

## 4. laborategia: NAT/NAPT

Helburuak:

1. NAT/NAPT teknikak ezagutzea, baita bere konfigurazioa ere Linux eta CISCO makinetan.
2. Sare-ekipoen muntaia eta konfigurazioan trebatzea.
3. Sare-monitorizaziorako tresnen erabileran trebatzea.

Denbora: 2 o. 25'

Lan metodologia:

1. Ondo errepasatu nola konfiguratzten den IP-a linux eta IOS makinetan.
2. Dokumentazioa irakurri, eta bete galdeategia moodle-n.
3. Laborategian, ariketak egin, gidoian agertzen diren ahala, eta behar dituzun apunteak hartu.
4. Erabili dituzun makinak itzali eta utzi lanpostua aurkitu duzun bezala. Ahaztu gabe, fakultateko sare-kableak konektatu berri.

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

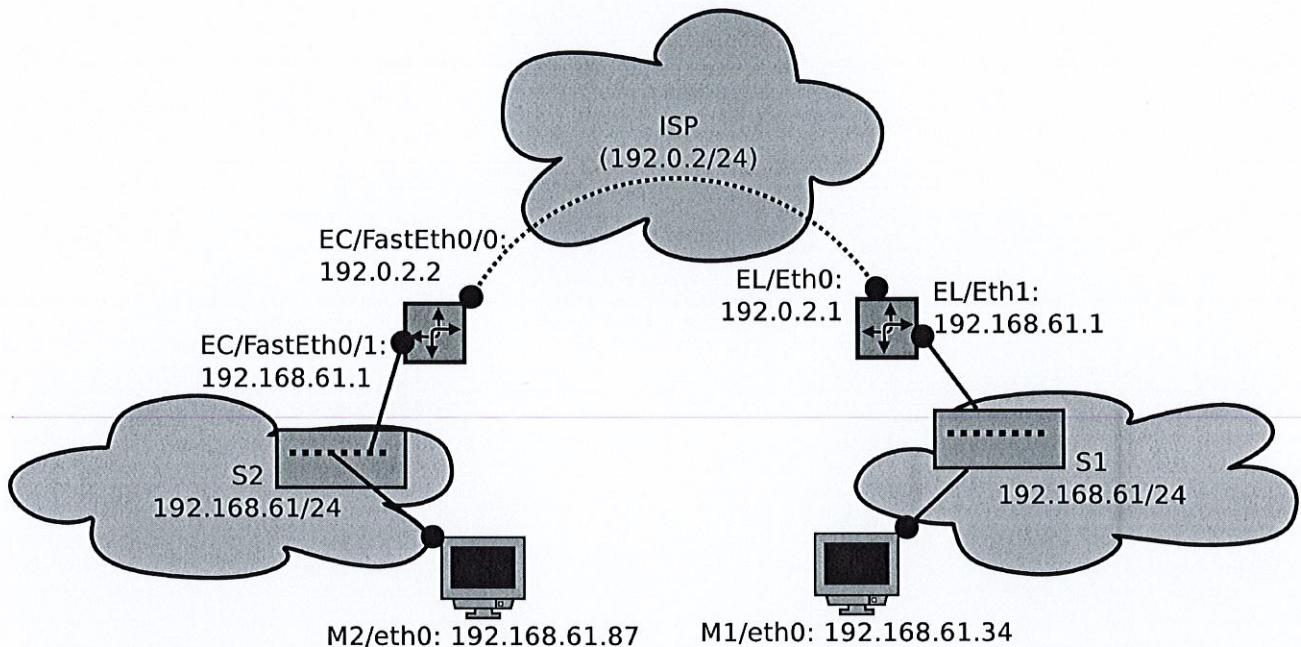
Gogoratu sare publikoko bideratzaileek ez dituzte IP helbide pribatuera zuzendurik dauden datagramak birbidaltzen. Honek suposatzen du RFC 1918 helbideak erabiltzen dituzten makinak Internetetik isolatuta daudela. Arazoa larria izan daiteke, kontuan hartuta dagoeneko ez da gelditzen IPv4 helbide publikorik 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 Internet-era doazen edo Internet-etik datozen datagrametan (normalean portuak ere ordezkatzen dira, horregatik zehatzagoa litzateke NAPT izendatzea). Normalean, Internetarekin 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 hau erabiliz ez dugu helbide publikorik aurrezten. Bigarren ariketan aztertuko dugu. NAT dinamikoa erabiliz, IP helbide publiko multzo bat kudeatzen da, eta hauek dinamikoki lotzen dira helbide pribatuekin. NAT dinamikoaren 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 sare eta makinak IP helbide esleipena desberdina izango dugu (ikusi 1. irudia). Aurreko laborategian bezala, **puntu-lerroak** kable gurutzatu baten erabilera adierazten du. Kable horrekin sare publiko bat simulatuko 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). Hau posible da 192.168.61.0/24 helbideratze-tartea RFC 1918-an helbide pribatu bezala definituta dagoelako. Ikusiko dugun bezala, NAT-ek ahalbidetzen du M1 eta M2 makinen arteko komunikazioa, makinen helbide pribatu horiek publikoekin ordezkatuz beren arteko komunikazioetan. EL-k eta EC-k NAT zerbitzariarenak egingo dute beraien sare pribatarentzat, lehenengoa zerbitzari dinamiko bezala eta bigarrena berriz zerbitzari estatiko gisa.

Hirugarren sareak ISP baten lana egingo du, eta suposatuko dugu S1 eta S2 sareek ISP horren bidez dutela beren Interneterako sarbidea (goranzko bidea). Errealitatean, EC eta EL konektatu beharko genituzke ISP horren sargune batera (edo PoP: *Point of Presence*), baina horretarako hirugarren biderataile bat beharko genuke mahai gainean. Beraz, zuzenean konektatuko ditugu bi makina horiek, eta gure experimentuetarako nahikoa izango da. Hori bai, ohartu EL-ren besterik ezeko bidea EC izango dela, eta kontrakoa: EC-ren irtenbidetzat EL hartuko dugu.

---

### 1. ariketa: sare fisikoaren ezarpena

1. Abiatu EL eta EC. EL-tik kontsola ireki EC-ekin, kermit erabiliz (ikusi 1. laborategia). Egiaztatu zein txartela den EL/eth0 eta zein den EL/eth1. Ez egin aurrera honetan seguru egon arte.
2. Bi switchak piztu, eta EL eta ECrekin konektatu 1 irudia jarraituz (kable gurutzatua).
3. **Interfazeak konfiguratu** EL eta EC-en, irudian dagoen bezala. Bi biderataileen **birbidaltze-taulak osatu**, bietan besterik ezeko bideak gehituz, bat bestearen irteera izan dadin. Hau da, EL-en bide lehenetsia EC izango da eta alderantziz (bata bestearen ISPa balitz bezala).
4. **Birbidaltza gaitu EL eta EC-n<sup>1</sup>**. Egin ping EC-tik EL/eth0-ra. Ez badabil, berrikusi egindakoa, **ping-a ibili arte**. Nahasten bazara, eta EL/Eth0-ri ordez, EL/Eth1-i egiten badiozu ping-a, zer gertatuko da? Errorea jasoko al duzu?

---

<sup>1</sup>Ikusi 2. laborategia



5. Egin ping EL-tik EC/FastEthernet0/0-ra. Ez badabil, berrikusi orain arte egindakoa, eta **ez egin aurrera ping hori ondo ibili arte**. Nahasten bazara, eta EC/FastEthernet0/0-ri ordez, EC/FastEthernet0/1-i egiten badiozu ping-a, zer gertatuko da? Errorea jasoko al duzu?
6. Piztu M1 eta M2, UPV-ko sareari lotuta izan gabe, **ehu erabiltzailea gisa sartu, eta network-managerra gelditu** bietan. Egiaztatu beraien birbidaltze-taulak hutsik daudela. Baten bat ez badago hutsik, ondokoa egikarituz hustu: `ip route flush table main`.
7. M1 eta M2-ren **interfazeak konfiguratu**, irudian azaltzen diren IP helbideak ezarriz. Bi makinaren **birbidaltze-taulak osatu**, beren sareetatik ateratzeko besterik ezeko bideak gehituz.
8. Egin ezazu ping M1-etik EL-ra (bi interfazeetara), eta M2-tik EC-ra (bi interfazeetara). Hauetariko ping-en batean errorea jasoz gero, aurreko pausuak berrikusi eta zuzenketak egin (**ez jarraitu ping hauek guztiak ondo jaso arte**).
9. Egin ping M1-etik EC/FastEthernet0/0-ra. Zergatik ez duzu erantzunik jaso? Bidali al du EC-k erantzuna? Ez badakizu zer erantzun, abiatu wireshark M2-n, konfiguratu bere *capture* iragazkia ICMP trafikoa harrapatzeko, eta errepikatu M1->EC/FastEthernet0/0 egindako pinga. Ikusten al duzu orain gertatutakoa?<sup>2</sup> Zer gertatuko da M2-tik EL/eth0-ra egiten badugu ping? Eta M2—>EL/Eth1 ping egiten badugu?

## NAT zerbitzari estatiko baten konfigurazioa IOS-en

IOS-ren hizkeran, sare pribatuari *inside* (barrukoa) deitzen zaio, eta publikoari *outside* (kanpokoa). CISCO bideratzalean itzulpen estatikoak konfiguratzeko ondoko bi pausuak betar behar dira:

1. Adierazi zein interfaze dauden konektaturik sare pribatura eta zeintzuk sare publikora. Horretarako, dagokion interfaze-konfigurazio lan moduan definitu interfazea pribatua ala publikoa den, eran honetan (**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 daitezten:

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

2. Gehitu sarrera bat NAT taulan, kanpora irtengo den helbide pribatu bakoitzeko. Horretarako, konfigurazio-globala moduan, idatzi beharko duzu, 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, ondoko komandoa erabili dezakezu:

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

---

<sup>2</sup> Benetako egoera batean, hau da, S1 eta S2 sareak benetako ISP bat 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 bideratzaleek ez baitute birbidaltzen helbide pribatu bat daraman datagramarik.



---

## 2. ariketa:NAT zerbitzariaren konfigurazioa eta abiatzea EC-en

---

1. Konfiguratu EC, NAT zerbitzari estatiko bezala, M2-ri 192.0.2.212 helbidea esleitzu. Egiaztatu NAT taularen edukia.
2. Wireshark exekutatu M2/eth0 eta EL/eth0 interfazeetan<sup>3</sup>, ping-ak sortutako trafikoa jasotzeko (definitu behar den iragazkia: **icmp[icmptype]==icmp-echo or icmp[icmptype]==icmp-echoreply**).
3. Bidali ping bat M2-tik EL/eth0-ra. Konparatu, bi makinetan wiresharkek atzemandako *ICMP echo request* datagramen iturburu helbideak. Berdina egin *echo reply* helburu helbidearekin.

## IP estaltzea Linux-en (*IP masquerading*)

Laborategiko hirugarren atal honetan ikusiko dugu nola lortu sare pribatu baten makina guztiak helbide publiko bakarra erabiltzea kanpoaldearekin komunikatzeko. Honi, *IP estaltzea*, PAT (*Port Address Translation*), edo NAPT (*Network Address and Port Translation*) deitzen zaio. Jakin ahal izateko nori helarazi kanpotik sare pribatura ailegatzen den trama bakoitza, portu esleipen bat egiten du NAT zerbitzariak. Hau da, barruko makina bakoitzari portu bat dagokio.

## Netfilter

Gure Linux sistemen kernel-a trafikoa atzemateko eta eraldatzeko *netfilter* softwarearekin dago egina. Datagrama bat netfilter-ri pasatzen zaionean, honek arau multzo bat arakatzen du, bilatuz zein araua egoki dakioko datagrama horri. Arauak bi zati ditu: baldintza (adibidez, datagrama portu zehatz batera bidalia izana), eta, datagramak baldintza betez gero, aplikatu behar zaion ekintza (adibidez, baztertua izatea). Arauak hiru multzotan daude antolatuta, taulak (ingelesetik *tables*) izenpean: iragazki-taula (*filter table*), itzulpen-taula (*nat table*), eta eraldaketa-taula (*mangle table*). Laborategi honetan itzulpen-taula landuko dugu, eta 6.ean iragazketena.

Taula bakoitzean, arauak kateetan multzokatzen dira (*chains*). NAT taulan ondoko bi kateak daude aurredefinituta:

- PREROUTING: datagrama jaso eta, birbidaltzeko taulan kontsultatu baino lehen, kateko arauak aplikatu. Hau DNAT moduan erabiltzen da (Destination NAT), datagramaren helburuko helbidea aldatzeko. Aldaera hau gure sare pribatuan zerbitzari bat dagoenean erabiltzen da. Ez da izango gure laborategiko kasua.
- POSTROUTING: datagrama jaso, eta birbidaltze taulan kontsultatu eta gero aplikatuko zaizkio kateko arauak. Hau SNAT moduan erabiltzen da (Source NAT), datagramaren iturburuko helbidea aldatzeko. Aldaera hau gure sare pribatuko bezeroak Internetera atera ahal izateko erabiltzen da. Hau ikusiko dugu laborategian.

## iptables

Netfilter konfiguratzeko eta kudeatzeko aplikazioa da. Honen erabilpena nahiko konplexua izan daiteke; horregatik, ohikoa da on-line eskuliburua erabili behar izatea, aukera bereziak edota xehetasunak kontsultatzeko. Bere sintaxia ondokoa da:

```
iptables [-t taularen_izena] komandoa kate_izena 1. parametroa 1. argumentua
N. parametroa N. argumentua
```

---

<sup>3</sup> Adi:Lubuntun instalatuta dagoen Wiresharken bertsioan iragazkiak interfaze bakoitzeko definitu behar dira, ez dago filtro bakarra 'Capture/options' leiohan.



-t parametroarekin zein taularekin lan egin behar duzu azaltzen da. filter da taula lehenetsiaren izena. Beste aukerak, gogoan izan, nat eta mangle dira. NAT taula maneiatzeko erabiltzen diren iptables dei guztiak 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). Parametroak eta argumentuak komandoaren arabera aldatzen dira.

NAT taularekin lotutako erabilpenaren adibide batzuk honako hauek dira:

- 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 Linux-en

1. EL-en NAT taula aldatu, M1-en sare-kide direnen helbide guztiak ordezkatzenko EL/eth0 interfazearen helbide publikoarekin.
2. Kontsultatu NAT taula, aurrekooa ondo egin duzula egiazatzeko.
3. Wireshark exekutatu M1 eta EL makinetan, telnet trafikoa harrapatzeko (*capture* iragazkia definitzeko: port 23)<sup>4</sup>.
4. Egin telnet EC/FastEth0-ra M1-etik (**telnet @helbidea**). EC-ek konexioa ukatuz erantzuten duenean, wireshark eten. Trama horiek aztertu, eta ikusi nola lotu diren portuak eta helbideak, ondoko taula betez. Jarri lerro bat M1-etik EC-era doan lehen datagramari (SYN datagrama) dagokion informazioarekin, eta beste bat EC-etik M1-era doan lehenengo datagramari (RST/ datagrama) dagokionarekin.

<b>192.0.2.0/24 sarea(EL-n atzemanda)</b>		<b>192.168.61.0/24 sarea (M1ean atzemanda)</b>	
Iturburu IP-a: portua	Helburu IP-a: portua	Iturburu IP-a : portua	Helburu IP-a: portua

5. Exekutatu Wireshark M1, M2, eta EL/eth0 konputagailuetan, ping trafikoa jasoz (iragazkia: 2.2 ariketarena).

<sup>4</sup> Adi:Lubuntun instalatuta dagoen Wiresharken bertsioan iragazkiak interfaze bakoitzeko definitu behar dira, ez dago filtro bakarra 'Capture/options' leiohan.



6. Bidali ping bat M1-etik M2-ra, eta eten Wireshark erantzuna jaso eta gero. Zein IP helbideari 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

7. Azaldutako NAPT teknika ikus dezakezu 3.3 ariketan. Baina ping kasuan, igorritako ICMP mezuk IP datagrametan zuzenean sartzen direnez, ez dira portuak erabiltzen. Hala ere, aurreko ariketan ikusi duzun bezala, EL-k lortu du egindako ping-ak eragindako erantzuna behar zaion makinari helaraztea. Aztertu wireshark-ek jasotako informazioa, ea ikusten duzun moduren bat EL-k jasotako *echo reply* mezua M1-erako dela asmatzeko.



## 5. laborategia: IPv6

### Helburuak:

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

### Lan metodologia:

1. Dokumentazioa irakurri, eta bete moodle-eko galdetegia. Ez segi aurrera galdetegiko galdera guztiak 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 egingo ditugunak honakoak dira:

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>1</sup>: interfaze bakoitziari 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 berakoak: helbide lokalak (fe80::/64 sorta). Horregatik, bertako unicast helbide bati ping6 egiten zaionean, adierazi behar da zein interfazetik nahi dugun bidalketa egitea.

---

<sup>1</sup> Konfigurazio automatikoa hau abiatzeko, kableak konektatuta egon behar du Linux sistemetan. CISCON, gaituta egon behar du v6-k interfaze horretan.



Konfigurazio globala ere automatikoa izaten da<sup>2</sup>, batez ere erabiltzaileen konputagailuetan. Bi era daude konfigurazio hau burutzeko: 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 zuzendutakoak.

## 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 burutzeko, helbide bikoitztua atzemateko ... Horretarako ondoko ICMPv6 mezuak erabiltzen ditu:

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

Hauetako mezuren bat atzemango dugu laborategian.

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

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

### Linuxen

*Router Advertisement* prozesuaren implementazioa Linuxen *radvd* programa da. Bere konfigurazioa */etc/radvd.conf* fitxategian gordetzen da. Fitxategi horretan adierazi behar den gutxienekoa iragarri behar den sareko aurrezenbakia da. Ondoko hau duzu horren konfigurazio minimoaren adibidea:

```
interface ethX
{
    AdvSendAdvert on;
    prefix @v6_sorta_global/aurrezenbakiaren_luzera
    {
    };
};
```

Adibide honetan, ethX da gure IPv6 sare lokalari lotuta dagoen bideratzailearen interfazea. Hortik iragarriko da definitutako aurrezenbakia. Aurrezenbaki hori gure ISP-k eman behar digu. Gure laborategiko bideratzaileen kasuan ez dago horrelako ISP-rik, 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 honi buruzko informazio gehiago behar izanez gero, man *radvd.conf* egin.

---

<sup>2</sup> Eskuz egitea ere badago, baina ez da ohikoa, batez ere host-eten.



## CISCON

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

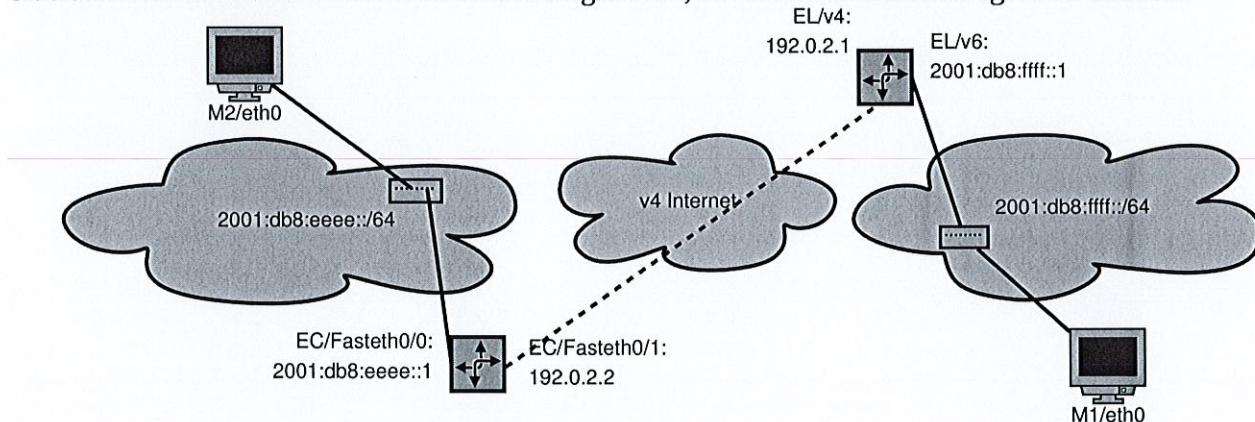
## Sare-topologia

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 baten erabilera adierazten du.

Irudian ikusten denez, laborategi honetan hiru sare ditugu:

- Bideratzaileak eta portatilak biltzen dituzten bi sareak. IPv6 sare hutsak dira.
- Bideratzaileak elkartzen dituen 'sarea'<sup>3</sup>. IPv4 sare bat da. Laborategi honetan Internet balitz har dezakegu sasi-sare hau.

Ohartu irudian ez direla adierazten portatilen interfazeen helbideak: **IPv6-n hainbat helbide izango dituzte interfazeek**, bertako eta globala gutxienez. Biak sortuko dira automatikoki, eta, beraz, ezin dugu inongo helbiderik esleitu portatilei irudian. Bideratzaileen kasua desberdina da: sare-helbidea eskuz esleitza ez da gutxitan egiten, 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 erabiliko ditugun tresnak honakoak dira<sup>4</sup>:

- Interfazeei IPv6 helbideak eskuz esleitzeko:

*ip* komandoa. Formatoa:

```
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 berria esleitu.

<sup>3</sup> Fisikoki ez dago sarea, baizik eta kable gurutzatua.

<sup>4</sup> Oharra: tresna hauei buruzko informazio gehiago behar izanez gero, erabili *man* komandoa.



- Interfazeen konfigurazioa ikusteko:  
`ifconfig` komandoa (urreko laborategietan bezala) edo `ip` komandoa. Formatoak, `ip` erabiilz:
 

```
ip -6 addr → interfaze guztien v6 konfigurazioa
      ip -6 addr sh dev int_izena → interfaze konkretu batena
```
- birbidaltze-taulekin lan egiteko: `ip` edo `route` komandoak. Formatoak:
 

```
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 bere erabilera.
- Konputagailuen arteko konektitatea egiaztatzeko: `ping6` programa. Betiko ping programaren funtzionamendu berbera du `ping6` programak, hau da, ICMPv6 echo request bidaltzen du eta ICMPv6 echo reply jasotzea espero du. Hala ere, bere erabilera desberdina da, bereiztu behar baita helbide globalei edo lokalei egiten zaien pinga. Helbide lokalei egiten zaienean, adierazi behar da zein interfazetik bidali behar den echo-request, interfaze guztiak daudelako helbideratze espazio berberean (espazio lokallean, alegia, fe80::/64). Ondokoak dira ping6 egiteko erabilera:
 

```
ping6 helbide_globala → helbide global bati egiteko.
      ping6 v6bertako_helbidea%int_izena → bertako helbide bati egiteko.
      ping6 -I int_izena v6bertako_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 berdinak dira, `ipv6` tartean kokatuta. Ariketetan ikusiko dugu bere erabilera.

---

### **1. ariketa: IPv6 konfigurazio lokala**

---

1. 2001:db8:ffff::/64 sarea eraikitzeko, piztu switchak, M1 eta EL/ethX<sup>5</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 EL-n. Baldin balego, ezabatu (`rm /etc/radvd.conf`).

---

<sup>5</sup> EthX izan behar du EL-ren oinarri plakan integratuta dagoen Ethernet interfazea, makina batzuetan eth0 eta beste batzuetan eth1 izango dena. Nahasten bazara, eta erantsitako sare txartelaren bidez konektatzer baduzu EL switcharekin, oinarri plakan dagoen interfazeak ez du dena. Autokonfigurazio lokala burutuko, eta ariketaren enuntziatuan aurreikusten diren gertaerak ez dira gertatuko.



3. EL-n desgaitu *privacy extensions* aukera: echo '0' > /proc/sys/net/ipv6/conf/all/use\_tempaddr).
  4. EL-ren bi interfazeak gaitu (`ifconfig int_izena up`).
  5. Aztertu EL-ren bi interfazeen v6 konfigurazioa<sup>6</sup>. Zein motakoak 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, **v6 interfazean soilik icmpv6** trafikoa atzemateko (*capture iragazkia: icmp6* ).
  8. Orain piztu M1, eta Network Managerra desgaitu makina horretan. Desgaitu interfaze birtualak M1ean (vmnet1 eta vmnet8), ez oztopatzeko. Desgaitu *privacy extensions* M1ean: `echo '0' > /proc/sys/net/ipv6/conf/eth0/use_tempaddr`.
  9. Wireshark-ek ICMPv6-ko *Neighbor Solicitation* erako mezu bat atzemanen duenean<sup>7</sup>, gelditu eta aztertu atzemandakoa. Aztertu portatilaren v6 interfazearen IPv6 konfigurazioa. Nork bidali du mezua? Zertarako, zure ustez?

Zer edo zergatik esperimetu hau errepikatu behar baduzu, ez ibili portatila berriz itzaltzen eta pizten: nahikoa duzu portatilaren interfazea desgaitu (down) eta berriz gaitu (up), harrapaketa abiatuta duzula.

  10. Egin `ping6` ELtik M1-era. 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 switchera, eta biak piztu.
  12. M2an egiteko: Desgaitu Network Managerra, eta interfaze birtualak (vmnet1 eta vmnet8), ez oztopatzeko, eta desgaitu *privacy extensions*.
  13. EL-n egiteko: Ireki kermit saio bat ELtik EC kontrolatzeko.
  14. EC-n: FastEthernet0/0 interfazean v6 gaitu:  

```
Cisco(config-if)# ipv6 enable
Cisco(config-if)# exit
```
  15. EC-n: IPv6 birbidaltzea ere gaitu:  

```
Cisco(config)# ipv6 unicast-routing
```
  16. EC-n: Aztertu interfazearen v6 konfigurazioa eta v6 birbidaltze-taula:  

```
Cisco# sh ipv6 interface
Cisco# sh ipv6 route
```
  17. Ping egin EC-tik M2-ra:  

```
Cisco# ping ipv6
```
- Eskatuko dizkizu ping-a burutzeko parametroak, helburuko IPv6 helbideaz hasita. **Ez jarraitu ping hau ondo ibili arte.**

---

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

---

<sup>6</sup> Interfazeren batek ez badu v6 konfiguraziorik, ziur aski nahastu zara eta ez duzu konektatu oinarri plakan dagoen sare txartela.

<sup>7</sup> Ez badu ezer harrapatzen, ziurtatu SOILIK v6 interfazean ari zarela harrapatzen. Hala eta guztiz ere ez badu ezer harrapatzen, desgaitu eth0 eta gaitu berriz.



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

```
ip -6 addr add helbide_globala dev ethX8
```

Eta errepikatu 1. ariketako 5. urrata.

2. Berriro aztertu EL-ren IPv6 birbidaltze taula. Zein bide berria agertu da?

3. M1-etik saiatzen bazara *ping6* egiten EL/v6-ri berriki esleitu diozun helbide globalari, zergatik ez duzu erantzuna jasoko? Laguntza: Ateratzen al da ICMPv6 echo request mezua portatilatik? Erantzuna ez badakizu, erabili wireshark v6 trafiko atzemateko eta aztertu ea bidaltzen den ala ez.

4. EL bideratzailean: /etc/radvd.conf fitxategia sortu<sup>9</sup> editore batekin (adibidez, *vi*, *nano*, *emacs* edo *pico*), eta behar den moduan konfiguratu radvd deabrua (ikusi 2. orrialdea).

5. Gaitu EL-n IPv6 bideratzaile-lana:

```
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

6. Abiatu wireshark EL/v6 interfazean, v6 interfazean IPv6 trafiko atzemateko iragazkiarekin.

7. Abiatu<sup>10</sup> radvd EL-n: *radvd start*.

8. Begiratu ea M1/eth0 interfazeak v6 helbide globala duen. Horrela denean, gelditu wireshark eta aztertu atzemandako trafikoa. Adierazi ezazu nola lortu duen portatilak helbide global hori.

9. Aztertu portatilaren v6 birbidaltze-taula. Zein bide berria agertu da? Nori dagokio bide horren hurrengo bideratzailearen helbidea? Azt ertu wiresharkek harrapututakoa, ea helbide horren arrastoa aurkitzen duzun.

10. Egin berriro 3. urratsetako *ping6* hori. Ez badabil, errepasatu egindakoa, ibili arte.

11. Begiratu portatilaren itzulpen taula. Zenbat IPv6 helbide daude esleituta EL/v6 interfazeari? Zergatik?

### CISCOren konfigurazioa

12. EC-n: 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-taula. Helbide globala esleituta, EC hasiko da irtenbidearena egiten, eta, beraz, *Router Advertisement* mezuk igortzen. Hori jasota, M2-k bere burua konfiguratuko du komunikazio globaletarako.

13. M2/eth0 interfazearen konfigurazioa aztertu, helbide globala hartu dela egiazatzeko, eta IPv6 birbidaltze-taula berrikusi, bide globala sartu dela ere egiazatzeko. Egin ping6 M2-tik EC-ko IPv6 helbide globalera, eta alderantzizkoa. Ez jarraitu bi ping hauek 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.

<sup>8</sup> Dagokiona idatzi: eth0, eth1, ...

<sup>9</sup> Gerta daiteke dagoeneko fitxategia sortua izatea; kasu horretan, egiaztatu bere edukia.

<sup>10</sup> Ezergatik gelditu behar baduzu, egin 'sudo killall radvd'.



## 3. EL-n: tunela sortu:

```
ip tunnel add tunel_izena mode sit remote bestea_IPv4 local gure_IPv4
```

Non:

*tunel\_izena*: nahi duzun izena, tunela identifikatzeko zure sisteman. Tunela interfaze birtual moduan kudeatuko du Ubuntuk.

*mode sit*: IPv6 datagramak IPv4 datagrametan sartuta ibiliko direla adierazteko.

*bestea\_IPv4*: Beste muturraren IPv4 helbidea, hau da, EC/FastEthernet0/1-ena.

*gure\_IPv4*: EL/v4-ren IPv4 helbidea.

Aztertu tunelaren konfigurazioa, *ifconfig* erabiliz.

## 4. EL-n: tunela gaitu:

```
ip link set dev tunel_izena up
```

5. EL-n IPv6 birbidaltze-taulan gehitu bide bat beste IPv6 **sarera** joateko tunelaren bidez:

```
ip -6 r add beste_sareko_IPv6 dev tunel_izena
```

## 6. EC-n, tunela sortu:

```
Cisco(config)# interface tunnel zenbaki Bat
```

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

```
Cisco(config-if)# ipv6 enable
```

Interface 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. EC-n, IPv6 birbidaltze-taulan gehitu bide bat beste v6 **sarera** joateko:

```
Cisco(config)# ipv6 route @v6_best_sarea Tunnel tunelaren_zenbakia
```

## 8. Egiaztatu tunela badabilela:

- Egin ping6 EL-tik EC/FastEthernet0/0-era, eta kontrakoa. Ez badabil, errepasatu egindako eta **ez jarraitu ondo ibili arte**.

- Egin ping6 EL-tik M2-ra, eta kontrakoa. Ez badabil, errepasatu egindako eta **ez jarraitu ondo ibili arte**.

- Egin ping6 M1-etik EC/FastEthernet0/0-era, eta kontrakoa. Ez badabil, errepasatu egindako eta **ez jarraitu ondo ibili arte**.



- Egin ping6 M1-etik M2-era, eta kontrakoa. Ez badabil, errepasatu egindako eta **ez jarraitu ondo ibili arte.**
9. Abiatu wireshark EL/v4 interfazean, iragazkirik gabe. Abiatu wireshark M2-n ere bai, eta egin *ping6* portatil batetik bestera. Aztertu eta alderatu tunelaren barruan eta kanpoan atzemandako ICMP mezuk.

### SAIO AMAIERA

Zure konputagailuak itzali eta laborategitik atera baino lehen, mesedez, ondokoa 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 bere poltsan.



## 6. laborategia: Suhesiak

### Helburuak:

1. Linux eta IOS-en oinarrizko suhesi-konfigurazioak egiten ikastea.
2. Interfazeen eta bideratze estatikoaren oinarrizko konfigurazioen errepasoa, Linux eta IOS-en.
3. Sare-ekipoen muntaia eta konfigurazioan trebatzea.

### Lan metodologia:

Laborategira joan baino lehen:

1. Dokumentazioa irakurri eta 1. ariketa egin.
2. Moodle-eko galdeategia bete.

Laborategian bertan:

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

### Bibliografia

Linux-eko suhesiak:

<https://help.ubuntu.com/community/IptablesHowTo>

man iptables

IOS-eko ACL-ei buruz:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfacls.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html)

<http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>

### Suhesiak Linux-en

4. laborategian *netfilter* softwarea eta bere *iptables*<sup>1</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).

Iragazki-taula (**filter taula, alegia**) hiru kateetan dago antolaturik: gure makinarantz zuzendurik datozen datagramei aplikatzen zaiena (INPUT katea), gure makinak sortzen dituen datagramei aplikatzen zaiena (OUTPUT katea), eta makina bideratzaile bezala lan egiteko konfiguratuta dagoenean, birbidalitako

<sup>1</sup> Bertsio zaharra, ipchains, oraindik erabilgarri dago sistema askotan.



datagramei aplikatzen zaiena (FORWARD katea). Datagrama bakoitza, dagokion kateko araukin alderatzen da, banan banan. Datagramak arau baten baldintza betetzen badu, hauetako bat gertatuko da:

- Arau horren ekintzak datagramaren prozesamenduaren bukaera suposatzea. Hori da ACCEPT eta DROP ekintzen kasua, besteak beste.
- Arau horren ekintzak datagramaren prozesamenduaren bukaera ez izatea. Horrela izanik, adierazitako ekintza bete eta gero, kateko hurrengo araukin alderatuz jarraituko du datagramaren prozesamenduak. Hori da LOG ekintzaren kasua, hurrengo ekintzan gertatukoa grabatu nahi denean erabilia. Kasu horretarako baldintza bera duten bi arau jarraian sartzen dira taulan: lehena. LOG ekintza duena, gertatukoa erregistratzeko jartzen da, eta bigarrena, ACCEPT 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>2</sup> (bitakora, alegia), eta bigarrenak trafiko bera atzematen du, eta baztertzen du.

Datagma kateko bukaeraraino ailegatzen bada, kate horren besterik ezeko ekintza egikarituko da. Besterik ezeko ekintza hori -P komandoarekin (policy) definitu daiteke, baina definituta ez badago, ACCEPT egikarituko da.

---

### **1. ariketa: iptables-en erabilera**

---

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

1. Konsultatu (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
```

2. Zein da ondoko bi ekintzen arteko aldea?

```
iptables -A OUTPUT -j DROP
```

```
iptables -A OUTPUT -j REJECT
```

3. Zein eragina du ondoko araua azkena jartzea bere katean?

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

---

<sup>2</sup> Log mezuak, sistemaren log-en konfigurazioan adierazten den lekuaren gordeko dira. Gure makinak, log mezuak /var/log/syslog fitxategian gordetzen daude konfiguraturik.



---

### 2. ariketa: gotorleku baten konfigurazioa Linuxen

1. Piztu M1 eta M2 makinak, UPVko sareari lotu gabe, eta Network Managerra desgaitu. Sortu lab6 izeneko fitxategi bat M1ean, eta hor idatzi M1 makinako netfilter-a hurrengo arautegia 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 da. 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 egiazatzeko.
4. Konektatu bi erabiltzaile makinak kommutagailu bat erabiliz, eta konfiguratu beraien interfazeak 192.168.64.100/24 (M1) eta 192.168.64.200/24 (M2) IP helbideekin.
5. Aztertu M1 eta M2 birbidaltze taulak, eta ez badira egokiak (interfazeak ondo konfiguratu badituzu, zuzenak izan beharko litzateke), egokitu. Kontuan izan sare lokal isolatua egin dugunez, taulan ez dugula *default* biderik behar.
6. Egiaztatu ping bat 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 M2-tik M1-era ping bat egiten, erantzunik jasotzen ez duzula ikusteko. Egiaztatu, `cat /var/log/syslog | grep baztertuta` egikarituz, datagrama baztertua izan dela iragazkiaren erruz.
9. Aldatu ezazu berriz M1-en iragazki-taula (lab6 fitxategia egokitu eta berriz egikaritu), barrurantz datorren ICMP trafikoa baztertu dezan, baina beste aldea jankin araziz.
10. Egin ping bat M2-tik M1-era, eta ikusi zein desberdintasun dagoen 8. atalean jasotako erantzunarekin.

---

### 3. ariketa: Suksesien konfigurazioa Linux-en

1. **Ezabatu M1-en iragazki taula eta lab6 fitxategia.** Piztu EL eta Network Managerra 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 makinaren birbidaltze-taulak berrikusi, eta, beharrezkoan denean, osatu. Kontuan izan oraingo honetan bai gehitu beharko duzula bideren bat M1 eta M2 birbidaltze-tauletan. EL-n birbidaltzea gaitu. Horrekin sareko hiru makinaren IP konfigurazioa osatuta egongo da.



4. Ping-ak erabiliz egiaztatu beraien artean konexioa dagoela. 30 ping bidali M2-tik M1-era eta idatzi erantzunen bataz besteko denbora. *33/892ms*
5. M2tik telnet egin M1era. Eskaerak M1era heldu behar du, eta honek baztertuko du (*connection refused* erantzungo du), telnet zerbitzaria ez baitako abiatuta M1ean.
6. Bideratzailearen netfilter-a konfiguratu hurrengo arautegiaren arabera:
  - Baztertu bideratzaileari zuzendutako trafiko guztia.
  - Bideratzaileak lotzen dituen sareen artean, ICMP trafikoa esterik ez utzi pasatzen.
7. Egiaztatu
  - Ezinezkoa dela ping egitea erabiltzaile makinatik bideratzailera.
  - Telnet egiten badugu M2tik M1era, eskaera ez dela heltzen, hau da, ez dugu jasoko *connection refused* mezua pantailan.
8. Egiaztatu posible dela ping egitea M1 eta M2-ren artean. 30 ping bidali M2-tik M1-era (-c aukera) eta idatzi erantzunen bataz besteko denbora. Alderatu ariketa honen 2. atalean lortutako balioarekin eta ondorioak atera. *33/779*
9. Netfilterra konfiguratzeko fitxategiren bat sortu baduzu, **ezabatu ezazu**.

## Suhesiak IOS-en: atzipen-zerrendak (ACL)

Linux-en iptables komandoaren bidez egiten den iragazketaren kudeaketa, ACL (Access Control Lists) edo atzipen-zerrenden bidez egiten da IOS-en<sup>3</sup>. Aurrerago landuko diren komandoak, gure praktikarako behar direnak soilik izango dira. ACL-en erabilpenari buruzko informazio zabalagoa lortzeko, informazioa bilatu daiteke Internet-en:

ACL bat zenbaki batez identifikatuta dagoen arau multzo bat da. IOS-en, zerrenden definizioa eta hauen aplikazioa banatuta daude: lehenik eta behin, zerrenda definitzen da, eta ondoren zerrenda hori interfaze bat (edo gehiagorri) lotzen zaio, interfaze horretarik sartzen den (in) edo ateratzen (out) trafikoari ezartzeko. Esleipen hori egin eta gero, interfaze horretatik aaldutako noranzkoan pasatzen diren datagrama guztiei aplikatzen zaie erazagututako arauak, hauek arauen batean definituta dagoen baldintza bete arte. Ez badu araurik betetzen, datagrama **baztertua izango da**.

### Zerrenden definizioa

Zerrenda bat sortzeko, arauak banan-banan gehitu behar dira access-list komandoa erabiliz (konfigurazioa-orokorra moduan). Komandoaren sintaxia, definitu behar den arauaren arabera alda daiteke, baina orokorrean ondoko eskema dauka:

```
access-list identifikadore_zenbakia {permit|deny} baldintza
```

Zerrenda identifikatzeko ezin da edozein zenbaki aukeratu, eta zenbaki-multzo hori kudeatzen ari garen arau-motarekin dago erlazionatuta. 1 taulan, hauetariko batzuk kontsultatu ditzakezu, eta baita taulan agertzen diren zerrenda-moten ezaugarri orokorrak.

Guk, soilik IP zerrenda zabalduekin egingo dugu lan, erabilienak direlako. Hauen sintaxia honakoa da:

```
access-list zerrenda_zenbakia {deny|permit} protokoloa {@IturburuIP  
Maskara_inbertsoa | host @IturburuIP | any} {@HelburuIP  
Maskara_inbertsoa | host @HelburuIP | any} {operadorea portua}
```

<sup>3</sup>Pakete-iragazkiaz gain, ACL-ak beste erabilpen batzuk dituzte.



PROTOKOLOA	MOTA	TARTEA	IRAGAZKIA
IP	Estandarra	1-99 eta 1300-1999	Iturburua
IP	Zabalduak	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	Zabalduak	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, horrela idatziko genuke: 192.168.64.0 0.0.0.255

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

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

HELBIDEA	HELBIDE LABURTUA	ESANAHIA
XXX.XXX.XXX.XXX 255.255.255.255	any	Datagrama guztiak
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, eta baita sare horretatik 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

Honetarako, ip access-group komandoa erabiltzen da (interfaze-konfigurazio) moduan. Honen oinarritzko sintaxia ondokoa da:



`ip access-group identifikadore_zenbakia norabide_aukera`

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

Interfaze eta zerrendaren arteko lotura kentzeko, esleipen komandoa errepikatu behar da, aurretik *no* hitza jarri:

`no ip access-group identifikadore_zenbakia norabide_aukera`

Ondoko adibidean, oraintxe definitutako zerrenda, Fast1 interfazearekin lotuko dugu, hain zuzen ere, interfaze honetatik 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 ordenetan definitzen diren zerrenda bateko arauak, hori izango baita datagramei aplikatzeko jarraituko den ordena. Eta datagma batek, arau batean definitutako baldintza betetzen duenean, arau horretan definitutako ekintza aplikatzen zaio (*permit* edo *deny*), eta **ez da konparaketa gehiagorik egingo** arau eta datagramaren artean.
- Orokorean, zerrenda batean definitu behar duzu zein trafikoa onartuko den. Beste guzta, baztertua izango da.
- Ezin dira zerrendaren erdian arauak txertatu `access-list` komandoa erabiliz, amaieran gehitzea besterik ez dago. Beraz, zerrenda osatzen duten arauak sartzerakoan nahastu egiten bagara, zerrenda ezabatu eta berriz hasi beharko dugu. Bestela, badago ACL baten konfigurazioa lantzea interfaze bat balitz bezala. Ondoko adibidean arau bat txertatzen da 101 zerrendaren erdian:

```
internetrouter#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
internetrouter(config)#ip access-list extended 101
internetrouter(config-ext-nacl)#18 permit tcp any host 172.162.2.11
internetrouter(config-ext-nacl)#^Z
```

- Zerrenda batetik arauak kentzeko, nahikoa da *no* hitza jartzea, `access-list`, komandoaren hasieran, eta ezabatu nahi den araua zehaztu. Kontuz: ez bada arau zenbakia zehazten, zerrenda osoa ezabatuko da. Arau baten zenbakia jakiteko, aztertu behar duzu zerrendaren edukia sh komandoarekin. Adibidez:

```
internetrouter#show access-lists
Extended IP access list 101
10 permit tcp any any
15 permit tcp any host 172.162.2.9
20 permit udp host 172.16.1.21 any
30 permit udp host 172.16.1.22 any
```

- Zerrenda bat interfazi bat baino gehiagori esleitu daki, baina interfazi bat, noranzko bakotzean, zerrenda bakarra esleitu daki.
- Suhesi bat konfiguratzean, ez diozu bere interfaze guztiei eta noranzko guztietan ACL-ak esleitu behar. Askotan, nahikoa da soilik interfaze batzuk konfiguratzea, eta soilik noranzkoren batean. Adibidez, soilik kanpotik datorren trafikoa kontrolatu behar badugu, soilik kanpoko interfazeko 'in' noranzkoan esleitu behar dugu ACL bat.



- Interfaze batek esleituta dituen ACLak ikusteko: `cisco# show ip interface Interfazearen_izena`

#### **4. ariketa: Suhesien konfigurazioa IOS-en**

1. Zein eragina izango du ondoko araua azkena jartzea ACL batean?  
access-list zerr\_zenbakia deny any any *Deagle desberdintako litzelak azkena  
ondoriaz ez du izango oregainik*
2. M1 EC/FastEth0-rekin konektatu, eta M2 EC/FastEth1-ekin bi switch-ak erabiliz; interfazeak ere konfiguratu:

M1/eth1 y M2/eth1: zeuden bezala, ez dituzu ikutu behar.

EC/FastEth0: 192.168.64.1/24

EC/FastEth1: 192.168.65.1/24

3. Behar bezala konfiguratu bideratzailearen birbidaltze-taulak, eta IP bideraketa gaitu. Egiaztatu ping baten bidez, makina guztiak atzigarri daudela, baita M1 eta M2ren arteko telnet eskaerak heltzen direla. Bidali 30 ping M2-tik M1-era eta jaso erantzunen batez besteko denbora. Konparatu 3. ariketan lortutakoarekin.

4. Konfiguratu trafiko-iragazketa bideratzailean ondoko segurtasun-arautegia jarraituz:

- Baztertu bideratzailera zuzendutako, edo bideratzaileak bidalitako ICMP trafiko guztsia.
- Bideratzaileak lotzen dituen bi sareen zehar, ICMP trafikoa soilik utzi pasatzen.

5. Egiaztatu ezin duzuela bideratzailera ping-ik egin erabiltzaile makinatik, ezta M1 eta M2 arteko telnet eskaerak helarazi ere.

6. Egiaztatu posible dela ping bat egitea M1 eta M2 makinaren artean. Bidali 30 ping M2-tik M1-era (-c aukera) eta gorde erantzunen bataz besteko denbora. Konparatu ariketa honetako 3. atalean lortutakoarekin, eta 3. ariketan lortutakoarekin. *0.458 ms*

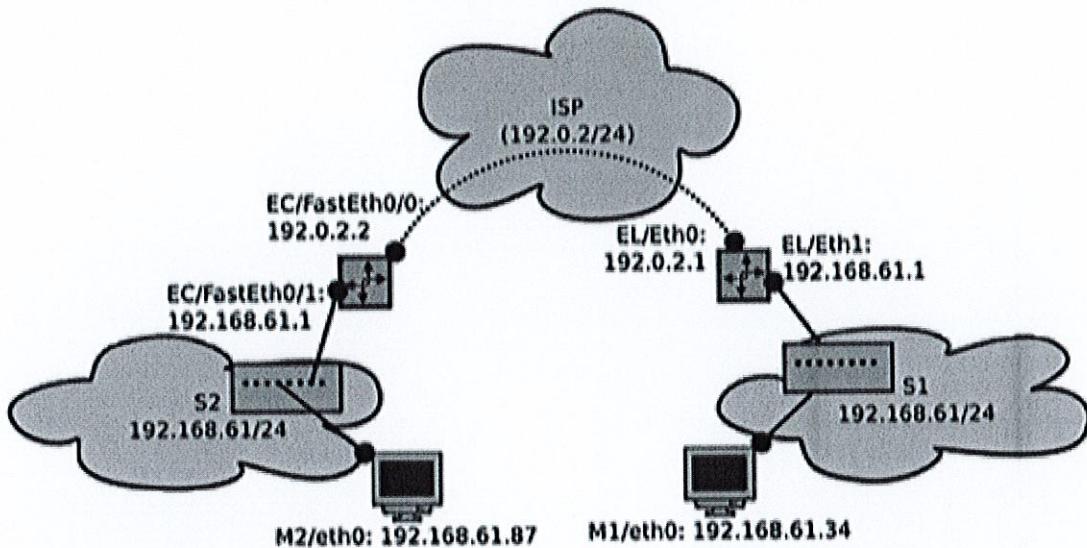
### **SAIO AMAIERA**

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

- Zure saioko apunteak eta fitxategiak eraman eta ezabatu laborategiko makinetan.
- Itzali makina guztiak.
- Egiaztatu 6 kableak gorde dituzula bere poltsan.



## 4. Laborategia



### 1. Ariketa

EC konfiguratzan:

```
Kermit. set line /dev/ttyS0. set carrier-watch off . connect  
{root,enable}. configure terminal. interface FastEthernet0/1. ip address  
192.168.61.1 255.255.255.0. no shutdown. no ip domain-lookup. line console 0 .  
no exec-timeout
```

EL konfigurazioa:

```
Ifconfig. ifconfig eth0 up. ifconfig eth1 up. ifconfig eth0  
192.0.2.1 up. ifconfig eth1 192.168.61.1 up.
```

Birbidaltze-taulak:

EC:

```
>configure terminal  
>ip route 192.0.2.2 255.255.255.0 192.0.2.1  
>ip routing
```

EL:

```
>route add default gw 192.0.2.1  
> echo 1 > /proc/sys/net/ipv4/ip_forward
```

M1 konfigurazioa:

```
Sudo service network-manager stop  
>ifconfig
```



```
>ifconfig eth0 up  
>ifconfig eth0 192.168.61.87 up
```

#### M2 konfigurazioa:

```
Sudo service network-manager stop
```

```
>ifconfig
```

```
>ifconfig eth0 up
```

```
>ifconfig eth0 192.168.61.34 up
```

#### Birbidaltze-taulak:

**M1 eta M2:**

Hustu birbidaltze taulak. **Ip route flush table main.**

```
>route add default gw 192.168.61.1
```

### 2. Ariketa

EC konfiguratu nahi da NAT zerbitzari estatiko bezala, M2ri 192.0.2.12 helbidea esleitzuz. **Interface FastEthernet0/1. Ip nat inside. Exit. Interface FastEthernet0/0. Ip nat outside. Exit. Configure terminal. Ip nat inside source static 192.168.61.87 192.0.2.212.** Wireshark exekutatuko da. **Sudo -b wireshark.** Ondorengo iragazkia jarriz. **Icmp[icmptype]==icmp-echo or icmp[icmptype]==icmp-echo reply.** Azkenik, ping bat bidaliko da M2tik EL/eth0ra. **Ping -c 1 192.0.2.1.** Eta wireshark-ek atzematen dituen icmp echo request datagramen iturburu helbideak konparatu.

### 3. Ariketa

M1-en sarekide diren helbide guztaik EL/eth0 interfazearen helbide publikoarekin aldatu. **Iptables -t nat -A POSTROUTING -j SNAT -t 192.168.61.1 -s 192.168.61.0/24.** Nat taula konsultatu. **Iptables -t nat -L.** Telnet trafikoa harrapatzeko exekutatu wireshark, capture iragazkia definitzeko port 23 ezarri. **Sudo -b wireshark.** Orain telnet egingo da. **telnet 192.0.2.2.**

M1, M2 eta ELn exekutatuko da wireshark ping trafikoa jasotzeko.



## 5.Laborategia

IPv6 sare baten konfigurazioa bi zatitan bereizten da: konfigurazio lokala eta konfigurazio globala. Konfigurazio lokala guztiz automatikoa izaten da, helbide fisikotik abiatuta esleitzen badio sistemak makinari IPv6 helbidea. Sistemak, konexio zuzenak ere sartzen ditu, interfaze bakoitzeko bat. Horregatik, ping6 erabiltzen da bidalketak egiteko. Nahiz eta konfigurazio globala ere automatikoa izan, bi era daude konfigurazio hau burutzeko: IPv6 sarea munduarekin lotzen duen bideratzaileak zuzenduta (stateless autoconfiguration) edo DHCPv6 zerbitzari bat erabilita (statefull autoconfiguration).

### Irtenbideak zuzendutako autokonfigurazio globala (stateless)

Sareko komputagailuek, bere interfazeak autokonfiguratzenten dituzte jasotako aurrezenbakia eta interfazearen helbide fisikotik abiatuta.

#### Linuxen

Radvd programa erabiltzen da, /etc/radvd.conf fitxategian gordetzen da honen konfigurazioa.

```
Interface ethX
{
    AdvSendAdvert on;
    Prefix @v6_sorta_globala/aurrezenbakiaren_luzera
    {
    };
}
```

#### CISCON

Bideratzailearen IPv6 birbidaltzea gaitzen dugunean, automatikoki hasiko da Router Advertisement mezuk zabaltzen bere sarean.

#### Linux Komandoak

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

Komando hau erabiltzen da interf\_izena interfazeari IPv6 helbidea bat esleitzeko. Esleitutako helbide bat aldatu nahi bada, lehenengo ezabatu 'del' eta ondoren berriz gehitu 'add' beharko da.

**Ifconfig edo ip:** komandoak erabiltzen dira konfigurazioa ikusteko.

**Ip -6 addr:** Erablitzen interfaze guztien v6 konfigurazioa ikusiko da.

**Ip -6 addr sh dev int\_izena:** Interfaze konkretu baten v6 konfigurazioa erakutsiko du.



**Ip edo route:** Komandoak erabiltzen dira birbidaltze-taulekin lan egiteko.

**Ip -6 r:** birbidaltze taula erakutsiko du.

**Ip -6 r sh dev int\_izena:** interfaze konkretu baten birbidaltze taula erakutsiko du.

**Ip -6 r flush dev int\_izena:** Interfaze konkretu bati dagozkion bideak ezabatzeko erabiltzen da komando hau.

**Ip -6 r add IPv6\_helburua dev int-izena:** Birbidaltze taulan bide bat sartzeko balio du.

**Ip -6 neigh sh:** itzulpen taula edo neighbour table erakusteko erabiltzen da.

**Ping6:** Konputagailuen arteko konektibitatea egiaztatzeko.

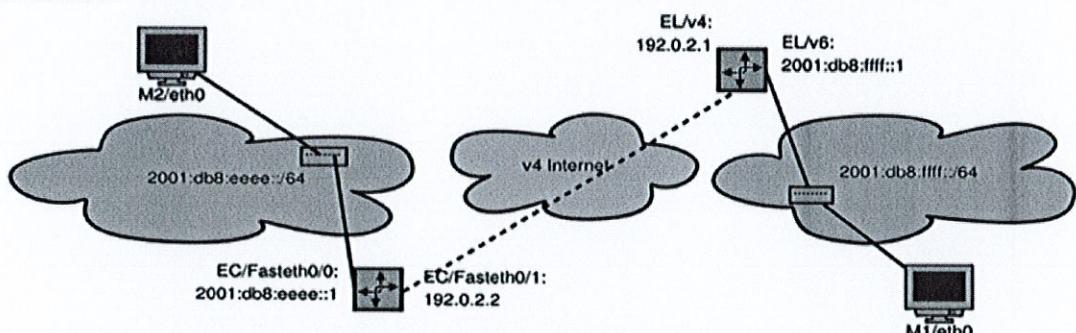
**Ping6 helbide\_globala:** Helbide global bati egiten zaio ping.

**Ping6 v6bertako\_helbidea%int\_izena:** Bertako helbide bati ping egiteko erabiltzen da.

**Ping6 -I int\_izena v6 berako\_helbidea:** aurrekoaren gauza bera egiten du.

## CISCO

IPv4n erabiltzen diren komando berdinak erabiltzen dira, ipv6 tartean kokatuta.



1 irudia: laborategiko sare-topologia.

### 1. Ariketa

2001:db8:ffff::/64 sarea eraikitzen, EL/eth0n.

Egiaztatu, /etc/radvd.conf ez dela existitzen. `rm /etc/radvd.conf`

Desgaitu privacy extensions aukera: `echo '0' > /proc/sys/net/ipv6/conf/all/use_tempaddr`

Bi interfazeak gaitu: `ifconfig eth0 up` eta `ifconfig eth1 up`



Aztertu EL-ren bi interfazeen v6 konfigurazioak. ***ifconfig***. v6 helbideak helbide fisikotik lortu dira.

Birbidaltze taula aztertu. ***Ip -6 r***.

```
fe80::/64 dev eth0 proto kernel metric 256
```

```
fe80::/64 dev eth1 proto kernel metric 256
```

Bi bide horiek agertu dira, ifconfig up egin dugunean.

Wireshark abiatuko dugu. ***Sudo -b wireshark***. Capture eta icmp6 iragazkia ezarri.

M1 piztuko da, eta Network Managerra desgaitu. ***Sudo service network-manager stop***. Interfaze birtualak desgaitu. ***Ifconfig vmnet8 down*** eta ***ifconfig vmnet1 down***. Privacy extension desgaitu. ***Echo '0' > /proc/sys/net/ipv6/conf/eth0/use\_tempaddr***.

ELtik M1-ra ping6 bidali, zein erabili behar da? Kasu honetan, helbide globalak ez daude oraindik definituta, ondorioz, ondorengo komandoa erabiliko da. ***Ping6 fe80::223:54ff:fe78:bd69%eth0***.

M2 makina pitzu eta M1 ekin egin den bezala desgaitu Network managerra eta interfaze birtualak eta privacy extension. ***Sudo service network-manager stop***. ***Ifconfig vmnet8 down*** eta ***ifconfig vmnet1 down***. ***Echo '0' > /proc/sys/net/ipv6/conf/eth0/use\_tempaddr***.

Kermit zaioa ireki ELn. ***Kermit. Set line /dev/ttyS0. Carrier-watch off. Connect.***

EC-n FastEthernet0/0 interfazean v6 gaitu. ***Configure terminal.***

***Interface FastEthernet 0/0. Ipv6 enable. Exit.***

Ipv6 birbidaltza ere gaitu. ***Ipv6 unicast-routing. Exit.***

Aztertu interfazearen v6 konfigurazioa eta v6 birbidaltze-taula: ***sh ipv6 interface. Sh ipv6 route.***

Ping egingo da EC-tik M2-ra. ***Ping ipv6.***

## 2. Ariketa

EL/v6 ri esleituko diogu irudian agertzen den ipv6 helbide globala. ***Ip -6 addr add 2001:db8:ffff::1 dev eth0.***

***Ifconfig eth0.*** Oraingoan, helbide globala agertuko da.

***Ip -6 r.*** Egiten badugu berriro bide berri bat gehitu dela ikusiko da.

```
2001:db8:ffff::/64 dev eth0 proto kernel metric 256
```

EL-n /etc/radvd.conf fitategia sortuko dugu. ***nano /etc/radvd.conf***, eta konfiguratuko dugu eth0.



```
Interface eth0
{
    AdvSendAdvert on;
    Prefix 2001:db8:ffff::1/64
    {
    };
}
```

IPv6 bideratzale-lana gaitu.

**echo 1 > /proc/sys/net/ipv6/conf/all/forwarding**

Wireshark abiatuko dugu eta v6 interfazean ipv6 trafikoa atzemateko iragazkia jarriko da.

Ondoren, abitau radvd. **Radvd start.**

Ping egingo da M1etik EL-ra, helbide globala erabiliz.

**Ping6 2001:db8:ffff::1.**

### **CISCOren konfigurazioa**

FastEthernet0/0ri esleituko diogu ipv6 helbide globala.

**Configure terminal**

**Interface FastEthernet0/0**

**Ipv6 address 2001:db8:eeee::1 Exit**

Aztertu interfazearen v6 konfigurazioa eta v6 birbidaltze-taula: **sh ipv6 interface. Sh ipv6 route.**

**Ping 6 2001:db8:eee:0:223:54ff.fe3d:5b24**

### **3. Ariketa**

EL/v4 eta EC/FastEthernet0/1 interfazeak konfiguratu irudian bezala.

EL/v4: **ifconfig eth1 192.0.2.1 up**

EC/FastEthernet0/1: **configure terminal. Interface FastEthernet0/1.**

**Ip address 192.0.2.2 255.255.255.0**

**No shutdown. Exit. Ip routing.**

Ping egingo dugu EL-tik EC-ra eta alderantziz.

EL-tik **Ping -c 1 192.0.2.2** eta EC-tik **ping 192.0.2.1.**

EL-n tunela sortuko dugu:

**Ip tunnel add 13 mode sit remote 192.0.2.1 local 192.0.2.2.**

Eta tunela gaituko da:

**Ip link set dev 13 up**

Orain IPv6 birbidaltze-taulan bide bat gehituko da beste IPv6 sarerako.



***Ip -6 r add 2001:db8:eeee::1 dev 13***

Ondoren, ECKo konfigurazioa gauzatuko da, tunela sortu

***Interface tunnel 13. Ipv6 enable. Tunnel source 192.0.2.1.***

***tunnel destination 192.0.2.1. tunnel mode ipv6ip. Exit.***

IPv6 birbidaltze-taulan v6rako bide bat gehitu.

***Ipv6 route 2001:db8:ffff:/64 Tunnel 13***

***Ip routing.***

Ping6 bidaliko zaio lehenik eta behin, EL tik ECKo helbide globalari.

***ping6 2001:db8:eeee::1***

Ping6 EL-tik M2ko helbide globalera.

***ping6 2001:db8:eeee:0:223:54ff:fe3d:5b24***

Ping6 M1-tik M2-ra.

***ping6 2001:db8:eeee:0:223:54ff:fe3d:5b24***

## 6.Laborategia

### 1. Ariketa

***iptables*** komandoa IP paketeen filtraketen arauak konfiguratzeko erabiltzen da Linux kernel-en. Komando honek hainbat erabilera ditu:

- ***Iptables -F:*** iragazki taula osoa ezabatzen du.
- ***Iptables -L:*** iragazki taula osoa pantailaratzen du.
- ***Iptables -A OUTPUT -p icmp -j ACCEPT:*** komando kate honen bidez, zehaztuko da, lehenik eta behin, ze motatako eragiketak egiten ari garen, -A OUTPUT-aren bidez kanpo eragiketa dela zehazten da, -p icmp-k icmp protokoloa erabiliko dela ezarriko du, eta -j ACCEPT-aren bidez, paketeak onartuko ditu eta prozesatzeari utziko dio kate honetan.
- ***iptables -D INPUT 2:*** INPUT 2 iragazkia ezabatuko da.
- ***iptables -A INPUT -j LOG --log-prefix "Iragazkia INPUT:"***: kanpoko kateei buruzko paketeek jasango du aldaketa soilik. --log-prefix-aren bidez Loggin egiterakoan mezu hau agertuko zaio log mezuaren aurretik.
- ***iptables -I INPUT 3 -j DROP:*** iragazki bat ezarriko da. INPUT katean sartuko da iragazkia, eta 3. Izango da kasu honetan. Eta -j DROP-aren bidez, paketeak baztertzea eskatuko zaio eta kate honetan normak prozesatzeari utziko dio.



- ***iptables -A FORWARD -p icmp -j ACCEPT:*** Aurretik ikusi dugun komandoaren oso antzekoa da baina kasu honetan, eragiketak FORWARD motako paketeen gainean izango dira.
- ***iptables -A FORWARD -d 158.227.112.1 -p tcp -dport 23 -j ACCEPT:*** -d 158.227.112.1 erabilita, paketeen helburua zehazten da eta, -dport 23-aren bidez, Helburuko portua zehazten da, kasu honetan 23 portua izango da. Besteak, paketeen iragazkien ezaugarriak eta erabiliko diren protokoloak zehazten dute.
- ***iptables -A FORWARD -s 158.227.112.0/24 -j DROP:*** -s aukera erabiltzen da, jatorrizko helbidea zehazteko, kasu honetan, 158.227.112.0/24 sarea izango da. -j DROP-aren bidez, atzeko planoan paketeak ez ditu onartuko eta normak prozesatzeari utziko dio.
- ***iptables -A FORWARD -p icmp -j ACCEPT --icmp-type echo-request:*** echo-requesta bat egingo du.

Hainbat eragiketa desberdin ikusi ditugu dagoeneko. DROP eta REJECT haien artean. Kasu honetan, biek ez dituzte onartzen paketeak, baina REJECT-en kasuan, hau egin duela adierazi egingo dio erabiltzaileari, ordea DROP-ek atzeko planoan egingo du eta erabiltzaileak ez du honen berri izango.

Definituta ez badago, besterik ezeko ekintzarik –P komandoarekin, ez du izango eraginik ondoko arau hau azkena jartzerik, bestela bai, eta paketeak onartuko lituzke.

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

#### 4. Ariketa

M1 eta M2 makinak piztu. **Sudo service network-manager stop.** Sortu lab6 fitxategi bat M1en. Eta bertan M1 makinako netfilter-a hurrengo arautegia betetzeko behar diren komandoekin. **nano lab6. Chmod +x lab6.** Exekutatzeko ahalmena emateko.

lab6 fitxategiak honako hau izango du barruan.

```
Iptables -F
Iptables -A INPUT -p icmp -j ACCEPT.
Iptables -A OUTPUT -p icmp -j ACCEPT.
Iptables -A INPUT -j LOG
Iptables -A INPUT -j DROP
Iptables -A OUTPUT -j LOG
Iptables -A OUTPUT -j DROP
```



Fitxategia exekutatu. **Sudo ./lab6. Iptables -L.** Taula erakusteko.

**M1 konfigurazioa**

```
Ifconfig eth0 up  
Ifconfig eth0 192.168.64.100/24 up
```

**M2 konfigurazioa**

```
Ifconfig eth0 up  
Ifconfig eth0 192.168.64.200/24 up
```

Konfigurazioa aztertzeko birbidaltze taulak begiratu. **Netstat-rn.** Eta makina batetik bestera ping egingo da. **Ping -c 1 192.168.64.200.** Barrurantz datorren icmp trafikoa baztertzen aldatu. **Nano lab6.**

```
Iptables -F  
Iptables -A INPUT -p icmp -j LOG --log-prefix "baztertuta"  
Iptables -A INPUT -p icmp -j DROP.  
Iptables -A OUTPUT -p icmp -j ACCEPT.  
Iptables -A INPUT -j LOG  
Iptables -A INPUT -j DROP  
Iptables -A OUTPUT -j LOG  
Iptables -A OUTPUT -j DROP
```

Berriz egikarituko da lab6. **Sudo ./lab6. Ping -c 1 192.168.64.100.** Ez da erantzunik jaso, egiaztatuko da, **cat /var/log/syslog | grep baztertuta,** egikarituz.

```
May 3 15:38:05 U002613 kernel: [ 1730.941444] baztertuta[N=eth0  
OUT= MAC=00:23:54:78:bd:69:00:23:54:3d:5b:24:08:00  
SRC=192.168.64.200 DST=192.168.64.100 LEN=84 TOS=0x00  
PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=2195  
SEQ=1
```

Barrurantz datorren icmp trafikoa baztertu, baina beste aldeari jakinaraziz. **Nano lab6.**

```
Iptables -F  
Iptables -A INPUT -p icmp -j LOG --log-prefix "baztertuta"  
Iptables -A INPUT -p icmp -j REJECT.  
Iptables -A OUTPUT -p icmp -j ACCEPT.  
Iptables -A INPUT -j LOG  
Iptables -A INPUT -j DROP  
Iptables -A OUTPUT -j LOG
```



Iptables -A OUTPUT -j DROP

Ping -c 1 192.168.64.100.

## 5. Ariketa

M1 iragazkia ezabatu. **Rm lab6. Iptables -F.** EL piztu eta Network managerra desgaitu. **Sudo service network-manager stop.** Konfiguratu M1, M2 eta EL-ren interfazeak. **M1 -> ifconfig eth0 192.168.64.100/24 up. M2-> ifconfig eth0 192.168.65.100/24. EL -> ifconfig eth0 192.168.64.1/24 eta ifconfig eth0 192.168.65.1/24. M2 ->route add -net 192.168.64.0/24 gw 192.168.65.1. M1 -> route add -net 192.168.65.0/24 gw 192.168.64.1.** 30 ping bidali M2tik M1era. **ping -c 30 192.168.64.100.** **telnet 192.168.64.100.** Ez du funtzionatuko ez baitago tenet zerbitzaria abiatuta M1en. **Netfilter-a konfiguratu EL-n. Nano lab6.**

Iptables -F

Iptables -A INPUT -j DROP

Iptables -A OUTPUT -p icmp -j ACCEPT

Iptables -A OUTPUT -j DROP

**Chmod +x lab6. ./lab6.** Ping egiten saiatzen bagara ez dira helduko.

**Ping -c 1 192.168.65.1.** EZ da helduko. **telnet 192.168.64.100.** Ez da connection refused mezua pantailan jasoko.

30 ping bidali M2tik M1era. **ping -c 192.168.64.100. rm lab6. Iptables -F.**

## 6. Ariketa

Access-list zerr\_zenbakia deny any any ezartzeak ez du izango eraginik, azkenean berdin ere ez duelako onartuko. Hau jarri edo ez.

### Konfiguratu EC:

Configure terminal. Interface FastEthernet0/0. Ip address

**192.168.64.1 255.255.255.0 . Exit. Interface FastEthernet0/1. Ip address**

**192.168.65.1 255.255.255.0. ip routing.**

Ongi dabilela ikusteko ping-a bidaliko da M2tik M1era. **ping -c 30 192.168.64.100.**



**Access-list 101 deny icmp any 192.168.65.1 0.0.0.255  
Access-list 101 permit icmp any any**

**Interface FastEthernet0/1. Ip access-group 101 in**

**Access-list 102 deny icmp 192.168.65.1 0.0.0.255 any  
Access-list 102 permit icmp any any**

**Interface FastEthernet0/1 Ip access-group 102 out**

**Access-list 103 deny icmp any 192.168.64.1 0.0.0.255  
Access-list 103 permit icmp any any**

**Interface FastEthernet0/0 Ip access-group 103 in**

**Access-list 104 deny icmp 192.168.64.1 0.0.0.255 any  
Access-list 104 permit icmp any any**

**Interface FastEthernet0/0 Ip access-group 104 out**

Egiaztatuko da ezin dela ping egin M1 eta M2tik bideratzailera. **Ping -c 192.168.65.1 eta ping -c 192.168.64.1.**

Baina posible dela M1 eta M2 artean ping egitea. **Ping -c 30 192.168.64.100**



# KSO Laborategiak

## 1.Laborategia

### LINUX komandoak:

**ifconfig** Sare-txartelak konfiguratzeko erabiltzen den komandoa da. Komando honen bidez, IP helbideak ezarri, maskara zehaztu, edota interfazea aktibatu edo desaktibatu daiteke.

**ifconfig interfazearen\_izena helbidea/aurrezenbakiaren\_luzera up** komando honen bidez makinaren sare-interfazea birkonfiguratu daiteke, nahi den IP helbideak esleitzu.

**ifconfig interfazearen\_izena helbidea/aurrezenbakiaren\_luzera down** makinaren sare-interfazeko helbide hori desgaitzko erabiltzen da komando hau.

**ip** Sare konfiguraziorako erabiltzen diren tresna batzuen ordezkoa da ip programa. Hasiera batean, *ifconfig*, *router*, eta beste batzuen erabilera baztertzeko agertu zen, baina oraindik ez da lortu hori.

**ping** Sare-administrazioan gehien erabiltzen den tresnetakoa da. Makina bat sare-bidez atzigarri dagoen edo ez jakiteko erabiltzen da. Honen funtzionamendua ICMPn dago oinarritua. ICMP echo request mezu bat bidaltzen da atzigarri dagoen edo ez jakin nahi dugun makinara, eta ICMP echo response mezua heldu arte itxarongo da. Edo denbora agortu arte.

**arp** Komando hau ARP taula atzitu eta kudeatzeko erabiltzen da. Taula hau cache bat da non helbide fisiko eta IP helbideak gordetzen diren Ethernet sareetan. Sarreren iraungitze-epea 2 minutukoa da.

**Wireshark** Protokolo-analizatzailea edo sniffer bat da. Sare-interfazeek jasotzen duten trafikoa gorde eta pantailaratzen du, erabilizaleak erazagututako trafikoa atzemateko iragazkien arabera. Terminaletik Wireshark exekutatzeko, **sudo -b wireshark** idatzi behar da eta lehio bat zabaltzen da, non sare-interfazeek jasotako trafikoa agetuko den.

**sudo service network-manager** internetera konektatzeko erabiltzen den gailua konektatzeko (**restart**) edo gelditzeko (**stop**) erabiltzen da komandoa.



## **CISCO komandoak:**

***kermet*** komando hau erabiliz CISCO bideratzailearen konfigurazioan aldatekat egiteko programa bistaratzen da. Honen barruan hainbat komando ezberdin erabiliko dira konfigurazia burutzeko.

***set line /dev/ttys0*** komando hau erabiliko da erabiliko den serie portua zehazteko

***set carrier-watch off*** linea telefonikoa erabiliko ez denez eramailearen detekzioa desgaituko da.

***connect*** bideratzailearekin konexioa irekitzeko erabiltzen da komando hau. Ondoren, *return* sakatu behar da, eta username eta pasahitza sartu. Eta CISCO# barruan sartzen da.

CISCO# modu pribilegiatuan sartu ondoren, sareak konfiguratzeko ondorengo komandoak erabiltzen dira.

***configure terminal*** komando hau erabili eskero, makina osoari dagozkion konfigurazioak egiten dira.

***interface <Portuaren izena>*** komandoa erabiltzen bada, Portu horri dagokion sarearen konfigurazio guztia egin daiteke.

***ip address <ip\_helbidea maskara\_formatu\_dezimalean>*** erabiliko da IP helbide bat esleitzeko aurretik sartutako portuari

***no shutdown*** komandoak interfazea gaitzeko balio du.

***no ip domain-lookup*** komando honen bidez komando bat gaizki tekleatu eskero, sistema ez blokeatzea ahalbidetuko du.

***line console 0*** erabiliz berriz ere prompt-a aldatuko da.

***no exec-timeout*** erabiltzen da denboragailua desgaitzeko, horrela denbora gehiegi egon eskero ezer egin gabe ez ixteko kontua.

***sh ip interface brief*** exekutatuz bideratzaileko interfazeen-konfigurazioa ikusten da.



## **Ariketak:**

### **1.Ariketa**

***1.- Zure makineko interfazeen zerrenda eta haien konfigurazioa ikusteko, egin ifconfig (baliokidea: ip add sh). Zenbat interfaze agertu dira? Zeintzuk dira haien izenak?***

Guztira 4 interfaze agertu dira ***ifconfig*** komandoa erabili ondoren: *eth0*, *Vmnet1*, *Vmnet8* eta *Lo*. *Vmnet1* eta *Vmnet8* sare birtualak dira. *Lo* konputagailu lokala eta *eth0* sarerako interfaze lokala da.

***2.- Gure laborategietan eth0 izena duena besterik ez zaigu interesatuko. EHuko sarera lotzen zaituen interfazearen konfigurazioa aztertu (ifconfig eth0 edo, bestela, ip add sh eth0), eta honako galdera hauek erantzun:***

*eth0*-k esleituta duen IPv4: 158.227.133.175 da. Helbide horri dagokion IP maskara: 255.255.255.240.0 da. Eta sare-difusioa: 158.227.143.255 da.

Datu-eremuan gehienez, 1500 byte onartuko dituzte.

Guztira 7856 trama igorri dira eta horietatik batek ere ez du izan errorerik, eta ondorioz ez da egon talkarik.

Jasotako tramen batezbesteko tamaina 35600 byteko da.

### **2.Ariketa**

***1.- Zenbat oihartzun (echo) eskaera geratu dira erantzunik gabe? Bidalketa guztien zein ehunekoa da hori? Zenbatekoa da igarotako denborarik laburrena eskaera igorri eta erantzuna jaso arte? Eta luzeena? Bataz besteko? Bataz besteko aldea?***

0 izan dira erantzun gabe geratu diren eskaerak, ondorioz, bidalketa guztien %0 da erantzunik jaso ez duen ehunekoa.

Eskaera denbora minimoa: 0.152 ms.

Eskaera denbora maximoa: 0.231 ms.

Batezbesteko eskaera denbora: 0.190 ms.

Eskaera denboren batezbesteko aldea: 0.032 ms.



**2.- Zein da erantzunen TTL balioa? Egin orain ping berdina 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.**

TTLaren balioa 64 da. **ping -c 5 10.30.13.6** egin ondoren TTL = 60 da, ondorioz, 4 bideratzaile pasatu dira.

### 3. Ariketa

**1.- Ireki terminal-leiho bat M1 makinan. Konsultatu ezazu arp taula, terminal horretan 'arp -n' komandoa exekutatuz. Ba al dago sarrerarik taulan? Sarreraren bat balego, arp komandoaren -d aukera erabili taula husteko. Oharra: -d aukeraren erabilera konsultatu eskuliburuan (man arp).**

Bai, hainbat sarrera daude.

**2.- Exekutatu orain wireshark lehenengo terminalean, ARP edo ICMP edukia duten tramak atzemateko konfiguratu (capture/options lehioan arp or icmp filtroa ezarri), eta abiatu ('start' botoia sakatu). Bigarren leihoan berriz, ping bat exekutatu ondoko makinara, trama bakarra bidaliz (-c aukera). Wireshark-ek trafikorik jasotzen ez duenean (segundo batzuk), gelditu eskuratzea. Ordoren, arp taula berriz konsultatu. Zer sarrera daude orain? wireshark-ek eskaintzen duen informazioa aztertu, ondorengo galderak erantzuteko: Aukeratu eta aztertu ARP edukia daraman trametako bat: zein protokolo erabiltzen da TCP/IP arkitekturaren maila bakoitzean? Zein maila arte ailegatu zara? Hartu orain ICMP trama bat eta galdera berdinei erantzun. Erantzun al du ondoko makinak ping komandoari? Nola daki makinak horrek zein IP helbideari itzuli behar zion ICMP echo reply paketea? Nola lortu du ondoko makinak gure makinaren helbide fisikoa? Zertarako behar zuen gure helbide fisikoa?**

Direkzioa 00:23:54:3d:5b:f7



## 4.Ariketa

**1.- Ikusi bideratzailean interfaze-konfigurazioa, sh ip interface brief exekutatuz. Zenbat interfaze ditu bideratzaileak? Zein izen erabiltzen dira? Zeintzuk daude aktibatuta (up) eta zeintzuk ez? Orain egin sh interfaces eta erantzun ondorengo galderak, aktibatuta dauden interfazeei buruzkoak: Zein IP helbideak dituzte esleituta? Zein formatutan ematen dira IP helbideen maskarak? Ikusi ematen diren helbide fisikoen formatua, zer desberdintasuna dago Linux-en arp komandoak erabiltzen duen formatuarekin?**

3 interfaze ditu FastEtherneteak:

## 2.Laborategia

### LINUX Komandoak:

**nestat -rn** birbidaltze taula erakusten du komando honek.

**route** birbidaltze taulak konfiguratzeko erabiltzen da komando hau, ondorengo luzapenak erabiliz. **ip** komandoa erabiliz ere gauza berak lortu daitezke.

**route add -net <Helburuko\_ip\_sorta> gw <hurrengo\_bideratzailearen\_@IP>**  
**edo ip route add -net <Helburuko\_ip\_sorta> via <hurrengo\_bideratzailearen\_@IP>** Birbidaltze taulen bide berriak sartu behar badug, komando hau erabiltzen da.

**route add default gw <irtenbidearen\_@IP> edo ip route add default via <irtenbidearen\_@IP>** Komando honen bidez, besterik ezeko bide sartzeko berezia egin daiteke.

**route del -net <Helburuko\_ip\_sorta> edo ip route del -net <Hleburuko\_ip\_sorta>** Dagoeneko bide bat ezabatu nahi bada, komando hori erabiltzen da.

Birbidaltze ahalmena gaitzeko **ip\_forward** fitxategian 1 balioa idatziz egiten da, horretarako bi modu daude.

**echo 1 > /proc/sys/net/ipv4/ip\_forward** Hau da zuzenean



fitxategian idaztea.

***sysctl -w net.ipv4.ip\_forward=1*** Kernelen parametroak aldatzeko komando hau erabiltzea.

### **CISCO Komandoak:**

***sh ip route*** Modu pribilegiatuko sh komandoa erabili behar da birbidaltze taula ikusi nahi bada.

***clear ip route \**** Komando hau erabili eskero taula osoa ezabatuko da.

***ip route <aurrezenbakia> <maskara><Hurrengo\_bideratzailearen\_@IP>*** sartuz birbidaltze taulan bide berriak sartzea lortuko da, baina horretarako konfigurazio orokorreko lan moduan sartu behar da.

***no ip route <aurrezenbakia> <maskara>*** Komandoaren bidez taulan dagoen bide bat ezabatuko da.

***ip routing*** birbidaltze gaitasuna abiatzeko erabiltzen den komandoa da, lan modu pribilegiatuan.

### **Ariketak:**

#### **1.Ariketa**

1.- Taulak utzik daude.

***2.- EL-ren interfazeetako bati 192.168.64.1 helbidea esleitu, eta M2 konektatu duzun kommutagailu berari lotu interfaze hori (adi zein den EL makinaren eth0 eta zein eth1!!), kable normal bat erabiliz (ez gurutzatua!!).***

Guk sartutako bidea agertu da birbidaltze taulan, hau da, 192.168.65.0 sare multzora bidali nahi bada informazioa, 192.168.64.1 interfazea erabili behar da. Eta gauza bera egingo da beste makinarekin, 192.168.64.0 sare multzora bidali nahi bada, 192.168.65.1 interfazea erabiliko da.

3.- Ez litzateke aldatuko birbidaltze taulak, E/Xra konektatuta dauden makinak 192.168.64/24 azpisarean egongo lirateke eta E/Yra konektatuta dauden makinak 192.168.65/24 azpisarean.



4.- Ez. default gateway-ak sartu beharko lirateke edozein IP direkzio bateratu ahai izateko. Ondorioz, default gw horretan esan beharko genuke internetera bidali nahi diren mesuak hirugarren interfaze horretatik joan beharko direla.

## 2.Ariketa

- Idatzi paper batean sarean dauden lau interfazeen helbide fisikoak (#M1/eth0, #M2/eth0, #EL/eth0, #EL/eth1).***

MAQUINA / INTERFAZ	IP	MAC
E1/Eth0	192.168.64.1/24	00:0c:f1:bc:0e:4e
E1/Eth1	192.168.65.1/24	00:c0:df:e4:fe:2c
M1/Eth0	192.168.65.100/24	00:23:54:78:bd:69
M2/Eth0	192.168.64.100/24	00:23:54:3d:5b:24
ARP		

## 3.Ariketa



### 3.Laborategia

***dhcpd -f -cf /etc/dhcp/labo3.conf*** komandoaren bidez, emandako direktoriotik programaren konfigurazioa kargatuko da, non oinarrizko konfigurazio bat egin den.

```
##### 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 {}
```

***dhclient -d <interfazearen\_izena>*** Honela beste terminal batetik DHCP bezeroa abiatuko da nahi den interfazetik.

***ip helper-address <DHCP\_zerbitzariaren\_helbidea>*** komandoa erabiliz, DHCP eskaerak jasoko dituen interfazea reiay bezaia konfiguratuko da. Eta konfiguratu ze helbidetara bidali behar diren eskaera horiek.



### **3.Ariketa**

5.-

Erabilitako aplikazioa: bootstrap protocol, ondorioz DHCP protokoloa erabiltzen da.

Garraio maila: UDP erabiltzen da.

Sarea: IP.

Lotura: Ethernet.

### **Esoleipena**

Discover, Offer, Request, ACK egin dira hurrenez urren.

M1 interfazeari 192.168.61.1 IP helbidea esleitu zaio.

Aurretik erabili den komandoari esker gertatzen da hori, hau da,  
***dhclient -d <interfazeare\_izena>*** ezarri dugulako.



## 1. laborategia: Sarrera

Helburuak:

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

Estimazioa: 2 o. 25'

Lan metodologia:

1. Dokumentazioa irakurri, eta bete galdetegia moodle-n epe barruan.
2. Ariketak egin, gidoian agertzen diren 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 ondorengo ekipamendua aurkituko duzu:

#### 1. Erabiltzailearen makinak (2)

Eramangarriak dira. Kontu handiz ibili behar duzu honen konfigurazio fisiko eta logikoa zegoen bezala utziz.

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

erabiltzailea: **ehu**

pasahitza: **rlinux**

Egingo ditugun laborategietan, eskuineko konputagailua M1 deituko dugu, eta M2 ezkerrekooa.

#### 2. Linux bideratzailea

Mahaiaren erdian dugun PCa da. Honek Lubuntu dauka, eta gure ariketetan bideratzaile bezala erabiliko dugu (honetarako, bi sare-txartel ditu).

erabiltzailea: **root**

pasahitza: **rlinux**

Ondorengo laborategietan egingo ditugun ariketa era sare-eskemetan makina honek **EL** izena izango du.

### 3. CISCO bideratzailea

Linux bideratzailearen azpian, CISCO 2811 bideratzaile bat dago<sup>1</sup>. Bere kontrola EL makinatik egingo dugu, kermit urruneko programa erabiliz. Erabiltzailea: **root**. Pasahitzak: **enable**.

Hemendik aurrera bideratzaile honen izena **EC** izango da.

### 4. Kommutagailuak (switch-ak)

Maiha bakoitzean bi CISCO kommutagailu dituzu.

### 5. Kableak

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

## LINUX lan-inguruko tresna eta komando arrunt batzuk

Sare-konfigurazioa ezartzeko, testu-moduko komandoak erabil daitezke (terminala erabiliz idazten ditugunak, eta parametroak ezagutzeko **man** komandoa erabili 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 ahaltsuagoa).

### Ifconfig programa

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

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

---

#### 1. ariketa: ifconfig-en erabilera arrunta

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

- a) Ireki LibreOffice fitxategi bat.
- b) Pantailan, galderak erantzuteko **interesgarria den emaitza bat** lortzen duzun bakoitzean, kopiazu LibreOffice-n.
- c) Makina itzali aurretik LibreOffice fitxategiaren kopia bat eraman zurekin.

Ariketa hau taldekkide bakoitzak egin behar du bere aldetik, M1 makinan batek eta M2 makinan besteak.

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

1. Zure makinako interfazeen zerrenda eta haien konfigurazioa ikusteko, egin **ifconfig** (baliokidea: **ip add sh**). Zenbat interfaze agertu dira? Zeintzuk dira haien izenak?
2. Gure laborategietan **eth0**<sup>2</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 hauek erantzun:

---

<sup>1</sup> Bi mailetan dagoena CISCO 1700 eredua da. Gure laborategietarako, baliokideak dira.

<sup>2</sup> Konputagailuaren txartel kopuru eta konfigurazioaren arabera eth-ren ondoren dagoen zenbakia desberdina izan daiteke

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, beraien datu-eremuan? Zenbat trama jaso/igorri dira? Zenbat jasotze/igortze errore eman dira? Zenbat talka? Zein da jasotako/igortitako tramen batez besteko tamaina?

### *ip* programa

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

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

### Ping

Sare-administrazioan gehien erabiltzen den tresnetakoa da. Makina bat sare-bidez atzigarri dagoen edo ez jakiteko erabiltzen da. Ping oso programa simplea da, eta bere funtzionamendua ICMP protokoloan oinarritzen du: bidali ICMP echo request mezu bat atzigarria dagoen jakin nahi dugun makinara, eta itxaron honek erantzun arte ICMP echo response mezuarekin.

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

---

### 2. ariketa: *ping-en erabilera arrunta*

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

1. Zenbat oihartzun (echo) eskaera geratu dira erantzunik gabe? Bidalketa guztien zein ehunekoa da hori? Zenbatekoa da igarotako denborarik laburrena eskaera igorri eta erantzuna jaso arte? Eta luzeena? Bataz besteko? Bataz besteko aldea?
2. Zein da erantzunen TTL balioa? Egin orain ping berdina 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 hau, ARP taula atzitu eta kudeatzeko erabiltzen da. Gogoan izan, taula hau cache bat dela, non helbide fisiko eta IP helbideak gordetzen diren Ethernet sareetan. Bere izena, taula osatzeko eta mantentzeko erabiltzen den protokolotik hartzen du. Cache bat denez, taula behin-behineko da: sarrerak iraungitzen dira erabiltzen ez badira. Normalean, iraungitze-epena 2 minutuko da.

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

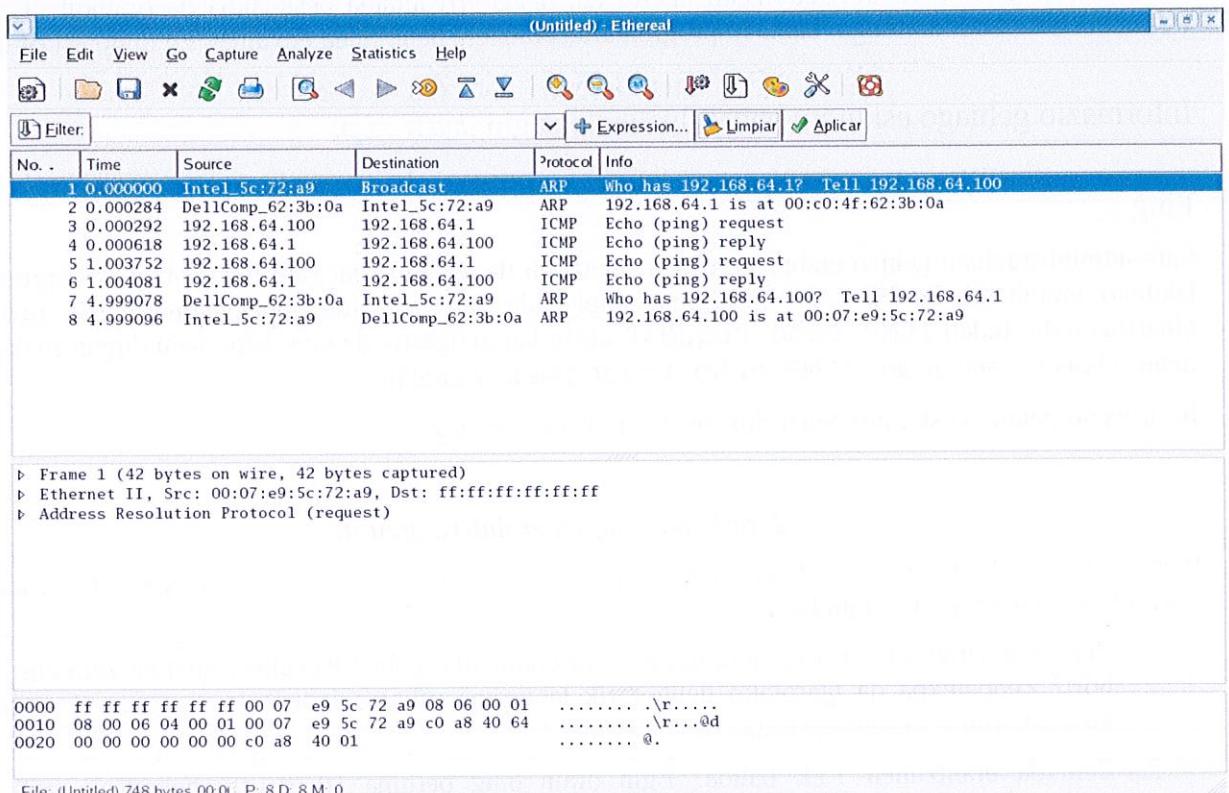
### Wireshark<sup>3</sup>

Protokolo-analizatzaile edo *sniffer* bat da. Sare-interfazeek (txartelek) jasotzen duten trafikoa gorde eta pantailaratzten du, erabiltzaileak erazagututako trafikoa atzemateko iragazkien (*Capture filter*) arabera. Derrigorrezko da sare-interfazea modo ‘promiskuoan’ egotea, hau da, saretik datozen trama guztiak jaso

<sup>3</sup> Lehen, Ethereal izenarekin ezaguna.

behar ditu (orokorrean, sare-txartel batek sistema eragileari makinarentzat diren tramak soilik pasatzen dizkio), eta, horretarako *root* moduan egikaritu behar da (**sudo** erabiliz). Analizatzailea erabiltzaile mailan exekutatzet den softwarea da, kernel-aren zatia den trama-iragazkiarekin komunikatuz. Iragazki honek, sare-txartelaren driver edo kontrolatzalearekin komunikatzen da, txartelaren bidez jaso edo igortzen den trama bakoitzaren kopia lortzeko. Analizatzaileak, iragazkian finkatutako baldintzak betetzen dituzten tramak jasoko ditu soilik (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-en trama-jasotzea.

Wireshark-ek ingurune grafikoa eskaintzen du, bere erabilera errazagoa eginez beste analizatzaile batzuekin konparatuta (adibidez `tcpdump`). Harrapaketa bat abiatzen denean, zabaldutako leihoa ikus dezakegu, denbora errealean, iragazkiak harrapatutako trafikoa. Trafiko hori lasai aztertzeko, ordea, harrapaketa gelditu eta atzemandako trafikoa arakatu 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.

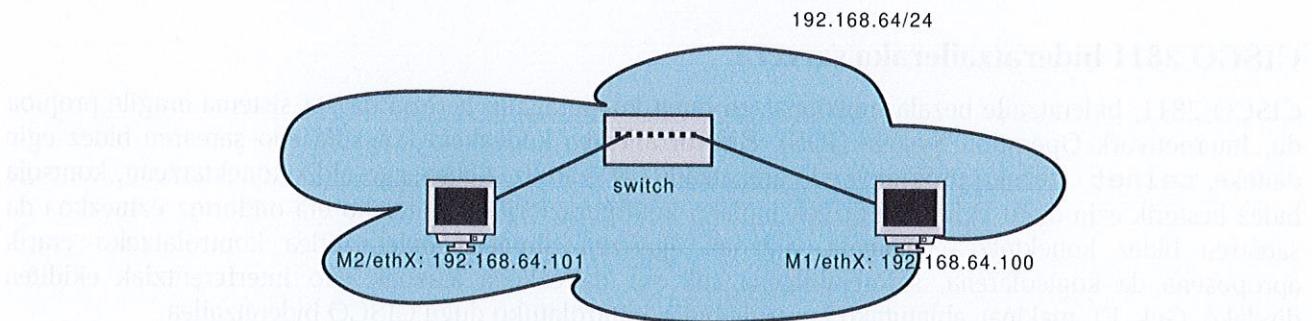
Wireshark exekutatzeko, terminal bat ireki, eta '**sudo -b wireshark**' idatzi; 1 irudiaren antzeko leihoa azalduko zaizu.

Irudian, iragazkirik gabeko trama-eskuratze bat egin da. Jasotako trafikoa, ARP eta ICMP da. Leihoa hiru zati ditu. Lehenengoan, jasotako tramen laburpena daukagu (trama bat lerroko). Bigarrenean, lehenengo leihoa aukeratutako tramaren detaileak ikus ditzakegu. Azkenik, hirugarrenean, tramaren edukia ikus daiteke hamaseitarrean eta ASCII formatuan.

*Aholkua: denbora soberan baduzu (bestela etxeen egin), 'man wireshark' exekutatu eta aztertu jasotako informazioa. Wireshark-i 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 ondorengo urratsak jarraitu M1 eta M2-n:

- 1) Gelditu network managerra: **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 esleitzu 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 kommutagailuetako bat, eta PIZTU ORAIN. Hartu sare-kable normaletako bat (ez hartu gurutzatua!) eta konektatu zure makina piztu duzun kommutadoreko aho batera. Ziurtatu aho horri dagokion led-a piztu egin dela konektatzerakoan, eta kolore gorritik berdera igaro dela.
- 6) Ea sarea dabilen frogatu. Horretarako ping egin M1etik M2-ra edo alderantziz. Zein IP helbideak erabili behar dituzu orain M1 eta M2 identifikatzeko? *Tindiketa*

## 3. ariketa: arp eta Wireshark-ekin trebatzen

1. Ireki terminal-leihoa bat M1 makinan. Konsultatu ezazu arp taula, terminal horretan '**arp -n**' komandoa exekutatuz. Ba al dago sarrerarik taulan? Sarreraren bat balego, arp komandoaren **-d** aukera erabili taula husteko. Oharra: **-d** aukeraren erabilera konsultatu eskuliburuan (**man arp**).
2. Exekutatu orain wireshark lehenengo terminalean, ARP edo ICMP edukia duten trama atzemateko konfiguratu (capture/options lehioan<sup>4</sup> **arp or icmp**<sup>5</sup> filtroa ezarri), eta abiatu ('start' botoia sakatu). Bigarren leihoa berriz, ping bat exekutatu ondoko makinara, trama bakarra bidaliz (-c aukera). Wireshark-ek trafikorik jasotzen ez duenean (segundo batzuk), gelditu eskuratzea. Ordoren, arp taula berriz konsultatu. Zer sarrera daude orain?

wireshark-ek eskaintzen duen informazioa aztertu, ondorengo galderak erantzuteko:

Aukeratu eta aztertu ARP edukia daraman trama bat: zein protokolo erabiltzen da TCP/IP arkitekturen maila bakoitzean? Zein maila arte ailegatu zara? Hartu orain ICMP trama bat eta galdera berdinei erantzun.

<sup>4</sup> Lubuntun instalatuta dagoen Wiresharken bertsioak lehio nagusian bertan du filtroak definitzeko laukia, eta ez 'Capture/options' aukera hartuta irekitzen den lehioan.

<sup>5</sup> Adi, minuskulak erabili.

Erantzun al du ondoko makinak ping komandoari? Nola daki makina horrek zein IP helbideari 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, bideratzale bezala funtzionatzen duen konputagailu berezia da eta sistema eragile propioa du, Internetwork Operation System (IOS). Bideratzailaren kudeaketa kontsola edo sarearen bidez egin daiteke, `telnet` izeneko programa edo arakataile 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-erabilpenagatik sor daitezkeen arazoak edo interferentziak ekiditen direlako. Guk, EL makinan abiatutako kontsola bidez kontrolatuko dugu CISCO bideratzailea.

Kontsola bidez konektatzeko bi gauza behar ditugu:

- 1) Konputagailu bat, serie portua libre duena, eta terminal-emuladore softwarea. Gure konputagailua EL izango da, eta `kermit` programa erabiliko dugu.
- 2) Kable bat, konputagailua eta bideratzailea fisikoki konektatzeko. Hau izango da hasieran aipatutako kable urdina, DB-9 konektorea (serie portua) eta RJ-45 konektorea (bideratzailaren kontsola portua) dituena.

Kontsola bidezko konexioa ezartzeko ondorengoa egin beharra dago:

1. Kablea ondo konektatu: bideratzailaren 'console' konexiora (urdina), eta konputagailuan serie portuan.
2. Ireki terminala konputagailuan, eta `kermit` programa exekutatu (`kermit` idatziz). Prompt-a azalduko zaizu:

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

3. Aukeratu erabiliko duzun serie portua:

```
(/root/) C-Kermit> set line /dev/ttys0
```

4. Linea telefonikoa erabiliko ez dugunez, eramailearen detekzioa desgaitu:

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

5. Bideratzalearekin konexioa ireki:

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

6. Return sakatu eta zure username (root) eta pasahitza (enable) eskatuko dizkizu. Ondoren prompta agertuko zaizu:

```
CISCO#
```

## CISCOren IOSa

IOSaren testu komandoen interfazearen sintaxia nahiko erraza da, baina honen erabilera zaila egiten da ehunka komando daudelako (eta komando bakoitzeko aukera anitz). Linuxekin alderatuta, IOSak lan modu piloa ditu (Linuxen bi, `sudo` eta arrunta), eta modu bakoitzean komando-multzo desberdina dugu. Modu batetik bestera pasatzeko komando bereziak erabiltzen dira, eta laguntza gisa, prompt-ak esaten digu momentu bakoitzean zein modutan gauden. Ondokoak dira ohiko lan-moduak eta bakoitzari dagokion prompt-a:

- Erabiltzaile modua: `CISCO>`  
Ez dugu erabiliko, ezta, normalean, ikusiko ere.

- Modu pribilegiatua : **CISCO#**

Normalena, modu honetan sartuko gara zuzenean bideratzailea piztean.

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

Modu honetan egiten dira makina osoari dagozkion konfigurazioak.

- Konfigurazio espezifikoetarako moduak. Asko dira (17 baino gehiago), eta IOSren bertsioaren araberakoak. Gure laborategietan erabiliko dugun ia bakarra Interfaze-konfigurazio modua da. Honakoa da bere prompt-a: **CISCO(config-if)#**

Modu honetan interfaze bati bakarrik dagozkion konfigurazioak egiten dira.

Ezin da edozein lan-modu batetik edozein bestera zuzenean pasa. Ariketa desberdinak egin ahala ikusiko ditugu lan-moduen arteko ibilbideak eta oinarritzko komandoak.

*Aholkua: IOS erabilera hobeto ezagutzeko (CLI-Command Line Interface) ikusi bere 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 bideratzaile, eta ireki konsola bat EL-n, EC kontrolatzeko (ikusi aurreko orria).
2. Ikusi zein den duzun prompt-a CISCO makinan Zein lan-modutan zaude? Ez bazaude modu pribilegiatuau, tekleatu:  
**CISCO> root**  
Eta eman pasahitza.
3. Probatu nola erabiltzen den on-line laguntza IOSen: **Help** tekleatu eta erantzuna aztertu.
4. Ikusi bideratzailean interfaze-konfigurazioa, **sh ip interface brief** exekutatz. Zenbat interfaze ditu bideratzaileak? Zein izen erabiltzen dira? Zeintzuk daude aktibatuta (up) eta zeintzuk ez? Orain egin **sh interfaces** eta erantzun ondorengo galderak, aktibatuta dauden interfazeei buruzkoak: Zein IP helbideak dituzte esleituta? Zein formatutan ematen dira IP helbideen maskarak? Ikusi ematen diren helbide fisikoen formatua, zer desberdintasuna dago Linux-en **arp** komandoak erabiltzen duen formatuarekin?
5. Erabiltzen ari zaren konsolaren konfigurazioa ikusteko, **sh line 0** egin. Bilatu 'timeouts idle EXEC' parametroaren balioa. Ziur aski, 5 minutukoa da. Horrela uzten baduzu, lata emango dizu laborategietan, CISCO konsolan lan egiten ez baduzu 5 minuto jarraian saioa etengo baitu eta berriz abiatur beharko duzu. Segituan ikusiko dugu nola desgaitu iharduera ezarako denboragailu hori.
6. Konfigurazio-orokorra modura pasa, **configure terminal** exekutatz. Ikusi prompt-a aldatu dela. Lan modu honetan gaudela desgaituko dugu beste portaera latoso bat CISCON: komando bat gaizki teklatzen dugun bakoitzean sistema ez blokeatzeko tarte batean, ondokoa egikaritu:

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

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

7. Iharduera ezarako denboragailua desgaitzeko konsolaren konfiguraziorako lan modu espezifikora aldatu behar da. Horretarako, egin **line console 0**, eta prompt-a aldatuko zaizu. Orain egin:

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

8. Atera konsola konfiguratzeko modutik. Bi eratara egin dezakezu:

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

Lehena hartuko dugu:

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

9. Orain interfazeen konfigurazioa aztertuko dugu. Ondo ikasi hau. Laborategi guztietai hainbat aldiz egin beharko baituzu. Edozein interfazearen konfigurazioa aldatzeko, interfaze horren konfigurazio lan-modu espezifikora igaro behar dugu, **interface interfazearen\_izena** tekleatuz (prompt-a aldatuko da). Aldatu FastEthernet0/0 interfazea konfiguratzeko lan modura.
10. Orain, 192.168.64.11/24 helbidea esleitu Fastethernet0/0 interfazeari. Horretarako, ondorengo komandoak exekutatu behar dira:
  - IP helbidea esleitzeko:  
**ip address ip\_helbidea maskara\_formatua\_dezimalean**
  - Interfazea gaitzeko:  
**no shutdown**
  - Atera interfazea konfiguratzeko lan modutik eta grabatu egindakoa:  
**end**
11. Orain ping bat egiten bada erabiltzaile makina bat eta 192.168.64.11 helbidearen artean, ez du funtzionatuko, oraindik ez dugulako interfaze hori fisikoki sarera konektatu. Egoera berdinean egongo ginateke sare-kablea gaizki balego, muturren bat deskonektatuta egonez gero, edota konektoreren bat puskatuta. Alegia, konexio fisikoa ez dabil. Egikaritu **sh ip interface brief** komandoa, konekta ezazu fastethernet0/0 kommutagailura 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 bideratzaileik. Horretarako ping erabili bideratzailean, makina horien kontra. Zenbat oihartzun bidali eta jaso dira ping bakoitzean? Kontrolatu al dezakezu, linuxen egiten den moduan, zenbat oihartzun bidaltzen diren?

## Laborategitik joan aurretik, GOGORATU:

- Gorde erabilitako sare kable guztiak bere poltsan.
- Itzali makina guztiak: M1, M2, Linux bideratzailea, Cisco bideratzailea, eta kommutadoreak.
- Hurrengo laborategietara ekarri behar duzu enuntziatu hau eta hartutako apunteak.

## 2. Laborategia: Birbidaltzea konfiguratzen

Helburuak:

1. IP datagramen birbidalketa prozesua errepasatzea.
2. Bideratzaileak nola konfiguratzen diren ikastea (bide estatikoak), Linux eta CISCO inguruneetan.

Denbora: 2 o. 25'

Lan metodologia:

1. Dokumentazioa irakurri, eta bete galdeategia moodle-n.
2. Laborategian, ariketak egin, gidoian agertzen diren ahala, eta behar dituzun apunteak hartu.
3. Erabili dituzun makinak itzali eta utzi lanpostua aurkitu duzun bezala. Ahaztu gabe, fakultateko sare-kableak konektatu berriz.

### 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 etxearen praktikatzeko, GNS3 simuladorea erabili: <http://www.gns3.com/>.

### Birbidaltze-taulak eta IP konfigurazioa

IP erabili behar duten makina guztiak behar dute birbidaltze-taula bat, bai bideratzaileek, baita erabiltzailearen makinek ere. Berez, birbidaltze-taula ondo osatzea behar-beharrezkoa da makina sarean ibili ahal izateko. Halaber, edozein makinaren IP konfigurazioa osatzeko, ondoko bi urrats bete behar dira:

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

Bideratzaileen kasuan, hirugarren urratsa ere gehitu behar da:

3. Birbidaltzko ahalmena gaitu. Hau ere laborategi honetan ikasiko duzu.

Bi erako sarrerak egoten dira birbidaltze-taula batean:

- Zuzenean lotuta ditugun sareetara joateko bideak.  
Sarrera hauek sistemak berak gehitzen ditu, interfaze bat IP helbidea esleitzeko diogunean.
- Beste bide guztiak.

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



## Birbidaltze-taulekin lan egitea Linuxen

Ondokoak dira erabiltzen diren komando nagusiak<sup>1</sup>:

- netstat

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

- route

Hau birbidaltze taulan bide berriak sartu behar badugu edo bideak ezabatzeko erabiliko dugu. Bide bat sartzeko komandoa honakoa da:

```
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 baditu **route** komandoak. Gehiago jakin nahiz gero, edo zalantzak baditzu, kontsultatu sistemaren laguntza **man route** eginez.

- Gauza berdinak 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

Kernelaren **ip\_forward** parametroari '1' balioa eman behar zaio. Hori egiteko bi era posible honakoak dira:

- Zuzenean parametro hori gordetzen duen fitxategian idatziz:  
`echo 1 > /proc/sys/net/ipv4/ip_forward`
- Kernelaren parametroak aldatzeko **sysctl** tresna erabili:  
`sysctl -w net.ipv4.ip_forward=1`

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

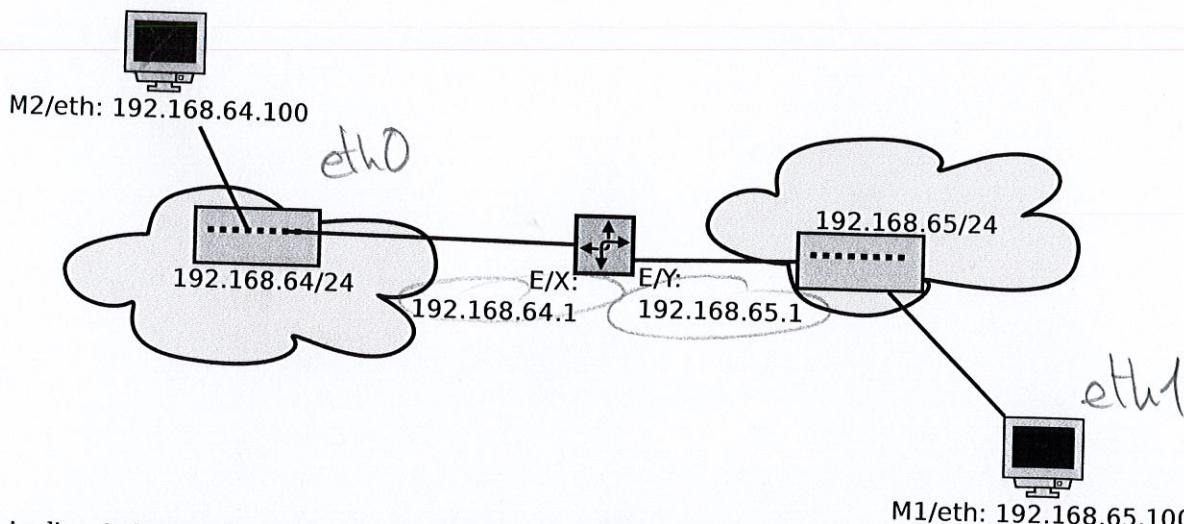
## Sare-topologia

Laborategi honetan sare bana osatuko dugu mahaian dugun kommutagailu bakoitza erabiliz. Gero, bi sare horiek elkartuko ditugu bideratzaile bat erabiliz, 1 irudian azaltzen den bezala<sup>2</sup>.

<sup>1</sup> Adi: hauek ez dira modu bakarrak lan hauetan egiteko, beste era asko badaude.

<sup>2</sup> Oharra: Benetako interfazeen izenak ez dira izango irudian agertzen direnak, baizik sistema bakoitzak esleitutakoak.





1 irudia : Ariketetarako sarea. E bideratzalea EL izango da 1. eta 2. ariketan, eta EC izango da 3. ariketan.

### 1. ariketa: sarearen ezarpen fisikoa

#### 1. Sarea fisikoki eraiki. Honetarako:

- Kendu M1 eta M2 konputagailuetatik unibertsitateko sare-kablea, alde batera utzi, eta PIZTU BI MAKINAK. M1 eta M2-n desgaitu network-managerra (**sudo service network-manager stop**). Interfaze birtualak badaude gaituta, desgaitu (**ifconfig interfazearen\_izena down**).
- Birkonfiguratu M1 eta M2 makinen interfazeak, aurreko taulan finkatutakoaren arabera (ikusi 1. laborategia zalantzak badituzu).
- PIZTU MAHAIKO BI KOMMUTAGAILU. M1 kommutagailu batera konektatu, eta M2 beste kommutagailura konektatu, kable normalak erabiliz (ez gurutzatua!!). Ziurtatu dagozkien ledak berdez gelditzen direla.
- PIZTU EL makina. Network managerra abiatuta balu, geldiarazi. Konsultatu interfazeen egoera, eta ez bidaude gaituta, gaitu **ifconfig interfazearen\_izena up** eginez. Ziurtatu zein den **eth0** txartela eta zein **eth1**<sup>3</sup>.  
*Aztertu EL-ren birbidaltze-taula*
- EL-ren interfazeetako bat 192.168.64.1 helbidea esleitu, eta M2 konektatu duzun kommutagailu berari lotu interfaze hori (adi zein den EL makinaren **eth0** eta zein **eth1**!), kable normal bat erabiliz (ez gurutzatua!!).
- Berrikusi EL-ren birbidaltze-taula. Zein bide agertu da? **E/A**
- Ping egin EL-tik M2-ra, 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 kommutagailuarekin konektatu, beste kable normal bat erabiliz (ez gurutzatua!!).
- Berrikusi EL-ren birbidaltze-taula. Zein bide agertu da? **E/A**
- Egin ping EL-tik M1-era. Ez badabil, berrikusi egindakoa eta **ez jarraitu ping hau ibili arte**.

<sup>3</sup> Gure laborategikomakina hauetan, integratuta dagoen txartelaren helbide fisikoa beti hasten da 00:0c:f1.



2. Egiaztatu EL-en 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 M1-etik M2-ra. 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 ulertzenean 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 M1-etik M2-ra, eta alderantzizkoa. Baten bat ez badabil, berrikusi egindakoa eta **ez jarraitu ping hauek ibili arte**.
4. M1 eta M2, EL-era konektatuta egoteaz gain, beste makina batzuk switch-etara konektatuta egongo balira, aldatuko zenituzke M1, M2 eta EL-en birbidaltze-taulak? Zein helbideratze-tartean egon beharko lirateke switch-etara konektatutako makinak? Erantzunak ez baditzu topatzen, kontsultatu irakaslearekin.
5. Gure laborategiko sarea isolatuta dago. Baino demagun EL-ek hirugarren interfazea baduela, `eth2` izenekoa, interfaze hori 158.227.112.0/20 sarera lotuta duela, 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 M1 eta M2-n, ICMP trafikoa soilik hartuz.
3. M2-tik M1-era ping bat egin (bakar bat, -c aukera erabiliz), eta trama-eskuratzea eten bi trama atzman eta gero.
4. Aztertu jasotako tramak. Zeintzuk 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 sistemana

- 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 azaltzeko 0.0.0.0 da aurrezenbakia eta maskara.

- Birbidaltzeko gaitasuna abiatzeko, lan modu pribilegiatuan: **ip routing**



---

**3. ariketa: Bide estatikoen konfigurazioa CISCO erabiliz**

---

Oraingoan, ELren ordez, EC erabiliko dugu sarean eta 2.5 ariketako neurketa errepikatuko dugu. Urratsak honakoak dira:

1. EL deskonektatu kommutagailuetatik.
2. EC PIZTU eta ireki kontsola bat EL-n EC kontrolatzeko (ikusi aurreko laborategiko dokumentazioa).
3. ECren interfazeak birkonfiguratu hasieran emandako taularen arabera. Aztertu ECren birbidaltze-taula, eta egiaztu espero duzun bezala dagoela. Zergatik ez diozu inongo sarrerarik gehitu behar?
4. EC bideratzailearen bideratze ahalmena gaitu.
5. Egiaztu, ping baten bidez, M1 eta M2-ren artean konexioa dagoela. Ez badabil, berrikusi egindakoa eta **ez jarraitu ping hau ibili arte**.
6. Errepikatu 2.5 ariketa, eta konparatu lortutako denborak.

Laborategitik joan aurretik, **GOGORATU**:

- Gorde erabilitako sare kable guztiak bere poltsan.
- Itzali makina guztiak: M1, M2, Linux bideratzailea, Cisco bideratzailea, eta kommutadoreak.
- Hurrengo laborategietara ekarri behar duzu enuntziatu hau eta hartutako apunteak.



### 3. laborategia: DHCP

Helburuak:

1. DHCP-ri buruzko ezagutza zabaldu eta sendotzea.
2. Linux inguru batean, DHCP zerbitzariak eta bezeroak konfiguratzeko ikastea.
3. CISCO inguru batean, DHCP proxy bat konfiguratzeko ikastea.
4. Sare-interfazeen oinarrizko konfigurazioaren eta birbidaltze taulen (Linux eta CISCO) errepasoa.
5. Sare-ekipoen muntaia eta konfigurazioan trebatzea.
6. Sare-monitorizaziorako tresnen erabileran trebatzea.

Denbora: 2 o. 25'

Lan metodologia:

1. Ondo errepasatu nola konfiguratzeko den IP-a linux eta IOS makinetan.
2. Dokumentazioa irakurri, eta bete galdetegia moodle-n.
3. Laborategian, ariketak egin, gidoian agertzen diren 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 PORTATILAK

### DHCP protokoloa

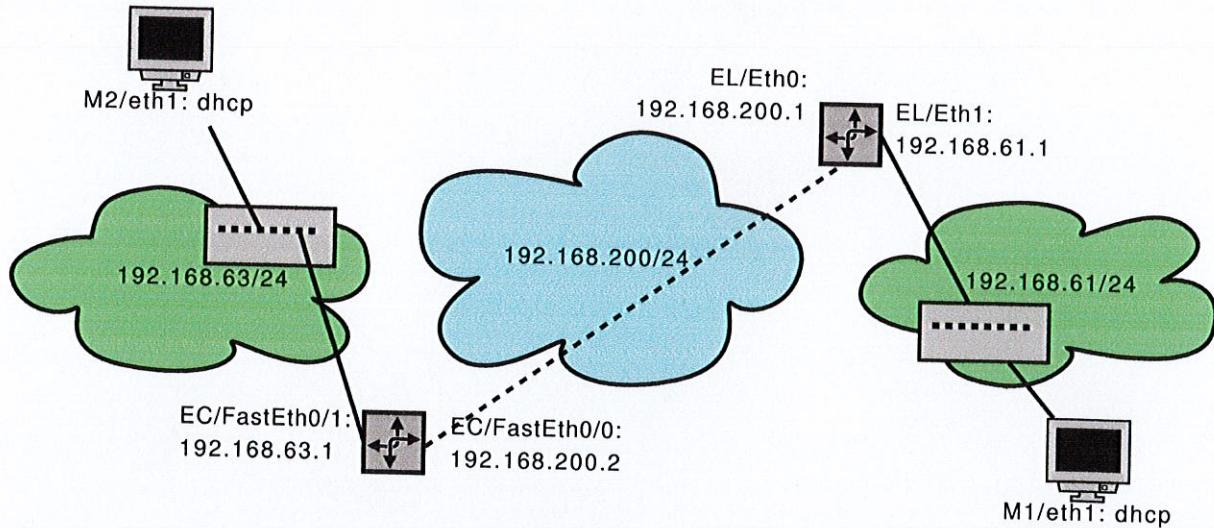
Protokolo hau, erabiltzaile makinaren IP parametro batzuk dinamikoki konfiguratzeko erabiltzen da. Gutxienez IP helbidea, aurrezenbakia, eta irtenbidea eman behar zaio makina bati bere IP konfigurazioa osatzeko, baina, tipikoki, bere sareko DNS zerbitzaria zein den ere ematen zaio. DHCP-k bezero/zerbitzari eredua jarraitzen du: bezeroek (aplikazio mailan, berez) eskaerak luzatzen dizkiote zerbitzariari DHCP protokoloa erabiliz, eta zerbitzariak erantzuten die eskatutako konfigurazio-parametroak bidaliz. Aplikazio mailak UDP erabiltzen du. RFC 2131-ak azaltzen du aplikazioko protokolo osoa.

### Sare-topologia

Erabili dugun sare-topologia 1 irudian dagoena da. Bideratzaileen IP konfigurazioa eskuz egingo dugu, baina M1 eta M2 makinaren 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 (honetan exekutatuko da DHCP zerbitzaria) daude.
- 192.168.63.0/24 sarean M2 eta EC ditugu. M2-k ere, EL-en dagoen DHCP zerbitzua erabiliko du.
- 192.168.200.0/24 sarean bi bideratzaile daude. Sare hau gauzatzeko ez dugu hirugarren kommutagailu bat mahai gainean, eta, horregatik, kable gurutzatu batekin lotuko ditugu zuzenean EC eta EL bideratzaileak. Baino, praktikan, kommutagailu 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>1</sup>.
2. Ondokoa egikaritu EL makinan: **`rm /etc/dhcp/lab03.conf`**
3. **EL-tik** konsola bidezko konexioa ireki EC-ekin, kermit erabiliz (ikusi 1. laborategia).
4. Kable normalak erabiliz, lotu bideratzaileak komutagailuekin, 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 zuzenak besterik ez dira agertu behar.
6. Bi bideratzaileen birbidaltze-taulak osatu zuzenean lotuta ez duten sarera joateko bide bat gehituz. Birbidaltze ahalmena gaitu bi bideratzaileetan. Egiaztatu birbidaltze taulen edukia bi bideatzaleetan. Ez bada espero duzuna, edo agertzen bada ulertzten ez duzu sarreraren bat, **ez segi aurrera taula konpondu arte**.
7. Ping bana egin EL-tik EC-ko interfaze bakoitzari. Haietako bat ez badabil, berrikusi orain arte egindakoa, ping hauek ibiltzen lortu arte.
8. Idem ECtik ELko bi interfazeetara. Baten bat ez badabil, berrikusi egindakoa, ping guztiak ibili arte.

**DHCP zerbitzari baten konfiguratzea eta abiatzea Lubuntu sistemean**

`dhcpd` programak Linux-eko DHCP zerbitzaria abiatzen du (informazioa on-line eskuliburu). Zerbitzaria exekutatzean, honek konfigurazioa kargatuko du `/etc/dhcp/dhcpd.conf` fitxategitik, guk beste konfigurazio-fitxategirik ematen ez badiogu. Fitxategi honen sintaxia oso konplexua izan daiteke DHCP zerbitzuaren funtzionalitate guztiak erabili nahiz gero. Guk oinarrizko konfigurazio bat egingo dugu, non:

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

<sup>1</sup> Oinarri plakan dagoenaren helbide fisikoa 00:0c:f1 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.
- EL-ren 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 horrela 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 EL-en**

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



2. Terminal bat ireki EL-en, eta abiatu DHCP zerbitzaria **dhcpd -f -cf /etc/dhcp/lab03.conf** exekutatuz. Ez kasu egin agertuko zaizun 'ERROR PID ...' mezuri.

**dhcpd** komandoari buruzko informazio gehiago nahiz gero, aztertu on-line eskuliburuan labotegira 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>2</sup>. Abiatuta dagoela, konektatu kable normal batekin 1 irudian agertzen den moduan. Interfaze birtualak desgaitu (**ifconfig interface\_izena down**) eta network manager **abiatuta ez dagoela egiaztatu**. Abiatuta balego, gelditu.
2. Egiaztatu birbidaltze-taula hutsik dagoela, **netstat -rn** egikarituz. Hutsik ez balego, hustu.
3. Exekutatu Wireshark M1-en<sup>3</sup>, DHCP trafikoa hartzeko edozein interfazean (**any** interfazea aukeratu). Horretarako behar den **capture** filtroan DHCP-k erabiltzen dituen portuak azaldu (bat bezeroentzat eta bestea zerbitzariantzat): **port bootpc or port bootps**.
4. Beste terminal batetik, abiatu DHCP bezeroa zure interfazean M1-en<sup>4</sup>:

**dhclient -d interfazearen\_izena**

5. Bezzeroaren iharduera zelatatu wireshark-aren leiohan, eta 6 trama atzematen dituenean<sup>5</sup>, Wireshark gelditu<sup>6</sup> eta gorde pantailan agertzen dena (hurrengo ariketan ere beharko duzu). Jasotako informazioa aztertu, eta erantzun ondoko galderak:
  - Aztertu lehenengo trama, eta esan zein protokolo erabiltzen den arkitekturako maila bakoitzean. Oharra: DHCP protokoloa identifikatzeko bere aurrekaria izan zenaren izena erabiltzen dela: *bootstrap protocol*. Zein protokolo erabiltzen duen DHCP zerbitzariak garraio mailan? Eman arrazoiren bat protokolo hori erabili behar izateko.
  - Atzman diren 6 trama horietan bi DHCP eragiketa burutu dira: esleipen bat eta berritze bat. Paper batean idatzi horietako eragiketa bakoitzean izandako DHCP mezu-trukea, mezu bakoitzaren DHCP mota eta IP jatorrizko eta helburuko helbideak identifikatuz.
  - Zein IP helbide esleitu zaio M1-en interfazeari (**ifconfig** erabili egiazatzeko)? Aztertu EL-en **/var/lib/dhcp/dhcpd.leases** fitxategia, egiazatzeko ikusitakoa bat datorren fitxategiaren edukiarekin. Zein sarrera agertu dira M1-en birbidaltze-taulan?
  - Nola da posible M1-ek DHCP zerbitzariarekin komunikatu ahal izatea IP helbiderik gabe eta birbidaltze-taula hutsik izanik?
6. Errepikatu ariketa honen 1-2-3-5 atalak M2 makinan. Zergatik ez du M2-k 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 M2-n abiatutako **dhclient** bezeroa.

---

<sup>2</sup> UPV-ko sarera lotuta abiatzen baduzu, unibertsitateko DHCP konfigurazioa abiatuko da, eta ezingo duzu laborategiko ariketak ondo egin. Gainera, kablerik gabe piztuz gero, ez da network managerra abiatuko.

<sup>3</sup> Ggoratu, sudo moduan, ehu erabiltzaile gisa sartu bazara.

<sup>4</sup> Gero gelditzeko, CTRL-C sakatu.

<sup>5</sup> Zer edo zergatik esperimetua errepikatu behar baduzu, hurrengo egikaritzapenetan 4 trama baino ez duzu jasoko. Hasierako DISCOVER eta OFFER mezuak ez dira bidaliko. Hasierako egoera berreskuratzeko, DHCP bezeroaren cachea ezabatu behar duzu: **echo "" > /var/lib/dhcp/dhcclient.leases**

<sup>6</sup>Aholkua: gorde jasotakoa fitxategi batean, etxera eraman ahal izateko idatzitako dokumentazioarekin batera. Horrela, edozein momentutan berriz analizatu dezakezu.



## Proxy DHCP

Aurreko ariketako 6. atalean agertzen den arazoa konpontzeko, Proxy DHCP zerbitzari bat erabil daiteke. (edo *DHCP relay agent*). Proxy-a atzigarri egongo da bezeroentzat, hauen eskaerak jaso eta zerbitzarantz bidaliz. Era berean, zerbitzariaren erantzunak jaso eta bezeroetarantz birbidaliko ditu. Gure laborategian, CISCO (EC) bideratzaileak proxy DHCP-rena egingo du, 192.168.63.0/24 sarean dauden makinenzat.

### Proxy DHCP baten konfigurazioa IOS-en

Egin behar den gutxienekoa ondokoa da:

- Bezeroek egindako DHCP eskaerak jasoko dituen interfazea relay bezala 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: DHCP proxy (relay) baten funtzionamenduaren analisia**

---

1. Ziurtatu DHCP bezerorik ez dagoela abiatuta M2 makinan. Horretarako, begiratu ea 'dhcp' hitza 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, EL-en bidez zerbitzua emanez 192.168.63.0/24 sareari. Horretarako komandoak ondokoak dira<sup>7</sup><sup>8</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 M2-n eta EL/eth0-n, DHCP trafikoa jasoz. Aurreko ariketan definitutako filtro bera erabil dezakezu.

4. DHCP bezeroa abiatu M2-n, M1-en egin zenuen bezala.

5. Eten Wireshark-ek 4 trama jaso ondoren. Egiaztatu, **ifconfig** erabiliz, M2/eth0-k IP helbide bat duela. Egiaztatu ere M2-ren birbidaltze-taula ondo bete dela.

6. Erantzun ondoko galderak, eskuratutako tramak aztertuz:

- Aldatu al ditu proxy DHCP-ak birbidalitako DHCP komando edo erantzunak?
- Aldatu al ditu proxy DHCP-ak birbidalitako datagramen IP goiburukoak?
- Alderatu M2-k eta M1-ek jasotako DHCP erantzunak. Zein da aldea?
- Nola jakin dezake DHCP zerbitzariak (EL-ek) zein saretan dagoen DHCP request eskaera bidaltzen dion bezeroa? Nahiz eta gure sarean urrutiko sare bakarra egon, kontuan izan egoera erreal batean urrutikoa sare desberdinak egon daitezkeela EL-n kontrolpean, eskaera guztiak interfaze beretik jasoz.

**GOGORATU: /etc/dhcp/lab03.conf fitxategia ezabatu laborategia utzi baino lehen.**

<sup>7</sup> Gauza bera **dhcrelay** erabiliz egin dezakegu Linux-en.

<sup>8</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)



3.7

$$\max z = 3x_1 - 2x_2 + 2x_3 + x_4$$

have made

$$3x_1 + 6x_2 + 3x_3 + 2x_4 \leq 36$$

$$x_1 + 2x_2 + 3x_3 + x_4 \geq 14$$

$$x_1 + x_2 + x_3 + 2x_4 \geq 10$$

$$x_1, x_2, x_3, x_4 \geq 0$$

~~Eddy Dude~~

$$\text{Min } B = 36x_1 + 14x_2 + 10x_3$$

Kosten minimale

Karen Knobbe

846726A323

$$6y_1 + 2y_2 + y_3 = 22$$

$$8x_1 + 3x_2 + x_3 = 2$$

$$y_1 + y_2 + y_3 \leq 1$$



3.6

$$\max Z = -3x_1 + 4x_2 + 2x_3 + 5x_4$$

$$4x_1 + 2x_2 + 4x_3 + 3x_4 \leq 48$$

$$x_1 - 2x_2 + x_3 - 2x_4 \leq -8$$

$$-2x_1 + x_2 - x_3 - x_4 \leq -6$$

	3	-4	-2	-5	0	0	0	0	$m_0 = 2$
	4	2	4	3	1	0	0	48	$m_1 = -1$
a <sub>1</sub>	1	<span style="border: 1px solid black; padding: 2px;">-2</span>	1	-2	0	1	0	-8	
a <sub>2</sub>	-2	1	-1	-1	0	0	1	-6	$m_2 = -\frac{1}{2}$
a <sub>3</sub>	3	-4	-2	-5	0	0	0	0	$m_0 = -5$
a <sub>5</sub>	4	2	4	3	1	0	0	48	$m_1 = 3$
a <sub>6</sub>	1	-2	1	-2	0	1	0	8	$m_2 = -2$
a <sub>7</sub>	-2	1	-1	-1	0	0	1	6	$m_3 = -1$
a <sub>8</sub>	0	1	1	<span style="border: 1px solid black; padding: 2px;">1</span>	0	0	0	1	M
	3	1	3	0	0	0	0	5M	$m_0 = -1$
a <sub>5</sub>	4	<span style="border: 1px solid black; padding: 2px;">-1</span>	1	0	1	0	0	-3M	$48 - 3M$
a <sub>6</sub>	1	0	3	0	0	1	0	8	$-8 + 8M$
a <sub>7</sub>	-2	<span style="border: 1px solid black; padding: 2px;">0</span>	0	0	0	0	1	-6 + M	$m_2 = 0$
a <sub>4</sub>	0	1	1	1	0	0	0	1	$m_3 = -2$
	7	0	4	0	1	0	0	2	$m_4 = -1$
a <sub>2</sub>	-4	1	-1	0	-1	0	0	3	$2M + 48 - (36 - 2M) = 84$
a <sub>8</sub>	1	0	3	0	0	1	0	2	$3M - 48 - (-36 + 3M) = 6$
a <sub>2</sub>	6	0	2	0	2	0	1	<span style="border: 1px solid black; padding: 2px;">-5</span>	$m_2 = -\frac{3}{5}$
a <sub>4</sub>	4	0	2	1	1	0	0	-2	$2M - 8 - (-36 + 2M) = 28$
	$\frac{42}{5}$	0	$\frac{24}{5}$	0	$\frac{9}{5}$	0	$\frac{2}{5}$	0	$48 - 2M - 36 - 2M = 12$
a <sub>2</sub>	$-\frac{2}{5}$	1	$\frac{1}{5}$	0	$\frac{1}{5}$	0	$\frac{3}{5}$	0	$84$
a <sub>6</sub>	$\frac{17}{5}$	0	$\frac{19}{5}$	0	$\frac{4}{5}$	1	$\frac{2}{5}$	0	6
a <sub>8</sub>	$-\frac{6}{5}$	0	$-\frac{2}{5}$	0	$\frac{2}{5}$	0	$-\frac{1}{5}$	1	$-18 + M$
a <sub>4</sub>	$\frac{8}{5}$	0	$\frac{6}{5}$	1	0	$-\frac{2}{5}$	0		12

what	is	process of	which	and
shrub	?	process of	which	and
what	process	which	and	and
what	process	which	and	and
what	process	which	and	and

Sistema @IP	Protocolo portas	Protocolo @IP	Protocolo porta	Otro/basta
Any	25 <del>10000-10000</del> Any	140.222.200.4	25	Alerta
Any	Any <del>10000-10000</del>	140.222.200.3	80	Alerta
140.222.200.4	25	Any	<del>10000-10000</del> 25	Alerta.
140.222.200.3	80	Any	<del>10000-10000</del> Any	Alerta
Default	Default	Any	Any	Default