozein trafiko baztertu, bai barrurantz nahiz kanporantz, eta baztertutako trafiko guztiaren erregistroa (*log*) gorde. Baztertutako datagrama baten erregistroa gordetzeko, *LOG* ekintza duen arau bat txertatu behar dugu datagrama baztertuko duen arauaren aurrean bertan, eta baldintza berarekin.

Oharra: hobe duzu zure fitxategi horren lehenengo komandoa taula garbitzea izatea. Bestela, egikaritzen duzun bakoitzean, arau berriak txertatuko dituzu, aurrekoak ezabatu gabe.

2. Egikaritu lab6 fitxategia (***sudo ./lab6***).

3. Aztertu iragazki-taularen edukia, behar bezala konfiguratu duzula egiaztatzeko.

4. Konektatu bi erabiltzaile makinak konmutagailu bat erabiliz, eta konfiguratu beren interfazeak 192.168.64.100/24 (M1) eta 192.168.64.200/24 (M2) IP helbideekin.

5. Aztertu M1 eta M2 birbidaltze-aulak, eta egokiak ez badira (interfazeak ondo konfiguratu badituzu, zuzenak izan behar lirateke), egokitu. Kontuan izan sare lokal isolatua egin dugunez, taulan ez dugula *default* biderik behar.

6. Egiaztatu *ping* egin dezakezula makina batetik bestera.

7. Aldatu lab6 fitxategia, barrurantz datorren ICMP trafikoa baztertzeko (DROP). Gehitu, gainera, *log* bat 'baztertuta' mezua baztertutako ICMP datagrama bakoitza grabatuta gera dadin. Egikaritu lab6.

8. Saiatu orain M2tik M1era *ping* bat egiten, erantzunik jasotzen ez duzula ikusteko. Egiaztatu, ***cat /var/log/syslog | grep baztertu***ta egikarituz, datagrama baztertua izan dela iragazkiaren erruz.

9. Alda ezazu berriz M1en iragazki-aula (lab6 fitxategia egokitu eta berriz egikaritu), barrurantz datorren ICMP trafikoa baztertu dezan, baina beste aldea jakinaraziz.

10. Egin *ping* M2tik M1era, eta ikusi zein desberdintasun dagoen 8. atalean jasotako erantzunarekin.

### 3. ariketa: Suhesien konfigurazioa Linuxen

1. Ezabatu M1en iragazki taula eta lab6 fitxategia. Piztu EL eta *Network Manager*ra gaituta badago, desgaitu.

2. Konektatu M1 EL/eth0-rekin eta M2 EL/eth1-ekin bi *switch* erabiliz, eta hiru makinaren interfazeak ondoren azaltzen den moduan konfiguratu:



M1/eth0: 192.168.64.100/24

M2/eth0: 192.168.65.100/24

EL/eth0: 192.168.64.1/24

EL/eth1: 192.168.65.1/24

3. Hiru makinien birbidaltze-aulak berrikusi, eta, beharrezkoa denean, osatu. Kontuan izan oraingo honetan gehitu beharko duzula bideren bat M1 eta M2 birbidaltze-aulatan. ELn birbidaltzea gaitu. Horrekin, sareko hiru makinien IP konfigurazioa osatuta egongo da.
4. Pingak erabiliz egiaztatu beren artean konexioa dagoela. 30 ping bidali M2tik M1era eta idatzi erantzunen batzuek denbora.
5. M2tik `telnet` egin M1era. Eskaerak M1era heldu behar du, eta horrek baztertuko du (*connection refused* erantzun du), *telnet* zerbitzaria ez baitago abiatuta M1ean.
6. Bideratzailearen *netfilter*a konfiguratu honako arautegi honen arabera:
  - Baztertu bideratzaileari zuzendutako trafikoa guztia.
  - Bideratzaileak lotzen dituen sareen artean, ICMP trafikoa besterik ez utzi pasatzen.
7. Egiaztatu:
  - Ezinezkoa dela *ping* egitea erabiltzaile-makinetatik bideratzaileari.
  - *Telnet* egiten badugu M2tik M1era, eskaera ez dela heltzen, hau da, ez dugula jasoko *connection refused* mezua pantailan.
8. Egiaztatu posible dela *ping* egitea M1 eta M2ren artean. 30 *ping* bidali M2tik M1era (-c aukera) eta idatzi erantzunen batzuek denbora. Alderatu ariketa honen 2. atalean lortutako balioarekin eta ondorioak atera.
9. *Netfilter*a konfiguratzeke fitxategiaren bat sortu baduzu, **ezaba ezazu**.

## Suhesiak IOSen: atzipen-zerrendak (ACL)

Linuxen *iptables* komandoaren bidez egiten den iragazketaren kudeaketa, ACL (*Access Control Lists*) edo atzipen-zerrenden bidez egiten da IOSen<sup>42</sup>. Aurrerago landuko diren komandoak, gure praktikarako behar direnak soilik izango dira. ACLen erabilerari buruzko informazio zabalagoa lortzeko, informazioa bilatu daiteke Interneten.

ACL bat zenbaki batez identifikatuta dagoen arau multzo bat da. IOSen, zerrenden definizioa eta horien aplikazioa banatuta daude: lehenik eta behin, zerrenda definitzen da, eta ondoren zerrenda hori interfaze bati (edo gehiagori) lotzen zaio, interfaze horretatik sartzen (*in*) edo ateratzen (*out*) den trafikoa ezartzeko. Esleipen hori egin eta gero, interfaze horretatik azaldutako noranzkoan pasatzen diren datagrama guztiei aplikatzen zaizkie erazagututako arauak, horiek arauen batean definituta dagoen baldintza bete arte. Ez badu araurik betetzen, datagrama **baztertu egingo da**.

### Zerrenden definizioa

Zerrenda bat sortzeko, arauak banan-banan gehitu behar dira ***access-list*** komandoa erabiliz (konfigurazioa orokor moduan). Komandoaren sintaxia definitu behar den arauaren arabera alda daiteke, baina, oro har, honako eskema hau du:

***access-list*** *identifikadore\_zenbakia* [***permit***|***deny***] *baldintza*

---

42 Pakete-iragazkiaz gain, ACLeke beste erabilera batzuk dituzte.

Zerrenda identifikatzeko, ezin da edozein zenbaki aukeratu, zerrenda motaren arabera baita. Zein zenbaki-tarte erabil daitekeen zein zerrenda mota izendatzeko 1. taulan azaltzen da.

Guk, soilik IP zerrenda zabalduekin egingo dugu lan, erabilienak direlako. Horien sintaxia honako hau da:

**access-list** zerrenda\_zenbakia **{deny|permit}** protokoloa **{@Iturburu|P**  
Maskara\_inbertsoa | **host** @Iturburu|P | **any** **{@Helburu|P** Maskara\_inbertsoa  
| **host** @Helburu|P | **any** **{operadorea portua}**

PROTOKOLOA	MOTA	TARTEA	IRAGAZKIA
IP	Estandarra	1-99 eta 1300-1999	Iturburua
IP	Zabaldak	100-199 eta 2000-2699	Iturburua, helburua, protokoloa, portua...
Ethernet	Kodea (Type)	200-299	Ethernet kode mota
DECnet	Protocol Suite	300-399	Iturburua
Appletalk	Protocol Suite	600-699	Iturburua
Ethernet	Helbideak	700-799	MAC helbidea
IPX	Estandarra	800-899	Iturburua
IPX	Zabaldak	900-999	Iturburua, helburua, protokoloa, portua...
IPX	SAP	1000-1099	Aplikazio mota (SAP, Service Access Point)

**1. taula. Atzipen-zerrenden zenbakitzea (aukera gehiago badaude).**

## IP helbideak zehaztu atzipen-zerrendetan

Iturburu eta helburu helbideak zehazteko erabiltzen den sintaxia nahiko berezia da. Berez, beste komandoen antzera, lehenik, IP helbidea adierazten da, eta, ondoren, maskara. Bitxikeria, maskara zehazterakoan dator: bit esanguratsuek 0 balioa hartzen dute, eta ez-esanguratsuek, berriz, 1 balioa. Adibidez, 192.168.64.0/24 sareko datagramak identifikatzeko, honela idatziko genuke: 192.168.64.0 0.0.0.255

Maskara berezi hauei *wildcard mask*, *komodin-maskarak* edo *maskara-inbertsoak* deitzen zaie.

Badaude bereziak diren bi helbide, eta, oso erabiliak direnez, era erosoago batean idatzi daitezke (ikus 2. taula):

HELBIDEA	HELBIDE LABURTUA	ESANAHIA
XXX.XXX.XXX.XXX 255.255.255.255	any	Edozein helbide
XXX.XXX.XXX.XXX 0.0.0.0	Host XXX.XXX.XXX.XXX	Host partikular bat

**2. taula. Host eta any helbideak.**

Adibidea: zerrenda baten definizioa

Ondorengo komandoen bidez, zerrenda bat osatuko dugu, 192.168.64.0/24 saretik edo 192.168.50.1 helbidetik datozen ICMP pakete guztiak ukatzeko, baita sare horretatik (192.168.64.0/24) egindako edozein *telnet* (23 portua) atzipena ere:

```
CISCO# configure terminal
```

```
CISCO(config)# access-list 101 deny icmp 192.168.64.0 0.0.0.255 any
```

```
CISCO(config)# access-list 101 deny icmp host 192.168.50.1 any
```

```
CISCO(config)# access-list 101 deny tcp 192.168.64.0 0.0.0.255 any  
eq 23
```

```
CISCO(config)# access-list 101 permit ip any any
```

Zerrenda eta interfaze-esleipena

Horretarako, **ip access-group** komandoa erabiltzen da (interfaze-konfigurazio) moduan. Horren honako oinarritzko sintaxi hau honako da:

**ip access-group** *identifikadore\_zenbakia* *norabide\_aukera*

*norabide\_aukera* *in* edo *out* izan daiteke, zein noranzko datagramari ezarriko zaizkien zerrendako arauak aukeratzeko: interfazetik jasotako datagramak (*in*), edo interfazetik bidalitakoak (*out*). Beraz, arruntena, interfaze bati bi zerrenda esleitzea da: bat jasotako trafikorako, eta bestea bidaltzen den trafikorako.

Interfazearen eta zerrendaren arteko lotura kentzeko, esleipen-komandoa errepikatu behar da, aurretik *no* hitza jarritz:

**no ip access-group** *identifikadore\_zenbakia* *norabide\_aukera*

Ondoko adibidean, oraintxe definitutako zerrenda Fast1 interfazearekin lotuko dugu, hain zuzen ere, interfaze horretatik bidaltzen den trafikoarentzat:

```
CISCO(config)# interface Fast1
```

```
CISCO(config-if)# ip access-group 101 out
```

```
CISCO(config-if)# exit
```

Zerrenda bat definitu eta aplikatzerakoan, gogoan izan:

- Garrantzitsua da zein ordenatan definitzen diren zerrenda bateko arauak, ordena horri jarraituko baitzaio datagramei aplikatzeko. Eta datagrama batek arau batean definitutako baldintza betetzen duenean, arau horretan definitutako ekintza aplikatzen zaio (*permit* edo *deny*), eta **ez da konparaketa gehiagorik egingo** arauaren eta datagramaren artean.
- Oro har, zerrenda batean definitu behar duzu zein trafiko onartuko den. Beste guztia baztertu egingo da.
- Zerrenda baten edukia ikusteko:

```
CISCO# show ip access-lists Zerrendaren-zenbakia
```

- Definitutako zerrendak zein diren ikusteko:

```
CISCO# show access-lists
```

- Badago ACL baten konfigurazioa lantzea interfaze bat balitz bezala, eta, horrela, zerrenda batetik arauak kendu edo txertatu. Honako adibide honetan, arau bat txertatzen da 101 zerrendaren erdian:

**CISCO# configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

CISCO(config)# **ip access-list extended 101**

CISCO(config-ext-nacl) **18 permit tcp any host 172.162.2.11**

CISCO(config-ext-nacl)# **exit**

- Zerrenda batetik arauak kentzeko, nahikoa da *no* hitza jartzea, *access-list*, komandoaren hasieran, eta ezabatu nahi den araua zehaztu. Kontuz: arau-zenbakia ez bada zehazten, zerrenda osoa ezabatuko da.
- Zerrenda bat interfazeari bati baino gehiagori eslei dakioke, baina interfaze bati, noranzko bakoitzean, zerrenda bakarra eslei dakioke.
- Suhesi bat konfiguratzean, ez diozu bere interfaze guztiei eta noranzko guztietan ACLak esleitu behar. Askotan, nahikoa da soilik interfaze batzuk konfiguratzea, eta noranzkoren batean soilik. Adibidez, kanpotik datorren trafikoa soilik kontrolatu behar badugu, kanpoko interfazeko *'in'* noranzkoan soilik esleitu behar dugu ACL bat.
- Interfaze batek esleituta dauzkan ACLak ikusteko: **CISCO# show ip interface**  
*Interfazearen\_izena*

**4. ariketa: Suhesien konfigurazioa IOSen**

1. Zein eragin izango du ondoko araua azkena jartzeak ACL batean?  
*access-list zerr\_zenbakia deny any any*
2. Bi *switch*ak erabiliz, M1 EC/FastEth0rekin konektatu, eta M2 EC/FastEth1rekin; interfazeak ere konfiguratu:  
M1/eth1 y M2/eth1: zeuden bezala, ez dituzu ukitu behar.  
EC/FastEth0: 192.168.64.1/24  
EC/FastEth1: 192.168.65.1/24
3. Osatu behar al dituzu bideratzailearen birbidaltze-etaulak? Gaitu ezazun IP bideraketa. Egiaztatu *ping* baten bidez, makina guztiak atzigarri daudela, baita M1 eta M2ren arteko *telnet* eskaerak helden direla ere. Bidali 30 *ping* M2tik M1era eta jaso erantzunen batez besteko denbora. Konparatu 3. ariketan lortutakoarekin.
4. Konfiguratu trafiko-iragazketa bideratzailean honako segurtasun-arautegi honi jarraituz:
  - Baztertu bideratzailera zuzendutako edo bideratzaileak bidalitako ICMP trafiko guztia.
  - Bideratzaileak lotzen dituen bi sareen zehar, ICMP trafikoa soilik utzi pasatzen.
5. Egiaztatu ezin duzuela bideratzailera *ping* egin erabiltzaile makinetatik, ezta M1 eta M2 arteko *telnet* eskaerak helarazi ere.
6. Egiaztatu posible dela *ping* egitea M1 eta M2 makinaren artean. Bidali 30 *ping* M2tik M1era (-c aukera) eta gorde erantzunen batzuek besteko denbora. Konparatu ariketa honetako 3. atalean lortutakoarekin, eta 3. ariketan lortutakoarekin.

**SAIO-AMAIERA**

Zure konputagailuak itzali eta laborategitik atera baino lehen, mesedez, **honako hau** bete:

- Zure saioko apunteak eta fitxategiak eraman eta ezabatu laborategiko makinetan.
- Itzali makina guztiak.

- Egiaztatu 6 kableak gorde dituzula beren poltsan.