IPv6 nonahi baliatzeko gidaliburua

Guillermo Cicileo
Roque Gagliano
Christian O'Flaherty
Mariela Rocha
César Olvera Morales
Jordi Palet Martínez
Álvaro Vives Martínez

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
ARGITALPEN ZERBITZUA
SERVICIO EDITORIAL

Internet Society™

Liburu hau Hezkuntza, Unibertsitate
eta Ikerketa Sailaren laguntzaz
argitaratu da.

EUSKO JAURLARITZA
GOBIERNO VASCO

HEZKUNTZA, UNIBERTSITATE
ETA IKERKETA SAILA

DEPARTAMENTO DE EDUCACIÓN,
UNIVERSIDADES E INVESTIGACIÓN

UPV/EHUko Euskara Zerbitzuak koordinatutako itzulpena
Itzultzailea: Elhuyar Fundazioa. Ixiar Iza.
Hizkuntza-begiralea: Juan Kruz Igerabide.

Begirale teknikoa: Maider Huarte, I2T (Ikerkuntza eta Ingeniaritza Telematikoa – Investigación e Ingeniería Telemática)

I.S.B.N.: 978-84-694-3496-3

Fotokonposizioa: Ipar, S. Coop.
Zurbaran, 2-4, 48007 Bilbao

IPv6 nonahi baliatzeko gidaliburua

Guillermo Cicileo
Roque Gagliano
Christian O'Flaherty
Mariela Rocha
César Olvera Morales
Jordi Palet Martínez
Álvaro Vives Martínez

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
ARGITALPEN ZERBITZUA
SERVICIO EDITORIAL

Internet Society™

Eskerrak

Internet Societyri (www.isoc.org), proiektu hau gauzatzeko behar zen diru-laguntza emateagatik eta atalen iraupena eta garrantzia etengabe sustatzeagatik.

6DEPLOY proiektuko kideei (www.6deploy.eu), liburu honen edukia lantzen laguntzeagatik, eta etengabe IPv6 zabaltzeko lan egiteagatik (dokumentuen, trebakuntzaren eta laguntza birtualeko mahaiaren bidez).

LACNICi (www.lacnic.net), liburu honi egindako ekarpenengatik, liburua itzultzen laguntzeagatik, eta Latinoamerikan eta Karibean IPv6-ren garrantziaz eta beharraz jabetzeko trebakuntza-lanak egiteagatik.

Liburu honen **egile** eta **laguntzaile** guztiei eta **diseinatzailearri**, haien ardurari eta lanari esker gauzatu baita proiektu hau, zeina egin baitugu Interneteko komunitateari IPv6 protokolo berria onartzen eta ezartzen laguntzeko.

Zuzendaritza Batzordea
Internet Societyren Argentina atala - ISOC-Ar

Aurkibidea

Egileak

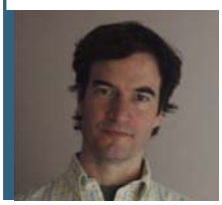
Guillermo Cicileo

Gaur egun, Argentinako unibertsitate nazionalen sareko (RIU) Koordinatzaile Nagusia da. FLIP6-ko (Foro Latinoamericano de IPv6) kidea da 2007tik. CLARAren (Cooperación Latinoamericana en Redes Avanzadas) sorreran parte hartu du, eta proiektuaren hasierako Batzorde Teknikoko kidea izan zen. Ondoren, 2005etik 2008ra, RedCLARA-ko Multicast lan-taldearen koordinazio-arduraduna izan zen, eta IPv6 eta Bideratze Aurreratua lan-taldeetako kide ere bai. CLARAk antolatutako bideratze aurreratuko tailerretan irakasle ere izan da, eta trebakuntza-saioak eman ditu, besteak beste, multicast, IPv6 eta BGPri buruz. Hori baino lehen, RETINA sareko zuzendariordea izan zen, non Eragiketak eta Teknologia Berriak alorren ardura baitzuen. Hango jardunean, sarean IPv6 jatorriz ezarri zuen, bai nazioarteko konektagarritasunari bai nazioko hedapenari dagokienez. Sare zientifiko eta akademiko nazional eta internazionalei lotutako lanetan aritu da hamabost urtez baino gehiagoz. Argentinan Internet2-ra eta Sare Aurreratuetara egindako lehen konexioa zuzendu zuen, baita Argentina RedCLARA-n sartzeko prozesua ere.

Roque Gagliano

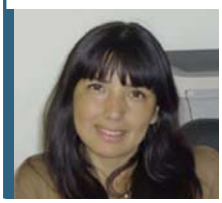
Hamar urte baino gehiagoko esperientzia du IP sareetan. Gaur egun, LACNICen egiten du lan (Latinoamerikako eta Karibeko Internet erregistroan), proiektuetako ingeniari senior gisa eta politikako alorreko arduradun gisa. Proiektu teknikoak koordinatzen ditu eta LACNICen eraginpeko eskualdetan baliabideak esleitzeko politiken garapen-prozesua kudeatzen du. LACNICen IPv6-ko irakasle eta trebatzaile ere bada, Latinoamerikan. IPv6-rekin lan egin du, halaber, LACNICen Montevideoko sare korporatiboaren eta Brasilgo zerbitzari kritikoen sarearen soluzioa diseinatzen. Beste herrialde batzuetan lehenengo IPv6 konexioak martxan jartzen lagundu du (Haitin, Sint Maartenen, Curaçaon eta Trinidad eta Tobagon). IETFn ere lan egiten du, bereziki IPv6-rekin eta zirkulazio-trukaketarekin zerikusia duten taldeetan. Hori baino lehen, ANTELen jardun zuen, Uruguain, sare-arkitekto gisa, MPLS teknologian oinarritutako sarerako IPv6 diseinatzen. Hori baino lehen Estatu Batuetan egin zuen lan, Sprint Nextel Corp. enpresan. Roque Gaglianok Ingeniaritza elektrikoko graduondoko bat egin du Kansasko Unibertsitatean (AEB), eta Ingeniaritza Elektrikoa ikasi du UDELAR Unibertsitatean (Uruguai). Fulbright beka bat eta OEAren beste bat jaso ditu, eta IEEEko kidea da.

Christian O'Flaherty



Konputazio Zientzietan lizentziatua (Hegoaldeko Unibertsitate Nazionala, Bahía Blanca, Argentina). Sistema Eragileetako eta Datu-sareak eta Datuen Teleprozesaketako irakasle gisa ekin zion ibilbide profesionalari, eta, ondoren, RETINA sare akademiko nazionalean jardun zuen, sareko eragiketa- eta plangintza-lanetan. Interneteko eragiketen arduradun izan zen, ondoren, Impsat Argentinan (satelite bidezko zerbitzuen hornitzaile bat da, eskualdeko IP zerbitzuen hornitzaile bihurtu zena). 2006 urtean Global Crossing-ek erosi zuen enpresa hori, eta Christian O'Flaherty Internet produktuaren arduradun gisa aritu zen han 2009ra arte. Orduan, Internet Societyko Senior Education Manager postua hartu zuen, eta horretan jardun du gaur arte. 2004tik 2008ra, politika-zerrenden moderatzaile eta politiken foro publikoko mahaiburu izan da, LACNICen. Gaur egun, ISOC Argentinako zuzendaritza-batzordeko eta Task Force Argentinako IPv6-ko kidea da.

Mariela Rocha



Informazio-sistemen Ingeniaritzan graduatua da (Unibertsitate Teknologiko Nazionala, Argentina), eta teknologia berriekin eta sareen ingeniaritzarekin erlazionatutako lanetan aritu da, batez ere ingurune akademikoan. 2003an hasi zen IPv6-rekin lanean, Floridako Unibertsitate Internazionaleko (FIU) tailerretan eta trebakuntza-saioetan parte hartuz; orduan RETINAn (Red Teleinformática Académica) egiten zuen lan, eta sare nazionalean IPv6-ren hedapena sendotzen lagundu zuen.

IPv6-ri buruzko trebakuntza-saio asko eman ditu Argentinako unibertsitateetan, zerbitzu-hornitzaileetan eta beste erakunde batzuetan (adibidez, NAP CABASEn). Gai horri buruzko hitzaldiak ere eman ditu Latinoamerikan.

2006tik, IPv6-ri buruzko Latinoamerikako Foroko eta Latinoamerikako eta Karibeko Task Forceko IPv6-ko koordinatzailea da.

Gaur egun, unibertsitateko interkonexio-sareko koordinatzaile teknikoa da (Red de Interconexión Universitaria). Han, Argentinako Unibertsitate Nazionalen sarean teknologia berriak hedatzen laguntzen du.

César Olvera Morales

Mexikoko Unibertsitate Nazional Autonomoan (UNAM) lizentziatutako fisikaria da. 1998tik 2002ra DGSCA-UNAMen aritu zen lanean, Interoperabilitate Laborategiko koordinatzaile gisa; hango lanak ziren IPv6, QoS, Multicast, MPLS eta abarri buruzko ikerketak eta probak egitea, gai horiei buruzko hitzaldiak, batzarrak eta mintegiak antolatzea, eta ekitaldi nazionaletan eta internazionaletan hizlari izatea. 2002an, Consulintelen hasi zen lanean; han, hainbat IST eta PROFIT proiektutan hartu zuen parte, IPv6 sareei buruzko ikerketak eta probak egiten, eta sare horiek diseinatzen eta instalatzen, batez ere bideratzea, PLC, QoS, Multicast, MPLS, VPN, segurtasuna eta antzeko alderdien ikuspegitik. ETSI, IPv6 Forum, Spirent, Agilent, Ixia eta abarrekin lankidetzan aritu da —IPv6 gailuen interoperabilitate, egokitasun eta prestazioen diseinua eta probak egiten—, baita IETFko IPv6-ri buruzko lan-taldeekin ere. IPv6-ri buruzko trebakuntza-saioak eman ditu Latinoamerikan eta Afrikan.

Jordi Palet Martínez

Ordenagailuekin, sareekin eta telekomunikazioekin lan egin du azken 25 urteetan, eta, gaur egun, Consulinteleko Zuzendari Nagusia eta Zuzendari Teknikoa da. Esperientzia du hizkuntza askotan programatzen, sistema eragileen migrazioak egiten, zirkuitu elektronikoak eta mikrokonputagailuak diseinatzen, aholkularitzan, eta sareak ezartzen eta diseinatzen. Urteak dira IETF, ISOC, IPv6 Forum, IPv6 Cluster, IPv6 Task Force eta RIRekin lankidetzan aritzen dela; askotan ematen ditu IPv6-ri buruzko trebakuntza-tailerrak mundu osoan, eta IPv6-ri buruzko artikulu, liburu eta dokumentu ugari idatzi ditu. Ikerketa, garapen eta berrikuntzako proiektu askotan hartu du parte (baita zuzendu ere), eta horietako gehienek zerikusia dute IPv6-rekin (6SOS, Autotrans, Euro6IX, Eurov6, 6POWER, 6QM, 6LINK, ENABLE, RiNG eta PlaNetS). IPv6-rekin ez ezik, PLC/BPL-rekin, IP mugikortasunarekin, segurtasunarekin eta bideratzearekin zerikusia duten teknologiekin ere lan egin du. Ohiko hizlaria da IPv6-rekin erlazionatutako hitzaldi eta ekitaldietan, eta batzorde askotako kidea da (besteak beste, FLIP6-ko ebaluazio-batzordekoa, sortu zenetik). AfriNIC, APNIC, ARIN eta LACNICekin lankidetzan aritzen da, IPv6-ri buruzko dibulgazioan eta trebakuntzan.

Álvaro Vives Martínez

Telekomunikazioetako goi-mailako ingeniaria da, telematikan espezializatua (Vigoko Unibertsitatea). Unibertsitate horretan, Europako I+G-ko proiektu batean hartu zuen parte, zeina TB digitalarekin eta Top-Box DVB-MHP multzo baten garapenarekin erlazionatua baitzegoen; irakasle gonbidatu gisa ere aritu zen. Ondoren, 2002an, Consulintelen hasi zen lanean. Consulintelen, IPv6-rekin erlazionatutako I+G-ko proiektu askotan hartu du parte, Espainia mailan eta Europa mailan (6SOS, Euro6IX, 6POWER, 6QM, Eurov6, ENABLE, RiNG eta 6DEPLOY). IPv6-rekin erlazionatutako lan asko egin ditu: bere gain izan ditu produkzio-zerbitzuak (besteak beste, DNS, http eta FTP), sareak kudeatu ditu, aplikazioak garatu ditu, ikastaroak eta hitzaldiak eman ditu, aholkularitza-proiektuetan lan egin du (Europan, Latinoamerikan eta Afrikan), eta IETF estandarizatzeko lanak egin ditu.

1. Sarrera

1.1. Gaur egungo egoera

Gauza jakina da oraindik IANAk (www.iana.net) kudeatzen dituen eta Eskualdeko Internet Erregistroei esleitu ez zaizkien IPv4 helbideen multzoa abiadura handian murrizten ari dela eta laster ahituko dela. Beste hitz batzuetan esateko, Interneteko helbideen sistema orokorra agortzen ari da.

Gaur egungo protokoloak (Internet protokoloaren 4. bertsio edo IPv4-k) lau mila milioi helbide inguru ditu, eta, Internetek izan duen arrakastaren ondorioz, datozen urteetan agortu egingo direla uste da.

Argi dago esleitutzat jotzen diren IPv4 helbide asko ez direla erabiltzen, zenbait arrazoi tarteko. Pentsatu izan da Internet Protokoloaren bertsio berri bat martxan jarri beharrik gabe erantzun geniezaiokeela IP helbideen eskariari —eta oraindik ere batzuek hala uste dute—, eta hori lor zitekeela, hain zuzen, IPv4 helbideen erabilera optimizatuz, erabiltzen ez diren helbideak berreskuratuz eta NAT erako teknologien erabilera zabalduz (NAT: Network Address Translation edo Sareko Helbideen Itzulpena).

Ideia hori pixkanaka hutsaltzen joan da; Internetera konektatzeko beren IP helbideak beharko dituzten gailuen kopurua, epe ertainean, oso handia da, eta horietako askok helbide bat baino gehiago ere beharko dute. Hala, IP helbideak eraginkorrago erabilita ere, IPv4 protokoloak ematen dituen lau mila milioi helbide pasatxo horiek ez dira nahikoa izango.

Bestalde, NATi esker orain arte Internet hazi egin den arren, nabarmentzekoa da sistema horrekin muturretik muturrerako konektagarritasuna galdu egiten dela, eta, beraz, NATek muturretik muturrerako (edo bezerotik bezerorako) aplikazioak eta zerbitzuak zabaltzea zaildu egiten duela; ondorioz, zerbitzu eta aplikazio horiek garatzea konplexuagoa eta garestiagoa da, eta, finean, NATek sareko berrikuntza oztopatzen du.

IPv6 protokolo berriak 340 trilioi trilioi (sextilioi) helbide dauzka; horren ondoan, IPv4-ren helbide kopurua hutsala da. Helbide-espazio handi horri esker, IPv6-k zenbait abantaila ditu bai egonkortasunean, bai malgutasunean eta bai sare-administrazioaren erraztasunean. Gainera, baliteke «IPv6-ren garaiak» aplikazioen eta zerbitzu-eskaintzen berrikuntza-bolada bat sortzea, atzean uzten baitu helbideak partekatu beharra.

IPv6 pixkanaka ezartzen ari dira sareetan, eta, trantsizio horretan, urte askoz arituko da IPv4-rekin batera. Protokoloarekin erlazionatutako lan teknikoa neurri handi batean dagoeneko egina badago ere, Interneteko zerbitzuen hornitzaileen sareetan zabaltzea falta da, batez ere.

1.2. Latinoamerikan eta Karibean, bide onetik

IPv6 gureganatzeko eta sustatzeko bidea luzea izan da, baina inoiz ere ez zaio bide horretan aurrera egiteari utzi.

Adibidez, 2005. urtean, LACNICek (Latinoamerikako eta Karibeko Helbideen Erregistroak) IPv6 Tour ekitaldia antolatu zuen lehenengoz; orduan, hamar jardunaldi egin ziren eskualdeko hamar herrialdetan. Jardunaldi horietan, 3.500 lagun inguruk hartu zuen parte. «Ebanjelizazio-jardunaldiak» izan ziren, parte-hartzaileek inolako ezagutzarik ez zutela jo baitzen. Lau urte geroago, egoera oso bestelako da.

LACNICek, bere baliabideak erabiliz eta 6DEPLOY proiektuko beste bazkide batzuen laguntzaz (Europako Batzordeak diruz lagundutako proiektu bat da hori), trebatze-jarduerak antolatu ditu dozena bat herrialdetan baino gehiagotan, eta 800 lagunek baino gehiagok parte hartu du trebakuntza horietan. Gaur egun antolatzen diren jardueren eta hasieran antolatutakoen artean alde handia dago. Orain ez dago IPv6 zer den azaldu beharrik. Aitzitik, IPv6-ren ezarpenaren alderdi praktikoak lantzen dira tailerretan. Tailer horietatik, lagun asko prestatua ateratzen da beren erakundeetan IP protokoloaren bertsio berriaren ezarpen-planak egiteko eta LACNICi helbideak eskatzeko. Makina hori martxan dago dagoeneko.

Gaur egun, badaude trukaguneak (IXPak) Latinoamerikako eta Karibeko sei herrialdetan gutxienez, eta beren azpiegituretan IPv6-rekiko zerbitzuak barneraturik dituzte. Herrialdeentzako goi-mailako domeinuen (ccTLD edo country codes Top Level Domains-en) % 75ek IPv6-ren egituran oinarrituta ebazten du bere herrialdeko domeinuen DNSa, zerbitzari primario eta/edo sekundario baten edo gehiagoren bidez.

2009ko lehen bederatzi hilabeteetan, Latinoamerikako eta Karibeko 60 erakundek baino gehiagok jaso dituzte dagozkien IPv6 helbideen blokeak; horrek alde handiz gainditzen du 2008 osoan LACNICek eta Mexikoko eta Brasilgo erregistro nazionalek guztira egindako 47 esleipenak.

Operadore batzuek dagoeneko IPv6-n oinarrituta ematen diete zerbitzua bezeroei. Hala, IPv6-rako trantsizio-bidean irmo aurreratzen ari garela erakusten duten gertaera eta adierazleen zerrenda egiten jarraitu dezakegu.

Gobernuetako foroetan ere asko aurreratu da. IPv6-ri buruzko gaiak ohikoak dira erakunde askoren agendetan —CITEL (Comisión Interamericana de Telecomunicaciones),

CTU (Caribbean Telecommunication Union) eta beste gobernu-foro batzuk—, eta, gainera, gobernuek IPv6 sustatzeko eta beren azpiegituretan protokolo berria ezartzeko hartu duten konpromisoa islatzen dute ebazpen batzuek.

Nahikoa da hori? Inondik inora ez. Baina, lehenago esan dugunez, badirudi elementu horiek norabide egokian bideratuak daudela.

Gaur egun, IPv4 helbideen % 10 besterik ez da gelditzen IANAk kudeatzen duen biltegi nagusian. Hori horrela, argi dago bizkorrago ibili behar dugula eta kemen handiagoz ekin behar diogula hartutako bideari. Izan ere, berehala egiten ez dugunak kostu handiagoak ekarriko dizkigu gero.

Erakunde batzuen lanak —hala nola LACNICenak eta ISOC edo Internet Societyrenak— funtsezko ekarpena egiten du IPv6-ren trantsizioak izan ditzakeen ondorio negatiboak arintze aldera. Azken finean, IPv6 ezinbestekoa da Interneten iraupen, egonkortasun eta bilakaerarako.

IPv6 nonahi baliatzeko gidaliburuaren asmoa ohiko inguruneetan IPv6-ren erabilera sustatzea da. Horretarako, ezagutza eta esperientzia partekatzen ditu, beste jende eta erakunde batzuek epe laburrean emaitzak lor ditzaten eta prozesu hau gauzatu ahal izan dezaten. ***IPv6 nonahi baliatzeko gidaliburu***an, konfigurazioaren adibide praktikoak daude, irakurleek protokolo berriaren erabilera benetako konfigurazio-ereduei jarraituz landu dezaten.

1.3. Zer da ISOC?

Internet Society (ISOC) nazioarteko erakunde independente bat da, irabazi-asmorik gabea; bulegoak Genevan (Suitza) eta Restonen (Virginia, Estatu Batuak) ditu. Interneti buruzko informazio teknikoki fidagarri eta objektiboaren truke globalerako zentroa, hezkuntza-hornitzailea eta Internetekin erlazionatuak dauden mundu osoko ekimenen bideratzaile eta koordinatzailea da ISOC. IETF (Internet Engineering Task Force), IAB (Internet Architecture Board) eta IRTF (Internet Research Task Force) erakundeen antolakuntzaren oinarria da.

ISOC 1992an sortu zen, Internetekin erlazionatutako estandarretan, hezkuntzan eta politiketan aitzindari izateko. Mundu mailako kide-sare aktibo baten laguntza du, zeinak laguntzen baitu Interneteko komunitate osoan eta mundu guztian ISOCen eginkizuna sustatzen eta lortzen. Elkarteak 80 kide instituzional eta 28.000 banakako kide baino gehiago ditu 80 ataletan baino gehiagotan, eta ISOCen teknologiako, hezkuntzako eta politikako ekimenen irismena eskualdeetaraino helarazten laguntzen dute horiek guztiek.

Hau da Internet Societyren webgunea: http://www.isoc.org.

1.4. Internet Societyren Argentina atala

Internet Societyren atalak ingurune geografiko jakin batean bizi diren pertsonek osatutako taldeak dira (adibidez, hiri batean edo herrialde batean), edo, bestela, Internetekin erlazionatutako gai jakin baten inguruko interesa duten pertsonek osatutakoak. Taldekide horiek beren borondatez antolatzen dira, eta, ISOCeko kide gisa, erakundearen xede eta printzipioekin bat datozen jarduerak egiten dituzte.

Argentinan, ISOCen Argentina atala (ISOC-Ar) irabazi-asmorik gabeko erakunde zibil bat da, independentea eta demokratikoa, Asociación Civil de Argentinos en Internet erakundearen esparruan lan egiten duena. 1999an sortu zen, eta pertsona juridiko gisa erregistratzea lortu du IGJ 297/2000 ebazpenaren bidez. Haren helburua da Internet sarearen eta Interneteko zerbitzuen eta edukien garapen irekia eta bilakaera lortzea, jende guztiaren mesederako, eta bereziki Argentinako Errepublikako biztanleen mesederako, besteak beste,. Horretarako, Interneteko mundu osoko komunitatearen jarduerak sustatzen ditu, eta, bereziki, Argentinan bizi diren Internet Societyko kideen arteko komunikazio estua eta hurbilketa bultzatzen du.

Internet Societyren xede eta helburuekin bat eginez, ISOC-Ar erakundeko kideok printzipio gidariak finkatzera bideratutako zenbait jarduera egin dugu. Adibidez, 2007tik, minusbaliotasunak dituzten pertsonentzako trabarik gabeko sare baten aldeko irisgarritasun-jardunaldiak antolatzen ditugu. Jardunaldi horietan, desgaitasunen bat dutenek Internet erabiltzeko dituzten oztopoen inguruko gaiak azaltzen eta eztabaidatzen ditugu, baita oztopo horiek gainditzen laguntzen duten eta indarrean dauden jardunbide egokiak ikusi ere. Beste ekintza eta mintegi batzuetan ere parte hartzen dugu, Internet Societyk diruz lagundutako proiektuak gauzatzen ditugu, eta, adibidez, 2008ko azaroan egindako Erabilgarritasunaren Eguna antolatu genuen.

1.4.1. Community Grants Programme (Komunitatearentzako Diru-laguntzen Programa)

ISOCek bere kide eta atalen artean sustatzen dituen jarduera bat da Komunitatearentzako Diru-laguntzen Programa.

Programa horrek diru-laguntza ematen du, honako helburu hauek lortzeko asmoa duten proiektuak garatu ahal izan daitezen:

- ISOCen xedea eta helburuak hobetzea (bereziki, ISOCen ekimen estrategikoekin eta printzipioekin bat badatoz);
- Ataletako komunitateei zerbitzuak eskaintzea;
- Atalen edo banakako kideen arteko lankidetza sustatzea;
- Interneteko komunitate osoan partekatzen den ezagutza hobetzea eta erabiltzea; eta
- Atalen iraunkortasuna eta garrantzia suspertzea.

1.4.2. *IPv6 nonahi baliatzeko gidaliburua* proiektua

Liburu hau Interneteko komunitateari, tokikoari eta globalari, tresna batzuk emateko egin dugu, IPv6 nonahi sustatu eta ezarri ahal izan dadin, baina baita IPv6 berandu ezartzeak sortzen digun kezkak eraginda ere.

IPv6 nonahi baliatzeko gidaliburuan, kapituluak ingurune jakinei begira idatziak daude. Hala, argi asko eta alferrikako termino teknikorik gabe azaltzen dira IP protokoloaren bertsio berria konfiguratzeko eta ezartzeko jarraitu beharreko urratsak, askotariko esparrutarako: bizitokietako sareak, sare akademikoak, enpresak, Interneteko zerbitzu -hornitzaileak (Internet Service Providers edo ISPak), azken erabiltzaileak eta zerbitzuak.

Proiektu hau Internet Societyri esker burutu dugu, zeinak ISOC-Ar atalean urte batzuk lehenagotik lantzen ari ginen ideia bat gauzatzeko aukera eman baitigu. Liburu hau egiteko, gaiaren inguruko bertako eta nazioarteko adituen laguntza izan dugu. Beren esperientzia eta jakinduriarekin, IPv6 ezartzeko bide luze baina saihestezina egiten lagundu digute.

Mónica Abalo Laforgia
Internet Societyren Argentina ataleko lehendakaria

Sebastián Bellagamba
Internet Societyren Latinoamerikarako
eta Kariberako eskualdeko bulegoko zuzendaria

Raúl Echeberría
LACNICeko zuzendari exekutiboa
Internet Societyko zuzendari-batzordeko kidea

2. Azken erabiltzailea

1. Sarrera

Kapitulu honetan, azken erabiltzaileentzako zenbait plataformatan (zenbait sistema eragiletan) IPv6-ren oinarrizko instalazioa eta konfigurazioa egiteko hastapenak azaltzen dira.

Sistema eragile hauek hartu dira kontuan:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 2000
- Mac OS X
- Linux
- BSD

Kasu batzuetan bertsio asko direnez —batez ere Linuxen eta BSDn—, adibide generikoak jarri ditugu, eta, horregatik, baliteke bertsio jakinen batean gure adibidearekiko desberdintasunak izatea. Desberdintasun horiek irakurleak ebatzi beharko ditu, eskuartean duen sistema eragileari buruzko dokumentazioaren laguntzaz.

2. IPv6-ren instalazioa

2001etik aurrerako sistema eragile gehienek onartzen dute, nolabait, IPv6.

Batzuetan, berez, ez dute IPv6-rako software «komertzialik», baizik eta probako bertsioren bat soilik, merkaturatutako bertsioetan sartua.

Adibidez, IPv6-ren softwarearekin hori gertatzen da Windows 2000n (baita Windows NTren bertsio zaharragoetan ere, zeinak ez baititugu dokumentu honetan deskribatuko, zaharregiak direlako), eta Windows XPren lehen bertsioan ere bai (alegia, Service Pack 1 edo SP1 atera aurreko bertsioan).

Gero eta ohikoagoa da, plataformek edo sistema eragileek IPv6 sartzea ez ezik, fabrikatzaileek IPv6 lehenestea ere, eta erabiltzaileek deus ere egin behar ez izatea.

Azaldutakoak mahaigaineko ordenagailuetarako eta ordenagailu eramangarrietarako balio du, baina baita sistema eragile horiek berak edo horien bertsio murriztuak erabiltzen dituzten beste gailuetarako ere, hala nola telefono mugikorretarako, agenda elektronikoetarako, jolaserako plataformetarako eta abarretarako. Batzuetan, bistan da, sistema eragileen bertsio murriztuek ez dituzte jatorrizko sistema eragilearen funtzio guztiak, eta, beraz, baliteke IPv6 konfiguratzeko eta probatzeko funtzioak (hemen ikusiko ditugunak) ezin atzitu izatea.

2.1. IPv6-ren instalazioa Windowsen

IPv6-ren pila osatuenetakoa Windows plataforma berrienetan dago:

- Windows XP SP1 eta berriagoak
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Lehenago esan dugunez, Windows plataforma batzuetan probako garapena (Technology Preview) besterik ez zegon. Horregatik, plataforma horietan, funtzioak mugatuak dira, eta ez dute fabrikatzailearen laguntza teknikorik:

- Windows XP, SPrik gabea
- Windows 2000, SP1 bitartekoa (SP1 barne)

Badago Windows NT 4.0ko garatzaileentzako bertsio bat ere, baina dokumentu honetan ez dugu horren xehetasunik emango.

Azkenik, hirugarrenek sistema eragile hauentzako IPv6 softwareak egin dituzte, baina ez dute Microsoften laguntza teknikorik:

- Windows 95/98/ME
- Windows 2000 SP2 eta berriagoak

Oro har, sistema eragile horiek ezaugarri hauek onartzen dituzte, nahiz eta ezaugarri batzuk bertsio berrienetan soilik onartzen diren:

- Konfigurazio automatikoa
- 6in4 tunelak
- 6to4 tunelak
- 6to4 errelea (*relay*)
- TEREDO tunelak
- ISATAP tunelak
- IPsec (eskuzko gakoak)

2.1.1. XPko edo 2003ko instalazioa

Esan liteke, berez, bai Windows XPn bai Windows Serverren IPv6 instalatua dagoela eta, beraz, instalatu ez, baizik eta aktibatu egiten dugula.

Bi plataforma horietan, IPv6 aktibatzeko bi era daude:

2.1.1.1. Komando-lerroa

DOS leihoan, exekutatu hau: **`ipv6 install`**

Segundo batzuen ondoren, mezu batek instalazioa behar bezala egin dela adierazten du.

Bertsioaren arabera, beste komando hau erabil daiteke: **`netsh interface ipv6 install`**

2.1.1.2. Interfaze grafikoa

Ingurune grafikoaren edo kontrol-panelaren bidez, bilatu Sare-konexioak, jarri IPv6 gaitu nahi zaion sare lokalaren edo haririk gabeko sare lokalaren gainean, egin klik saguaren eskuin-botoiarekin, eta hautatu Propietateak aukera. Sakatu Instalatu eta Protokoloa aukerak. Azkenik, aukeratu «Microsoft TCP/IP version 6».

Emaitza pantaila-argazki honen antzekoa izango da:

1. IRUDIA. **IPv6-REN INSTALAZIOA, XPN EDO 2003N. PANTAILA-ARGAZKIA**

2.1.2. Vistako instalazioa

Windows Vistak IPv6-ren softwarea instalatua eta lehenespenez gaitua du, merkaturatu zutenetik.

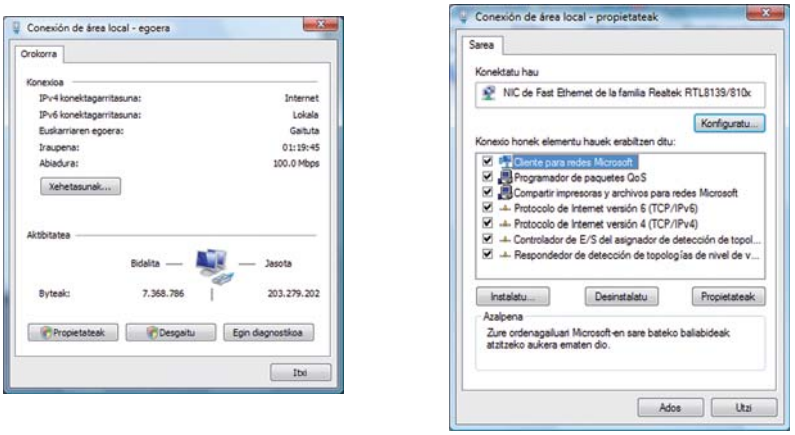
Beraz, ez da beste konfiguraziorik egin behar. Dena den, desgaituz gero, Windows XPko eta 2003ko netsh-i edo ingurune grafikoari dagokienez azaldu dugun bezala aktibatzen da.

Kontuan izan netsh erabiltzeko DOS leiho bat berariaz irekia izan behar dugula, administratzaile-baimen eta guzti.

XPrekin edo 2003ren aldean, Vistak funtzio gehiago ditu; besteak beste, hauek:

- IPsec pila osoa
- MLDv2
- Link-Local Multicast Name Resolution (LLMNR)
  - Ez du DNS zerbitzaririk behar. Segmentu bateko IPv6 nodoek multicast IPv6 helbide bati eskatzen diote izena. NetBIOSen funtzionamenduaren antzekoa.
- URLetan IPv6 helbideak erabiltzea onartzen du
- IPv6 Control Protocol (IPV6CP - RFC5072)
- PPP gaineko IPv6
- DHCPv6, bezeroan eta zerbitzarian
- Ausazko interfaze-identifikadorea, lehenespenez (RFC3041)
- Teredok NAT simetrikoak onartzen ditu
  - Lehenespenez, gaitua. Soilik erabiltzen da aplikazioak IPv6 onartzea behar badu eta jatorriz erabilgarri ez badago.

Instalatua dagoen egiaztatzeko, bai komandoak eta bai ingurune grafikoa erabil daitezke, XPn egiten den bezalatsu:



2. IRUDIA. **SARE-KONEXIOAREN PROPIETATEAK ETA IPV6-REN INSTALAZIOA, VISTAN**

2.1.3. Windows 7ko instalazioa

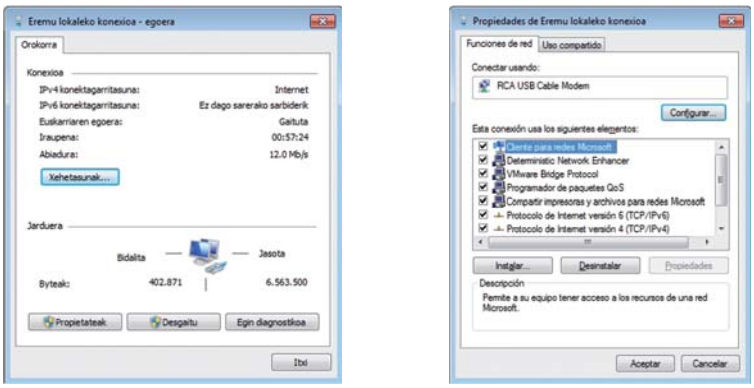
Windows 7k IPv6 instalatua eta lehenespenez gaitua izaten du, Vistak eta 2008k bezalaxe. Dena den, desgaituz gero, Windows XP edo 2003ko netsh-i edo ingurune grafikoari dagokienez azaldu dugun bezala aktibatzen da.

Kontuan izan netsh erabiltzeko DOS leiho bat berariaz irekia izan behar dugula, administratzaile-baimen eta guzti.

Hauek dira bertsio honen ezaugarriak:

- IPv6 onartzen du, Vistak eta Server 2008k egiten duten antzera
  - IPsec, MLDv2, LLMNR, IPv6 URLetan, IPV6CP, PPP gaineko IPv6, DHCPv6, Teredo
  - Hau, berriz, ez da berdina: ausazko interfaze-identifikadorea, lehenespenez (RFC3041)
    - Automatikoki konfiguratutako helbideetan, interfaze-identifikatzaileari dagokionez, ez du EUI-64 lehenespenez erabiltzen.
- Hobekuntza berriak:
  - IP-HTTPS (HTTP seguruaren gaineko IP)
    - Ostalariei aukera ematen die proxy zerbitzari bat edo suebaki bat zeharkatzeko, eta HTTPS tunel baten barruan IPv6 bidez sare pribatuekin konektatzeko. HTTPSk ez du datuen segurtasuna bermatzen, eta IPsec erabili beharra dago, IP-HTTPS konexioa segurua izan dadin. Informazio gehiago dago hemen: *http://msdn.microsoft.com/en-us/library/dd358571.aspx*.
  - DirectAccess
    - Sare korporatibora modu gardenean konektatzeko aukera ematen die erabiltzaileei, horretarako VPN konexio bat berariaz ezarri behar izan gabe. Bestalde, sare-administratzaileari bulegotik kanpoko ostalari mugikorrekin kontaktuan segitzeko aukera ematen dio, ordenagailu horietan eguneraketak eta mantentze-lanak egin ahal izan ditzan. Arkitektura horretan, IPv6-ren bezero bat sare korporatiboko IPv6-ren zerbitzari batekin komunikatzen da. IPv4-ko Internetetik ere egin daitezke konexioak, 6to4, Teredo eta ISATAP erabiliz. IP-HTTPS erabil daiteke. DirectAccessek IPsec tunelak erabiltzen ditu autentifikazioan eta baliabideetarako sarbidean segurtasuna bermatzeko.
    - Bezeroa Windows 7 edo Server 2008 izan daiteke. Zerbitzaria Server 2008 izan daiteke.

Vistaren kasuan bezala, ingurune grafikoa erabiliz begiratu daiteke instalatua dagoen:



3. IRUDIA. **SARE-KONEXIOAREN PROPIETATEAK ETA IPV6-REN INSTALAZIOA, WINDOWS 7N**

2.1.4. Windows 2000ko instalazioa

Windows 2000n IPv6-ren pila ahalik eta modu fidagarrienean instalatzeko, IPv6-ren pilari dagokion kodea deskargatu behar da lehendabizi, orain arte azaldutako kasuetan ez bezala, fabrikatzaileak ez baitu aurrez instalatzen.

Microsoftek ez du Windows 2000ko IPv6-ri buruzko laguntza teknikorik ematen, garatzen ari ziren bertsio bat besterik ez delako.

Beraz, lehenik eta behin, Microsoft IPv6 Technology Preview for Windows 2000 deskargatu behar dugu:

- tpipv6-001205-SP2-IE6, SP1erako eta SP2rako
- tpipv6-001205-SP3-IE6, SP3rako
- tpipv6-001205-SP4-IE6, SP4rako

Denak ala denak, hemen eskuratu daitezke:
http://www.sixxs.net/faq/connectivity/?faq=ossetup&os=windows

Deskargatu ondoren, honela egiten da instalazioa:

- Sartu sisteman, administratzaile-pribilegio lokalak dituen erabiltzaile gisa
- Atera IPv6 Technology Previewren fitxategiak, adibidez, C:\IPv6Kit helbidera
- Jarraitu SPn & IE6 fixed.txt fitxategiko prozedurari, fitxategia/setup/hotfix.ini aldatzeko
- Exekutatu setup.exe edo hotfix.exe
- Windows 2000ko mahaigainean, sakatu Hasi botoia, Ezarpenak aukera, eta Sarekonexioak. Eskuineko botoiarekin egin klik Sarekoak aukeran, eta, ondoren, sakatu Propietateak
- Egin klik eskuin-botoiarekin IPv6 protokoloa erantsi nahi zaien Etherneten oinarritutako konexioetan, eta, ondoren, sakatu Propietateak. Normalean, konexio horri *sare lokaleko konexio* deritzo

- Sakatu Instalatu
- Sareko osagai motaren elkarrizketa-koadroan, egin klik Protokoloan, eta, ondoren, Gehitun.
- Sareko protokoloa hautatzeko elkarrizketa-koadroan, egin klik Microsoft IPv6 Protocol aukeran, eta, ondoren, Ados botoian
- Itxi sare lokaleko konexioen propietateen elkarrizketa-koadroa.

2.2. IPv6-ren instalazioa Mac OS Xn

Applek IPv6 onartzen du Mac OS Xren 10.2 (Jaguar) bertsiotik aurrera, eta lehenespenez gaitua dago.

Beraz, instalatzeko, ez da deus ere egin beharrik.

2.3. IPv6-ren instalazioa Linuxen

Kernelen 2.4.x bertsiotik aurrera, IPv6 onartua dago.

Instalatua dagoen jakiteko:

```
#test -f /proc/net/if_inet6 && echo "Kernel honek IPv6 onartzen du"
```


IPv6-ren modulua instalatzeko:

```
#modprobe ipv6
```

Modulua badagoela egiaztatzeko:

```
#lsmod |grep -w 'ipv6' && echo "IPv6 modulua kargatua dago"
```

Moduluaren karga/deskarga automatikoa ere konfiguratu daiteke (/etc/modules.conf edo /etc/conf.modules):

```
alias net-pf-10 ipv6 #eskatzean kargatzea gaitzen du
alias net-pf-10 off #eskatzean kargatzea desgaitzen du
```

Konfigurazio iraunkorra egin daiteke, Linuxen bertsioaren arabera.

2.3.1. Konfigurazio iraunkorra Red Hat (7.1 bertsioa edo berriagoa) eta antzekoetan

Gehitu hau /etc/sysconfig/network-i:

```
NETWORKING_IPV6=yes
```

Berrabiarazi sarea:

```
# service network restart
```

Edo

```
#/etc/init.d/network restart
```

2.3.2. Konfigurazio iraunkorra SUSEn

Beheko lerro bat gehitu behar zaio honi: /etc/sysconfig/network/ifcfg-<Interface-Name>

```
SUSE 8.0: IP6ADDR="<ipv6-address>/<prefix>"
SUSE 8.1: IPADDR="<ipv6-address>/<prefix>"
```

2.3.3. Konfigurazio iraunkorra DEBIANen

IPv6 modulua kargatua dagoenean, /etc/network/interfaces editatu behar da; adibidez:

```
iface eth0 inet6 static
  pre-up modprobe ipv6
  address 2001:DB8:1234:5::1:1
  # Guztiz ezabatzen du konfigurazio automatikoa:
  # up echo 0 > /proc/sys/net/ipv6/conf/all/autoconf netmask 64
  # Bideratzailea automatikoki konfiguratua dago, eta ez du
    helbide finkorik.
  # Honi esker aurkitzen da:
  # (/proc/sys/net/ipv6/conf/all/accept _ ra).
  # Bestela, GW konfiguratu behar da:
  # gateway 2001:DB8:1234:5::1
```


Berrabiarazi egin behar da, edo:

```
# ifup --force eth0
```

2.4. IPv6-ren instalazioa BSDn

BSDren 4.5 bertsioak eta berriagoek IPv6 onartzen dute.

Oso software ona da, eta pila aldez aurretik instalatua dago. Beraz, ez da besterik egin behar.

3. IPv6-ren instalazioa egiaztatzea

IPv6 instalatu ondoren, modu bat edo gehiago ditugu instalazio hori behar bezala egin dela egiaztatzeko eta sare lokalean nahiz beste IPv6 sare batzuekin konektagarritasunik badugun ikusteko (plataformaren arabera).

3.1. Egiaztapena Windowsen

Ingurune grafikoaren bidez egiazta dezakegu IPv6-ren pila instalatu den (instalazioaren atalean azaldu dugu hori nola egiten den), baina ipconfig komandoa edo ipv6 if ere erabil dezakegu egiaztapena egiteko (Windowsen azken bertsioetan ez dago).

Interfazeen IPv6-ren konfigurazioari buruzko informazioa ematen digu ipconfig komandoak, eta IPv4-renari buruzkoa ere bai; ipv6 if komandoak, berriz, IPv6-ri buruzko informazioa soilik erakusten du.

Adibidez, gure Ethernet interfazea 5.a balitz (hori ordenagailu bakoitzaren hardwarearen araberakoa da), **ipv6 if 5** komandoaren emaitza honen antzekoa izango litzateke:

```
Interface 5: Ethernet: Local Area Connection
  Guid {F5149413-6E54-4FDA-87BD-24067735E363}
  uses Neighbor Discovery
  uses Router Discovery
  link-layer address: 00-01-4a-18-26-c7
  preferred global 2001:db8::fde7:a76f:62d5:3bb9, life
    6d21h3m20s/21h33s (temporary)
  preferred global 2001:db8::201:4aff:fe18:26c7, life
    29d23h51m39s/6d23h51m39s (public)
  preferred link-local fe80::201:4aff:fe18:26c7, life infinite
  multicast interface-local ff01::1, 1 refs, not reportable
  multicast link-local ff02::1, 1 refs, not reportable
  multicast link-local ff02::1:ff18:26c7, 2 refs, last reporter
  multicast link-local ff02::1:ffd5:3bb9, 1 refs, last reporter
  multicast link-local ff02::1:ff00:4, 1 refs, last reporter
  multicast link-local ff02::1:ff00:2, 1 refs, last reporter
  link MTU 1500 (true link MTU 1500)
  current hop limit 64
  reachable time 29000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1
  default site prefix length 48
```

Eta ipconfig komandoaren emaitza, berriz, honen antzekoa izango litzateke:

```
Configuración IP de Windows

  Adaptador Ethernet Publica:
    Sufijo conexión específica DNS :
    Dirección IP . . . . . . . . . . . . . : 10.10.10.250
    Máscara de subred. . . . . . . . . . . : 255.255.255.0
    Dirección IP . . . . . . . . . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
    Dirección IP . . . . . . . . . . . . . : fe80::200:1cff:feb5:c535%4
    Puerta de enlace predet . . . . . . . : 10.10.10.1

  Adaptador de túnel Consulintel:
    Sufijo conexión específica DNS :
    Dirección IP . . . . . . . . . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
    Dirección IP . . . . . . . . . . . . . : fe80::5:a0a:afa%5
    Puerta de enlace predet . . . . . : 2a01:48:20::d5ac:227d
```

```
Adaptador de túnel Automatic Tunneling Pseudo-Interface:
  Sufijo conexión específica DNS:
  Dirección IP . . . . . . . . . . . . . . : fe80::5efe:10.10.10.250%2
  Puerta de enlace predet . . . . . :
```

Eta **ipconfig /all** erabiltzen bada:

```
Configuración IP de Windows
  Nombre del host . . . . . . . . . . . . : dns1
  Sufijo DNS principal . . . . . . . . . : consulintel.com
  Tipo de nodo . . . . . . . . . . . . . . : difusión
  Enrutamiento IP habilitado . . : S
  Proxy de WINS habilitado . . . . : S
  Lista de búsqueda sufijo DNS . : consulintel.com

Adaptador Ethernet Pública:
  Sufijo conexión específica DNS:
  Descripción . . . . . . . . . . . . . . : Adaptador Fast Ethernet PCI
  basado en Intel (Genérico)
  Dirección física . . . . . . . . . . . : 00-00-1C-B5-C5-35
  DHCP habilitado . . . . . . . . . . . . : No
  Dirección IP . . . . . . . . . . . . . . : 10.10.10.250
  Máscara de subred . . . . . . . . . . . : 255.255.255.0
  Dirección IP . . . . . . . . . . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
  Dirección IP . . . . . . . . . . . . . . : fe80::200:1cff:feb5:c535%4
  Puerta de enlace predet . . . . . : 10.10.10.1
  Servidores DNS . . . . . . . . . . . . : 80.58.0.33
                                    80.58.32.97
                                    10.10.10.250
                                    fec0:0:0:ffff::1%1
                                    fec0:0:0:ffff::2%1
                                    fec0:0:0:ffff::3%1

Adaptador de túnel Consulintel:
  Sufijo conexión específica DNS:
  Descripción . . . . . . . . . . . . . . : Configured Tunnel Interface
  Dirección física . . . . . . . . . . . : 0A-0A-0A-FA
  DHCP habilitado . . . . . . . . . . . . : No
  Dirección IP . . . . . . . . . . . . . . : 2a01:48:20:0:200:1cff:feb5:c535
  Dirección IP . . . . . . . . . . . . . . : fe80::5:a0a:afa%5
  Puerta de enlace predet . . . . . : 2a01:48:20::d5ac:227d
  Servidores DNS . . . . . . . . . . . . : fec0:0:0:ffff::1%2
                                    fec0:0:0:ffff::2%2
                                    fec0:0:0:ffff::3%2
  NetBios sobre TCPIP . . . . . . . . . : Deshabilitado
```

```
Adaptador de túnel Automatic Tunneling Pseudo-Interface:
  Sufijo conexión específica DNS:
  Descripción. . . . . . . . . . . . . . . : Automatic Tunneling Pseudo-
  Interface
  Dirección física . . . . . . . . . . . : 0A-0A-0A-FA
  DHCP habilitado . . . . . . . . . . . . : No
  Dirección IP . . . . . . . . . . . . . . : fe80::5efe:10.10.10.250%2
  Puerta de enlace predet . . . . . :
  Servidores DNS . . . . . . . . . . . . : fec0:0:0:ffff::1%1
   . . . . . . . . . . . . . . . . . . . . . . . fec0:0:0:ffff::2%1
   . . . . . . . . . . . . . . . . . . . . . . . fec0:0:0:ffff::3%1
  NetBios sobre TCPIP . . . . . . . . . : Deshabilitado
```

Bestalde, interfazea bera atzi daitekeen ere begira daiteke, **ping** edo **ping6** komandoaren bidez (bata, bestea nahiz biak egoten dira erabilgarri, sistema eragile bakoitzaren bertsio jakinaren arabera). Adibidea, «loopback» helbidea erabiliz:

```
ping ::1
  Haciendo ping a ::1 desde ::1 con 32 bytes de datos:
  Respuesta desde ::1: tiempo<1m
  Respuesta desde ::1: tiempo<1m
  Respuesta desde ::1: tiempo<1m
  Respuesta desde ::1: tiempo<1m
  Estadísticas de ping para ::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Sareko txartel jakin baten «link-local» edo loturarekiko helbide lokalarekin ere egin daiteke proba (*local* helbidea da interfaze hori konektatzen den sare-segmentuan soilik baliozkoa dena); sareko txartela ipv6 if edo ipconfig erabiliz ikus daiteke. Hau lortzen da:

```
ping6 fe80::e8a7:b568:a076:6ba3 (norberaren link-local)
  Haciendo ping a fe80::e8a7:b568:a076:6ba3 desde
fe80::e8a7:b568:a076:6ba3%5 con 32 bytes de datos:
    Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
    Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
    Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
    Respuesta desde fe80::e8a7:b568:a076:6ba3: tiempo<1m
    Estadísticas de ping para fe80::e8a7:b568:a076:6ba3:
      Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
      Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Hurrengo urratsean, sare lokalarekiko konektagarritasuna egiaztatu behar da. Horretarako, sare lokal horretan bertan IPv6 behar bezala konfiguratua duen beste gailuren bat behar da (eta suebakiaren konfigurazioak ping komandoa erabiltzen uztea). Erabilera hau aurreko adibidekoaren antzekoa da, baina ping egin nahi zaion makinaren loturaren helbide lokala erabiltzen da (edo, balego, helbide global bat).

```
ping fe80::200:87ff:fe28:a0e0%5 (5. interfazeko hurrengo nodoaren link-local helbidea)
Haciendo ping a fe80::200:87ff:fe28:a0e0%5 desde
fe80::201:4aff:fe18:26c7%5 con 32 bytes de datos:
    Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
    Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
    Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
    Respuesta desde fe80::200:87ff:fe28:a0e0%5: tiempo<1ms
    Estadísticas de ping para fe80::200:87ff:fe28:a0e0%5:
      Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
      Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Bestalde, sare lokalaz kanpoko konektagarritasuna izanez gero, alegia, IPv6 baduten Interneteko beste makina batzuekiko konektagarritasuna izanez gero, honen antzeko emaitza bat lortzen da:


```
ping www.ipv6tf.org
Haciendo ping a www.ipv6tf.org [2a01:48:1:0:2e0:81ff:fe05:4658]
desde 2001:db8:0:0:2c0:26ff:fea0:a341 con 32 bytes de datos:
    Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo=99.661m
    Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo<106.572m
    Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo<88.624m
    Respuesta desde 2a01:48:1:0:2e0:81ff:fe05:4658: tiempo<76.629m
    Estadísticas de ping para 2a01:48:1:0:2e0:81ff:fe05:4658:
      Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
      Mínimo = 76.629ms, Máximo = 106.572ms, Media = 92.871ms
```

Beste urrats bat ere egin daiteke. Hain zuzen, gure makinatik helburuko makinara dauden sareko puntuen arteko saltoak bistaraztea edo traceroute deritzona (bide-aztarna). Horretarako, tracert edo tracert6 komandoa erabiltzen da, plataformaren eta bertsioaren arabera.

```
tracert www.lacnic.net
Traza a la dirección lacnic.net [2001:13c7:7002:4000::10]
sobre un máximo de 30 saltos:
1  <1 ms    <1 ms   <1 ms  2a01:48:1::ff0
2  29 ms    25 ms    7 ms  2a01:48::d5ac:227d
```

```
3  53 ms   60 ms   35 ms  tunnel105.tserv17.lon1.ipv6.he.net
   [2001:470:14:69::1]
4  75 ms  109 ms   34 ms  gige-g4-18.core1.lon1.he.net [2001:470:0:a3::1]
5  63 ms   43 ms   73 ms  10gigabitethernet1-1.core1.ams1.he.net
   [2001:470:0:3f::2]
6  447 ms 163 ms 112 ms  2001:7f8:1::a500:3549:2
7  297 ms 325 ms 319 ms  2001:450:2002:7f::2
8  303 ms 313 ms 656 ms  ar01.bb2.registro.br [2001:12ff:2:1::244]
9  297 ms 315 ms 313 ms  gw01.lacnic.registro.br [2001:12ff:1:3::212]
10 302 ms 320 ms 320 ms  www.lacnic.net [2001:13c7:7002:4000::10]
Traza completa.
```

3.2. Egiaztapena Mac OS Xn

Sistema/Red/Avanzado-ko Preferencias-en bidez, honako pantaila hau bistaratzen da, eta, TCP/IPn, automatikoki konfiguratua dagoela egiazta daiteke.

4. IRUDIA. **IPv6-REN KONFIGURAZIO AUTOMATIKOAREN EGIAZTAPENA, MAC OS XN**

Nahi izanez gero, terminalera jo daiteke, ifconfig komandoa erabiltzeko. Adibidez:

```
$ ifconfig

lo0:  flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
      inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
      inet 127.0.0.1 netmask 0xff000000
      inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=1<UP> mtu 1280
      inet6 2002:8281:57f9:1::1 prefixlen 16
en0:  flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
      ether 00:1b:63:bd:71:67
      media: autoselect status: inactive
```

```
        supported media: autoselect 10baseT/UTP <half-duplex>
10baseT/UTP <full-duplex> 10baseT/UTP <full-duplex,hw-loopback>
10baseT/UTP <full-duplex,flow-control> 100baseTX <half-duplex>
100baseTX <full-duplex> 100baseTX <full-duplex,hw-loopback> 100baseTX
<full-duplex,flow-control> 1000baseT <full-duplex> 1000baseT <full-
duplex,hw-loopback> 1000baseT <full-duplex,flow-control> none
   fw0:  flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 4078
         lladdr 00:1e:52:ff:fe:46:46:0c
         media: autoselect <full-duplex> status: inactive
         supported media: autoselect <full-duplex>
   en1:  flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAS
T> mtu 1500
         inet6 fe80::21e:52ff:fe73:c2a6%en1 prefixlen 64 scopeid 0x6
         inet6 2001:df8::80:21e:52ff:fe73:c2a6 prefixlen 64 autoconf
         inet 130.129.87.249 netmask 0xfffff800 broadcast 130.129.87.255
         ether 00:1e:52:73:c2:a6
         media: autoselect status: active
         supported media: autoselect
   en5:  flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
         ether 00:1e:52:d7:90:f5
         media: autoselect status: inactive
         supported media: none autoselect 10baseT/UTP <half-duplex>
   en2:  flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,
MULTICAST> mtu 1500
         inet6 fe80::21c:42ff:fe00:0%en2 prefixlen 64 scopeid 0x8
         inet 10.37.129.3 netmask 0xffffff00 broadcast 10.37.129.255
         ether 00:1c:42:00:00:00
         media: autoselect status: active
         supported media: autoselect
   en3:  flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,
MULTICAST> mtu 1500
         inet6 fe80::21c:42ff:fe00:1%en3 prefixlen 64 scopeid 0x9
         inet 10.211.55.8 netmask 0xffffff00 broadcast 10.211.55.255
         ether 00:1c:42:00:00:01
         media: autoselect status: active
         supported media: autoselect
   tun0: flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST>
mtu 1500
         open (pid 199)
```

Windowsen egindakoaren antzera, terminal-leiho batean ping6 eta traceroute6 komandoak erabil daitezke (kontuz: kasu honetan, traceroute6 komandoa osorik idatzi behar da):

```
$ ping6 www.ipv6tf.org
PING6(56=40+8+8 bytes) 2001:df8::80:21e:52ff:fe73:c2a6 -->
2a01:48:1::2e0:81ff:fe05:4658
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=0 hlim=49
time=643.332 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=1 hlim=49
time=87.239 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=3 hlim=49
time=82.984 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=4 hlim=49
time=202.559 ms
^C
--- www.ipv6tf.org ping6 statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 82.984/254.029/643.332 ms

$ ping6 fe80::21e:52ff:fe73:c2a6%en1
PING6(56=40+8+8 bytes) fe80::21e:52ff:fe73:c2a6%en1 -->
fe80::21e:52ff:fe73:c2a6%en1
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp _ seq=0 hlim=64
time=0.089 ms
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp _ seq=1 hlim=64
time=0.117 ms
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp _ seq=2 hlim=64
time=0.118 ms
16 bytes from fe80::21e:52ff:fe73:c2a6%en1, icmp _ seq=3 hlim=64
time=0.167 ms
^C
--- fe80::21e:52ff:fe73:c2a6%en1 ping6 statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.089/0.123/0.167 ms

$ ping6 www.ipv6tf.org
PING6(56=40+8+8 bytes) 2002:4e40:58c0:9:21e:52ff:fe73:c2a6 -->
2a01:48:1::2e0:81ff:fe05:4658
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=0 hlim=60
time=93.848 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=1 hlim=60
time=93.32 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=2 hlim=60
time=92.087 ms
16 bytes from 2a01:48:1::2e0:81ff:fe05:4658, icmp _ seq=3 hlim=60
time=89.836 ms
^C
--- www.ipv6tf.org ping6 statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 89.836/92.273/93.848 ms
```

Eta beste hainbeste traceroute6 komandoarekin:

```
$ traceroute6 www.ipv6tf.org
traceroute6 to www.ipv6tf.org (2a01:48:1::2e0:81ff:fe05:4658) from
2001:df8::80:21e:52ff:fe73:c2a6, 30 hops max, 12 byte packets
 1  2001:df8:0:80::3 433.216 ms 0.813 ms 1.108 ms
 2  htg0-ncore-2.gigabiteth5-2.swip.net 1.281 ms 1.141 ms 1.072 ms
 3  avk-core-1.gigabiteth6-0-0.swip.net 1.514 ms 1.432 ms 2.269 ms
 4  avk-core-2.tengigabiteth2-1.swip.net 1.444 ms 1.476 ms 1.275 ms
 5  ibr01-tu15.stkh01.occaid.net 3.865 ms 2.842 ms 2.926 ms
 6  bbr01-p2-0.lndn01.occaid.net 43.132 ms 42.645 ms 43.049 ms
 7  neosky-ic-8241-lon.customer.occaid.net 66.522 ms 66.901 ms 67.478 ms
 8  consulintel-neosky.consulintel.es 99.245 ms 106.983 ms 94.87 ms
```

3.3. Egiaztapena beste sistema eragile batzuetan

Oro har, gainerako sistema eragileetan (Unix, Unixen antzekoak, Unixetik eratorriak, Linux, BSD eta abar), ifconfig erabiltzea izaten da errazena. Baina, batzuetan, badute erabiltzaileentzako interfaze grafikoko ingurune bat (plataforma bakoitzak berea), non sareko interfazeen egoera kontrolatzen baita, besteak beste, IPv6-rena. Beraz, Mac OS Xrako azaldutako adibideen baliokideak dira.

Gainera, ping6 eta traceroute6 ere erabil daitezke, eta aurreko atalean Mac OS Xrako ikusitako adibide guztiak baliozkoak dira.

4. IPv6-ren konfigurazio aurreratua

Batzuetan, konfigurazio aurreratuak egin behar izaten dira. Adibidez, IPv6 helbide bat eskuz konfiguratzeko, edo konfigurazio hori aldatzeko, nahiz ezabatzeko.

Aurreko kasuetan bezala, sistema eragile desberdinetan desberdin egiten dira konfigurazioak.

4.1. Konfigurazio aurreratua Windowsen

Dena delakoagatik, IPv6 helbide bat eskuz konfiguratu beharra sor daiteke. Horretarako, netsh komandoa erabiltzen da, honela:

netsh interface ipv6 add address [**interface=**]<karaktere-katea (interfazearen izena edo indizea)> [**address=**]<IPv6 helbidea> [**/**<osoa>] [[**type=**]**unicast**|**anycast**] [[**validlifetime=**]<osoa>|**infinite**] [[**preferredlifetime=**]<osoa>|**infinite**] [[**store=**]**active**|**persistent**]

Adibidea:

netsh interface ipv6 add address 5 2001:db8::2 **type=unicast validlifetime=infinite preferredlifetime**=10m **store=active**

Bestalde, konfigurazioa berrikus daiteke netsh erabiliz (5. interfazea dela jota):

netsh interface ipv6 show address 5

Helbide bat eskuz konfiguratu ondoren, honela alda daiteke:

netsh interface ipv6 set address [**interface=**]<karaktere-katea> [**address=**]<IPv6 helbidea> [[**type=**]**unicast**|**anycast**] [[**validlifetime=**]<osoa>|**infinite**] [[**preferredlifetime=**]<osoa>|**infinite**] [[**store=**]**active**|**persistent**]

Adibidea:

netsh interface ipv6 set address 5 2001:db8::2 **preferredlifetime=infinite**

Azkenik, helbide hori ezabatu egin daiteke, honela:

netsh interface ipv6 delete address [**interface=**]<karaktere-katea> [**address=**]<IPv6 helbidea> [[**store=**]**active**|**persistent**]

Adibidea:

netsh interface ipv6 delete address 5 2001:db8::2 **store=persistent**

Bestalde, gerta liteke bide finko bat gehitu nahi izatea. Honela egiten da:

netsh interface ipv6 add route add route [**prefix=**]<IPv6 helbidea>/<osoa> [**interface=**]<karaktere-katea> [[**nexthop=**]<IPv6 helbidea>] [[**siteprefixlength=**]<osoa>] [[**metric=**]<osoa>] [[**publish=**]**no**|**yes**|**immortal**] [[**validlifetime=**]<osoa>|**infinite**] [[**preferredlifetime=**]<osoa>|**infinite**] [[**store=**]**active**|**persistent**]

Adibidea:

netsh interface ipv6 add route 2002::/16 5 fe80::200:87ff:fe28:a0e0 **store=persistent**

Non fe80::200:87ff:fe28:a0e0 baita 2002::/16 sarerako bidearentzat konfiguratu nahi den irteera-ataka.

Bide hori ezabatzeko:

netsh interface ipv6 delete route [**prefix=**]<IPv6 helbidea>/<osoa> [**interface=**]<karaktere-katea> [[**nexthop=**]<IPv6 helbidea>] [[**store=**]**active**|**persistent**]

Adibidea:

netsh interface ipv6 delete route 2002::/16 5 fe80::200:87ff:fe28:a0e0 **store=persistent**

Honela bistaraz daitezke bideratze-taulak

netsh interface ipv6 show route [[**level=**]**normal**|**verbose**] [[**store=**]**active**|**persistent**]

Adibidea:

netsh interface ipv6 show route

```
Publicar  Tipo      Mét Prefijo        Índ Puerta enl./Nombre int.
--------  --------  ---  ------------  ---------------------------
No        Manual    8  ::/0           13 Conexión de área local* 7
no        Manual    0  2002::/16      5 fe80::200:87ff:fe28:a0e0
no        Autoconf  8  2001:db8::/64  5 Local Area Connection
no        Autoconf  256 ::/0          5 fe80::200:87ff:fe28:a0e0
```

Azkenik, DNS-zerbitzari bat ere gehitu daiteke, honela:

netsh interface ipv6 add dnsserver [**name=**]<karaktere-katea> [**address=**]<IPv6 helbidea> [[**index=**]<osoa>]

XP SP1/2003 SP1 sistemetan, dns jarri behar da, dnsserver beharrean.

Adibidea:

netsh interface ipv6 add dnsserver "Local area network**"** 2001:7f9:1000:1::947c 1

Indizeak DNS zerbitzariak DNS-zerbitzarien zerrendan duen posizioa (lehentasuna) adierazten du.

Eta eskuz konfiguratutako DNS-zerbitzariak honela bistarazten dira:

netsh interface ipv6 show dnsservers [[**name=**]<karaktere-katea>]

Adibidea:

netsh interface ipv6 show dnsservers

DNS servers in LAN interface

```
Index   DNS server
------  ------------------------------------
1       2001:7f9:1000:1::947c
2       2001:7f9:1000:1::947c
```

Eta honela ezabatzen dira:

netsh interface ipv6 delete dnsserver [**name=**]<karaktere-katea> [[**address=**]<IPv6 helbidea>|**all**]

Adibidea:

netsh interface ipv6 delete dnsserver "Local area network**" all**

4.2. Konfigurazio aurreratua Linuxen

IPv6 helbide bat gehitzeko:

 # /sbin/ip -6 addr add <ipv6 helbidea>/<aurrezenbakiaren luzera> **dev** <interfazea>

 # /sbin/ifconfig <interfazea> **inet6 add** <ipv6 helbidea> /<aurrezenbakiaren luzera>

IPv6 helbide bat ezabatzeko:

 # /sbin/ip -6 addr del <ipv6 helbidea>/<aurrezenbakiaren luzera> **dev** <interfazea>

 # /sbin/ifconfig <interfazea> **inet6 del** <ipv6 helbidea> /<aurrezenbakiaren luzera>

Irteera-ataka bati dagokion bide bat gehitzeko:

 # /sbin/ip -6 route add <ipv6 sarea>/<aurrezenbakiaren luzera> **via** <ipv6 helbidea> [**dev** <gailua>]

#/sbin/route -A inet6 add <ipv6 sarea>/<aurrezenbakiaren luzera> **gw** <ipv6 helbidea> [**dev** <gailua>]

IPv6 bideratze-taulak ikusteko:

 # /sbin/ip -6 route show [**dev** <gailua>]

 # /sbin/route -A inet6

Irteera-ataka bati dagokion bide bat ezabatzeko:

 # /sbin/ip -6 route del <ipv6 sarea>/<aurrezenbakiaren luzera> **via** <ipv6 helbidea> [**dev** <gailua>]

 # /sbin/route -A inet6 del <sarea>/<aurrezenbakiaren luzera> [**dev** <gailua>]

Interfaze bati dagokion bide bat gehitzeko:

 # /sbin/ip -6 route add <ipv6 sarea>/<aurrezenbakiaren luzera> **dev** <gailua> **metric 1**

 # /sbin/route -A inet6 add <sarea>/<aurrezenbakiaren luzera> **dev** <gailua>

Interfaze bati dagokion bide bat ezabatzeko:

 # /sbin/ip -6 route del <ipv6 sarea>/<aurrezenbakiaren luzera> **dev** <gailua>

 # /sbin/route -A inet6 del <sarea>/<aurrezenbakiaren luzera> **dev** <gailua>

4.3. Konfigurazio aurreratua BSDn

IPv6 helbide bat gehitzeko:

#>ifconfig <interfazea> **inet6 add** <IPv6 helbidea>

IPv6 helbide bat ezabatzeko:

```
#>ifconfig <interfazea> inet6 del <IPv6 helbidea>
```

Konfigurazioa iraunkorra izatea nahi badugu, /etc/rc.conf fitxategia erabiltzen da:

```
ipv6 _ enable="YES"
ipv6 _ ifconfig _ rl0="2001:618:10:4::4 prefixlen 64"
```

Aukera posibleak eta lehenetsiak zein diren ikus daiteke /etc/defaults/rc.conf fitxategian.

Ordenagailua berrabiarazi egin behar da rc.conf-en egindako aldaketak aplikatzeko.

Bide lehenetsi bat gehitzeko:

```
#>route –n add -inet6 default <IPv6 helbidea>
```

Bide lehenetsia ezabatzeko:

```
#>route –n del -inet6 default
```

4.4. Konfigurazio aurreratua Mac OS Xn

IPv6 helbide bat gehitzeko:

```
# ifconfig <interfazea> inet6 2001:db8:1:1::2/64
```

IPv6 helbide bat ezabatzeko:

```
# ifconfig <interfazea> inet6 delete 2001:db8:1:1::2
```

Bide lehenetsi bat gehitzeko:

```
# route add -inet6 default [2001:db8:1:1::1, -interface en1]
```

Bide lehenetsia ezabatzeko:

```
#>route del -inet6 default
```

IPv6 bideratze-taulak ikusteko:

```
#  netstat -r -f inet6
```

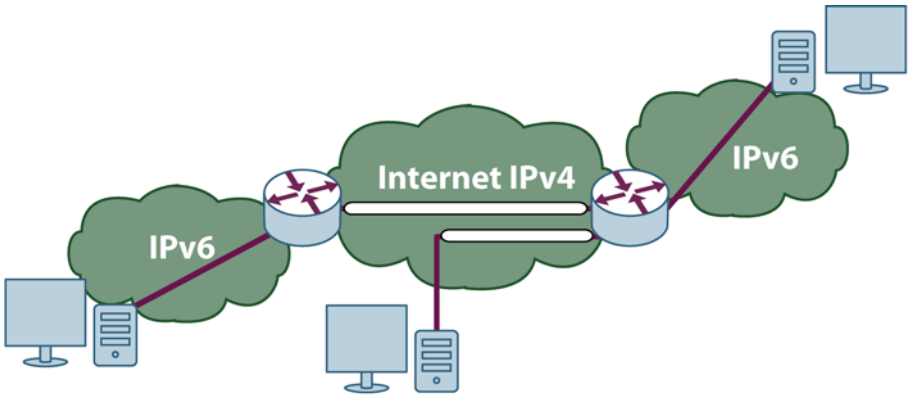
5. IPv6-ren trantsizio-mekanismoak

Gaur egun, ISP guztiek ez dute IPv6 beren sareetan, eta trantsizio-mekanismoak erabili behar dira.

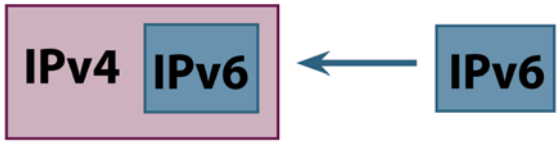
Funtsean, mekanismo horiek aukera ematen dute IPv4 eta IPv6 aldi berean aritzeko; baita, IPv6 jatorriz erabilgarri ez dagoenean, IPv4 sarearen bidez IPv6 erabiltzeko aukera ere. Horretarako, batez ere, *tunel* deritzegun mekanismoez baliatzen dira.

Tunel-mekanismoek IPv6 paketatu edo kapsulatu egiten dute IPv4 paketeen barnean, halako moldez, non erabilgarri dagoen IPv4 sarean garraiatzen baita IPv6.

Grafiko hauek tunel horiek nola dabiltzan eta IPv6 IPv4en nola paketatzen den erakusten dute:



5. IRUDIA. **IPv6-REN TUNELAK IPv4-N**



6. IRUDIA. **IPv6 IPv4-N KAPSULATZEA**

Trantsizio-mekanismo ugari dago, eta oso gai konplexua da kapsulatzearen hori. Horregatik, atal honetan, erabilgarrientzat jo ditugun tunel-mekanismoak soilik azaldu ditugu, alegia, tunel automatikoak; eta, zehatzago esateko, 6to4 eta Teredo deritzen tunel-mekanismo automatikoak.

IPv4 helbide publikoak erabiltzen direnean soilik funtzionatzen du6to4 sistemak. Adibidez, ordenagailu bat ADSL sare batera USB-modem baten bidez konektatua dagoenean. Kasu horretan, xehetasun teknikoak alde batera utzita, IPv4 helbidea erabiltzen da IPv6 helbidea eta tunel automatiko bat automatikoki konfiguratzeko; tunel automatikoari esker, IPv4 sarean zehar erabil daiteke IPv6.

Teredok (Linux, BSD eta Mac OS X sistemetan, Miredo), berriz, IPv4 pribatuekin funtzionatzen du; alegia, NAT edo sareko helbideen itzultzaileen atzean dago. Teredo erabiltzen da, adibidez, ADSL sare bateko konexio bat, moden baten bidez egin ordez, router edo bideratzaile baten bidez egiten denean. 6to4 sisteman egiten denaren antzera, automatikoki sortzen da IPv6 helbide bat bideratzaile/NAT horretara konektatutako ordenagailu bakoitzarentzat, eta IPv4 sarean zehar erabiltzen da IPv6.

Trantsizio-mekanismo horiek automatikoak direnez, ez dira konfiguratu behar izaten, eta sistema eragileak berak ikusten du sarean IPv6 konektagarritasunik badagoen edo ez (adibidez, ISPak ematen duena); eta, ez badago, 6to4 edo Teredo aktibatzen du.

Miredo erabili behar bada, Internetetik softwarea deskargatu eta instalatu besterik ez da egin behar.

6. IPv6-ren desinstalazioa

Oro har, ez da IPv6 desinstalatu beharrik. Baina, dena delakoagatik, desinstalatu behar izanez gero, plataforma garrantzitsuenetan desinstalatzeko informazioa jarri dugu hemen.

6.1. Desinstalazioa XP/2003/Vista/7 plataformetan

Plataforma horietako batzuetan, honela egiten da:

```
ipv6 uninstall
```

Beste batzuetan, berriz, netsh komandoa erabili behar da, ipv6.exe komandoa Windows XPra arte soilik agertzen delako:

```
netsh interface ipv6 uninstall
```


Ingurune grafikoa ere erabil daiteke, noski. Hain zuzen, instalatzeko egindakoaren aurkakoa egin behar da.

Oro har, sistema eragilea berrabiarazi egin behar da, ezusteko ondorioak ekiditeko.

Bestalde, pila jatorrizko egoera lehenetsira itzuli nahi izanez gero, hau egin daiteke (plataforma gehienetan):

```
netsh interface ipv6 reset
```

Windows Vistan, 2008n eta 7n, IPv6-ren pila ezin da guztiz desaktibatu, IPv6-ren pila IPv4-ren pilarekin erabat integratua dagoelako. Horren ordez, ingurune grafikoa erabil daiteke sareko interfaze jakin batean desaktibatzeko.

6.2. Desinstalazioa Windows 2000n

Hau da prozedura:

- Sartu sisteman, administratzaile-pribilegio lokalak dituen erabiltzaile gisa.
- Windows 2000ren mahaigainean, sakatu, hurrenez hurren, Hasi, Ezarpenak eta Sare-konexioak. Egin klik eskuin-botoiarekin Sarekoak aukeran, eta sakatu Propietateak.

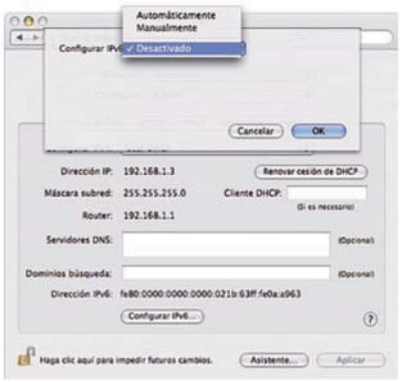
- Egin klik eskuin-botoiarekin IPv6 protokoloa kendu nahi zaien Etherneten oinarritutako konexioetan, eta, ondoren, sakatu Propietateak. Normalean, konexio horri *sare lokaleko konexio* deritzo.
- Aukeratu MSR IPv6 protokoloa, eta egin klik Desinstalatu botoian.
- MSR IPv6 protokoloa desinstalatzeko elkarrizketa-koadroan, sakatu Bai.
- Sare lokalaren elkarrizketa-koadroan sakatu Bai, ordenagailua berrabiarazteko.

6.3. Desinstalazioa Mac OS Xn

IPv6 interfaze guztietan desgaitu dezakegu, honela: **#ip6 –x**

Berriro gaitzeko, erabili hau: **#ip6 –a**

Ingurune grafikoa ere erabil dezakegu.



7. IRUDIA. **IPv6 DESGAITZEA, MAC OS XN**

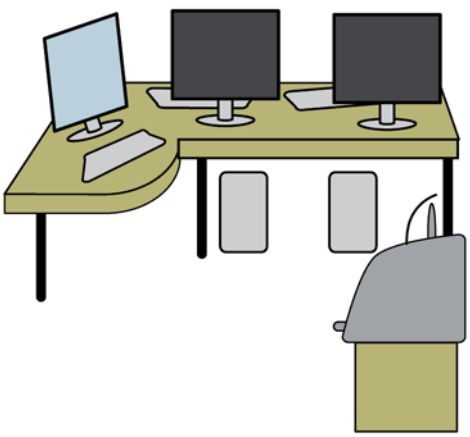
3. Home Office

1. Sarrera

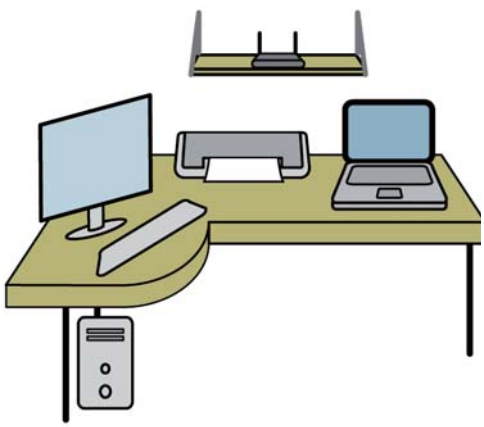
1.1. Zer da SOHO bat?

SOHO da bulego txiki bat edo etxean antolatutako bulego bat (Small Office, Home Office). Oro har, horrela deritze hamar langile edo gutxiago[1] dituzten bulegoei edo profesional independenteen taldeei (1. eta 2. irudiak).

Definizio hori oinarri hartuta, IPv6 duen Home Officeri buruz ari garenean, SOHO sare batez ari gara, zeinak IP protokolo berriarekin (IPv6) lan egin baitezake.



1. IRUDIA. **10 LANGILE BAINO GUTXIAGO DITUEN NEGOZIO TXIKI BAT**



2. IRUDIA. **ETXEKO BULEGO BAT**

1.2. IPv6 duen SOHO bat eraikitzea

Bere sarean IPv6 duen SOHO bat eraikitzen hasi aurretik, argi izan behar dugu zer zatiz osatua dagoen sare hori. Zati horiek zein diren argitu ondoren, ikusi behar dugu horietako zein konfiguratu behar dugun IPv6 erabil dezaten. Azkenik, konfigurazioa nola egin erabaki behar dugu.

Alegia, urrats hauek egin behar ditugu:

1 http://es.wikipedia.org/wiki/Small_Office,_Home_Office

1. SOHOaren zatiak identifikatu
2. IPv6-rekin ibiltzeko, horietako zein zati konfiguratu behar den zehaztu
3. SOHOa IPv6-rekin konfiguratu

2. SOHO bat osatzen duten zatiak identifikatzea

Aurreko paragrafoan esan dugunez, horixe da SOHO bateko sarea eraikitzean egin behar den lehenbiziko gauza. Identifikazio hori egiteko, komeni da hiru alderdi mugatu kontuan hartzea:

2.1. SOHOa osatzen duten ekipoen identifikazioa, bereizketa hau eginez:
2.1.1. Sareko gailuak
2.1.2. Terminalak

2.2. Sistema eragileen eta haien aldaeren identifikazioa:
2.2.1. Zerbitzarien sistema eragileak
2.2.2. Ordenagailuen eta eskuko ordenagailuen sistema eragileak

2.3. Aplikazioen identifikazioa
2.3.1. Zerbitzarietakoak
2.3.2. Terminaletakoak

Has gaitezen **2.1.** puntutik:

- Sareko gailuak. Gure sarean, erabiltzaile-interfazekoak ez diren gailuak —alegia, sareko komunikaziorako direnak— identifikatu behar ditugu. Adibidez, multzo honetakoak dira, besteak beste: terminalak edo ordenagailuak konektatzeko erabiltzen dugun kommutadorea, zerbitzua kontratatzean hornitzaileak instalatutako router edo bideratzailea, eta haririk gabeko konexioa ematen digun ekipoa.
- Terminalak. Talde honetakoak dira zuzenean erabiltzen ditugun gailuak. Besteak beste: mahai gaineko ordenagailuak, eskuko ordenagailuak, PDAk, IP-telefonoak eta aplikazioen zerbitzariak.

Beste kategoria batean, sareko inprimagailuak identifika ditzakegu; erabiltzailearentzat zuzeneko interfaze bat ez diren arren, ez dira sareko gailuak ere. Nolanahi ere, inprimagailuek sarearen barruan lan egitea nahi izaten dugu, eta, segur aski, kontuan hartu beharko ditugu IPv6-rekin lan egiteko orduan.

2.2. puntuan, lanerako erabiltzen ditugun sistema eragileak identifikatu behar ditugu. Horretarako, kontuan hartuko ditugu:

- Zerbitzarien sistema eragileak. Sareari zerbitzua (adibidez, posta elektronikoa) ematen dioten terminaletan exekutatzen diren sistema eragileak dira. Sistema eragileak dira, besteak beste, Linux, Windows eta Unix. Linux eta Windows dira SOHO sareetan gehien erabiltzen direnak.
- Ordenagailuen eta eskuko ordenagailuen sistema eragileak. Lanerako zuzenean erabiltzen ditugun gailuetan exekutatzen diren sistema eragileak dira. Horrelakoetan, Windows, Linux eta Mac OS erabiltzen dira gehien.

SOHO sarearen osagaien identifikazioa bukatzeko, elementu hauek bereizi behar ditugu, **2.3.** puntuaren arabera:

- Zerbitzarietako aplikazioak. Zerbitzarietako aplikazioak dira sareko gailuei zerbitzua modu zentralizatuan ematen dietenak. Besteak beste, DNS-zerbitzua, posta elektronikoa eta web-orriak.
- Terminaletako aplikazioak. Aplikazio horiek erabiltzen ditugu PDAn, eskuko ordenagailuan edo mahaigaineko ordenagailuan lan egiteko. Hauek dira ezagunenak, besteak beste: testu-editoreak, kalkulu-orriak, posta elektronikoko bezeroak, web-arakatzaileak, berehalako mezularitzako bezeroak, multimedia-zerbitzuen bezeroak eta neurrira egindako aplikazioak.

SOHOaren osagai guztiak identifikatutakoan, IPv6-ren bidez horietako zein ibiliko diren finka dezakegu. Hori da, hain zuzen, hurrengo urratsa.

3. Konfiguratu behar diren osagaiak finkatzea

Oro har, sarea berri samarra bada —alegia, sareko ekipoek hiruzpalau urte badituzte—, IPv6 onartzen ez duten sistema eragileak eguneratu besterik ez da egin behar.

Komeni da sareko ekipo guztien zerrenda egitea, eta ekipo bakoitzak IPv6-rekin duen bateragarritasunari buruzko informazioa bilatzea, ekipo horien bibliografian edo dokumentazioan. Gure ekipoek IPv6 onartzen ez badute, segur aski sistema eragileren bat eguneratu edo firmwareren bat instalatu beharko dugu, IPv6 onar dezaten.

Adibidez, Cisco bideratzaileek IOS 12.3T bertsiotik aurrera onartzen dute IPv6, eta Juniperren kasuan, berriz, JunOS-en bertsio guztiek onartzen dute. Bestalde, haririk gabeko konexioa duten ekipoen konfigurazioa, IPv6 onar dezaten, bideratzailearen markaren eta modeloaren araberakoa da. Adibidez, Apple[2] etxeko AirPort gailuek badute IPv6, eta D-link[3] etxeko haririk gabeko bideratzaileek ere bai.

Sistema eragileei dagokienez, badira urte batzuk Linux gehienek IPv6-ren pila kargatua dakartela , eta Unixen bertsioek ere bai (adibidez, Solaris sistema eragileek 8. bertsiotik onartzen dute IPv6). Mac OS sistema eragileek, berriz, 2003tik dakarte IPv6 lehenespenez (Panther bertsioetatik aurrera). Bestalde, Windows XP eta Windows Server 2003 sistemetan, oso erraza da IPv6-ren pila kargatzea. Windows Vistan, azkenik, ezaugarri hori lehenespenez gaitua dago.

Aplikazio gehienak ez dira IP protokoloaren bertsioaren araberakoak izaten, baina batzuk bai. Hori horrela, ekipoekin erabilitako irizpide bera aplikatzen da: kontuan hartu behar da, hain zuzen, ea eguneratu behar den instalatua dagoen bertsioa. Normalean, eragozpen gehienak neurrira egindako aplikazioetan izaten ditugu; IP protokoloaren bertsioaren araberakoak badira, baliteke programa horien programatzaileei deitu behar izatea, programen kodea alda dezaten.

2 http://www.apple.com/airportextreme/specs.html,
3 http://www.ipv6ready.org/logo_db/logo_search2.php?logoid_number=01-000322&btm=Search

Testuingurua hori izanik, gure sarean, segur aski, gailu batzuk IPv6-ra aldatzeko modukoak izango dira, eta beste batzuk ez. Orduan, IP protokoloaren bi bertsioak aldi berean exekutatu ahal izatea komeni zaigu; alegia, pila bikoitzeko mekanismoak edo *dual stack* deritzenak erabiltzea komeni zaigu.

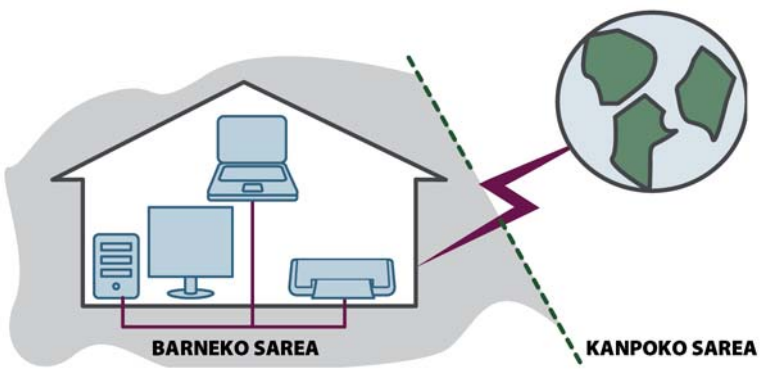
4. SOHOaren osagaiak IPv6-rekin konfiguratzea

Gailuak identifikatu ondoren, IP protokoloaren bertsio berria onartzeko softwarea eguneratu ondoren, eta aplikazioetan beharrezko aldaketak egin ondoren, azkenik, konfigurazioari ekiteko prest gaude.

Horretarako, bi fasetan banatuko dugu lana:

- Gure SOHOaren barneko sarearen konfigurazioa (LAN)
- Kanpoko konexioaren konfigurazioa (Internet)

Irudi honetan, bien arteko muga ageri da:



Bi lan horien nondik norakoak azaldu baino lehen, erabiliko ditugun IPv6 helbideak nola lortu ikusiko dugu. Badira zenbait aukera. Adibidez:

- Geure helbideak izatea, tokian tokiko Internet Erregistro edo RIRari eskatuta.
- Gure Internet hornitzaileak guri helbide sorta bat esleitzea.
- 6to4 helbideak erabiltzea (orduan IPv4 helbide publiko bat behar dugu, gutxienez, martxan jartzeko).
- *Tunnel broker* edo tunel-hornitzaileak erabiltzea, halako moldez, non IPv6 konektagarritasuna hornitzen duen guneren batekin tunel automatikoak ezartzen baitira. Horretarako, pila bikoitzeko ostalari bat eta hornitzailearen webgunea edo interfazea ikusteko nabigatzaile bat (tunela handik aurrera konfiguratzeko) besterik ez dugu behar.

Aukera horietako batekin, edo liburu honetan azaldu ez dugunen batekin, IPv6 helbideak izatea lortuko dugu. Orduan, sarea konfiguratzen hasteko prest gaude.

4.1. Barneko sarearen konfigurazioa

Oro har, bi aukera ditugu, gure SOHOaren barneko sarea IPv6-rekin ere aritzeko gauzatu dadin konfiguratzeko: eskuzkoa eta automatikoa.

Liburu honen asmoa irakurleak IPv6-rekiko esperientzia era praktikoan lortzea denez, sarea automatikoki nola konfiguratzen den azaltzera mugatuko gara.

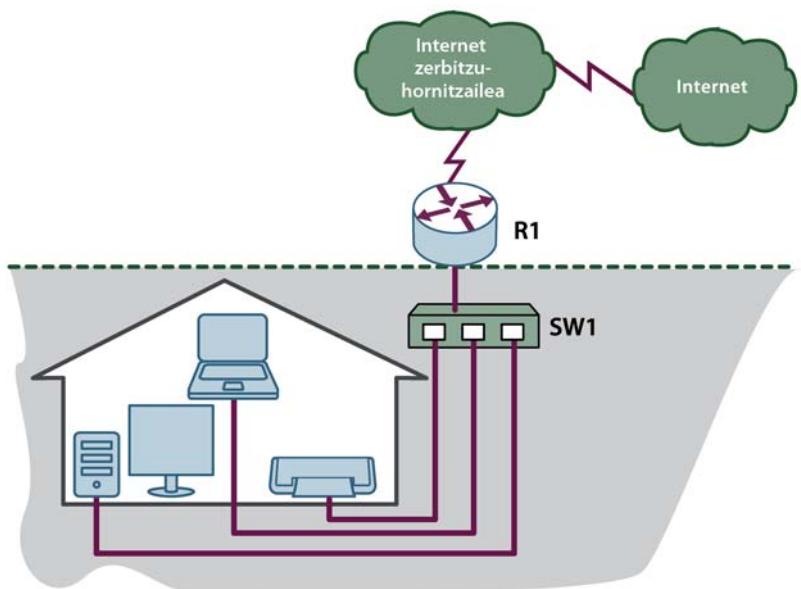
Sare batean IPv6 helbideak dituzten interfazeak automatikoki konfiguratzeko, interfaze horiek konfiguratu nahi dituzten gailuek horretarako datuak eskatu behar dituzte, eta beste gailuren batek datu horiek eman behar ditu.

Eskaera eta iragarpen horiek Neighbor Discovery[4] protokolokoak dira, eta, ICMPv6[5] mezu sorta baten bidez, konfigurazio automatikoa egiteko oinarri bihurtzen da protokolo hori.

Izenak laburtzeko, datuak eskatzen dituzten ICMPv6 mezuei NS (Neighbor Solicitation) eta RS (Router Solicitation) deritze, eta erantzunak ematen dituzten ICPMv6 mezuei, berriz, NA (Neighbor Advertisement) eta RA (Router Advertisement).

Sarrera hau eginik, ikus dezagun nola egin dezakegun SOHO sarearen konfigurazio automatikoa, sarearen topologiaren arabera.

Har dezagun adibide gisa 3. irudiko sarea.



3. IRUDIA. **LOTURA DEDIKATU BAT DUEN SAREA**

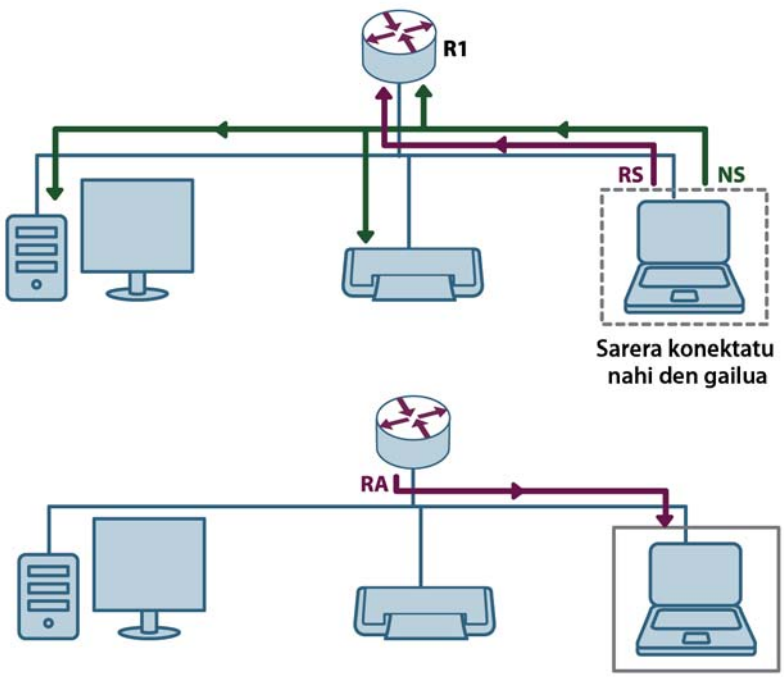
4 http://www.ietf.org/rfc/rfc2461.txt
5 http://www.ietf.org/rfc/rfc2463.txt

SOHO sarearen Interneteko lotura dedikatua da. Alegia, hornitzaileak konexio bat uzten du bezeroaren esku, hark, eta ez beste inork, erabil dezan. Horrelakoetan, bideratzaile bat egoten da, eta hara Interneteko lotura iristen da (3. irudian, R1 izenez adierazi da).

Bideratzailearen interfaze bat SOHOaren barneko sarera lotua dago, eta hara lotuak daude sareko gainerako gailuak ere. Lotura horiek guztiak kommutadore baten bidez egiten dira; kommutadore hori, gure adibidean, SW1 da.

Kasu honetan, gailu batek (eskuko ordenagailu batek, mahaigaineko ordenagailu batek edo beste zerbaitek), sarera konektatzean, NS mezu bat bidaltzen du, sareko nodo guztiek gailu bera ikus dezaten, eta, normalean, RS mezu bat ere bai. RS mezua jasotzean, R1 bideratzaileak RA erantzuna bidaltzen du; erantzun horrek gailuak automatikoki konfiguratzeko erabili behar duen IPv6 aurrezenbakia dauka.

Hau da mezu-segida horren eskema:



Adibidez, Juniper bideratzaileetan hau egin behar da[6], bideratzaileak jakin dezan IPv6 aurrezenbakia jakinarazi behar duela barneko sarea automatikoki konfiguratzeko:

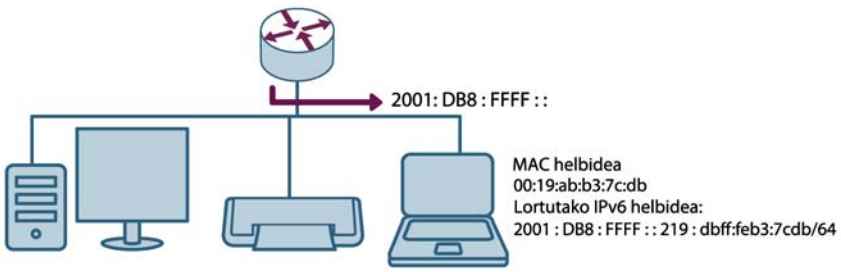
`ipv6 nd prefix-advertisement` `<IPv6 aurrezenbakia/IPv6 aurrezenbakiaren luzera>`

Cisco bideratzaileetan, berriz, nahikoa da interfazea IPv6 helbide batekin konfiguratzea, bideratzaileak helbide hori barneko sarerantz jakinaraz dezan (aurrezenbakiaren jakinarazpena ez egitea nahi denean, ordea, berariaz adierazi behar da).

6 http://www.juniper.net/techpubs/software/erx/junose700/swcmdref-a-m/html/i-commands318.html

Aurrezenbakia lortutakoan, gailuak bere IPv6 helbidea konfigura dezake, bideratzaileak jakinarazitako aurrezenbakian eta gailuaren MAC helbidean oinarrituta (EUI-64[7] metodoaren bidez).

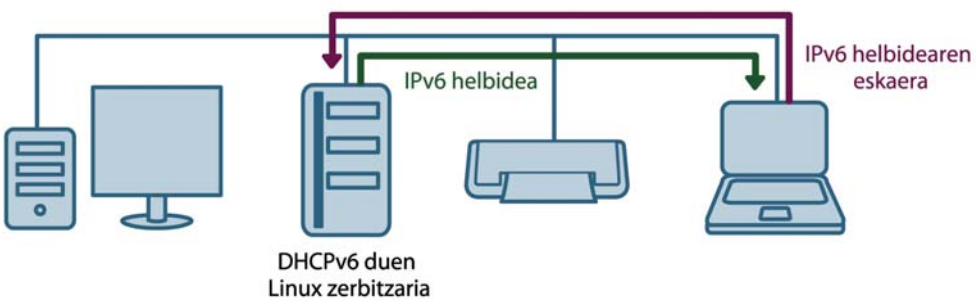
Konfigurazio automatikoa egin ondoren barneko sare batean IPv6 helbideak nola lortzen diren ageri da 4. irudiko ereduan (adibide bat da).



4. IRUDIA. **BARNEKO SARE BATEN KONFIGURAZIO AUTOMATIKOA**

Demagun, orain, SOHOan ezin dugula atzitu Internet zerbitzu-hornitzaileak konektatzeko utzi zigun bideratzailea, edo ez dagoela bideratzailerik. Orduan, RA mezua nork bidaliko duen ikusi behar dugu.

Aukera bat da barneko sarera konektatua dagoen ordenagailu bat erabiltzea, halako moldez, non, RA mezuak jakinaraziz, konfigurazio automatikoak egiteko aukera ematen baitu. Horrelakoa da, adibidez, Linux sistema eragilea duen eta radvd daemona[8] exekutatzen ari den zerbitzari bat. Beste aukera bat da, adibidez, DHCPv6-ren zerbitzari bat erabiltzea[9] (ikus 5. irudia).



5. IRUDIA. **KONFIGURAZIO AUTOMATIKOA, ZERBITZARI BATEN BIDEZ (ADIBIDEA)**

Daemon bat edo DHCPv6-ren zerbitzari bat erabiliko dugu, konfigurazioa benetan automatikoki egitera zenbateraino hurbildu nahi dugun. Izan ere, DHCPv6-ren zerbitzari bat, sareko aurrezenbakiak jakinarazteko ez ezik, beste datu batzuk emateko ere erabil dezakegu (adibidez, DNS-zerbitzarien helbideak). Haatik, radvd-ren kasuan, interfazeak automatikoki konfiguratu daitezen IPv6 aurrezenbakiak jakinarazteko aukera besterik ez

7 http://standards.ieee.org/regauth/oui/tutorials/EUI64.htm
8 http://en.wikipedia.org/wiki/Radvd
9 http://www.ietf.org/rfc/rfc3736.txt

dugu. Horiek horrela, egokia izan liteke bien arteko konbinazio batez baliatzea, sarearen administrazioa errazago kontrolatzeko.

Kasu batean zein bestean, sarea SOHO bat denez, edo IPv6 aurrezenbakia Internet zerbitzu-hornitzaileak esleitzen du, edo helbideak norberarenak dira.

4.2. Kanpoko konexioaren konfigurazioa (Internet)

Puntu honetara iritsi garenerako, segur aski, erabakia izango dugu SOHO sarea nola konfiguratu, aldizka IPv6-rekin lan egin ahal izan dezan. Alegia, LANeko gailuak IPv6 bidez komunikatzea lortu dugu.

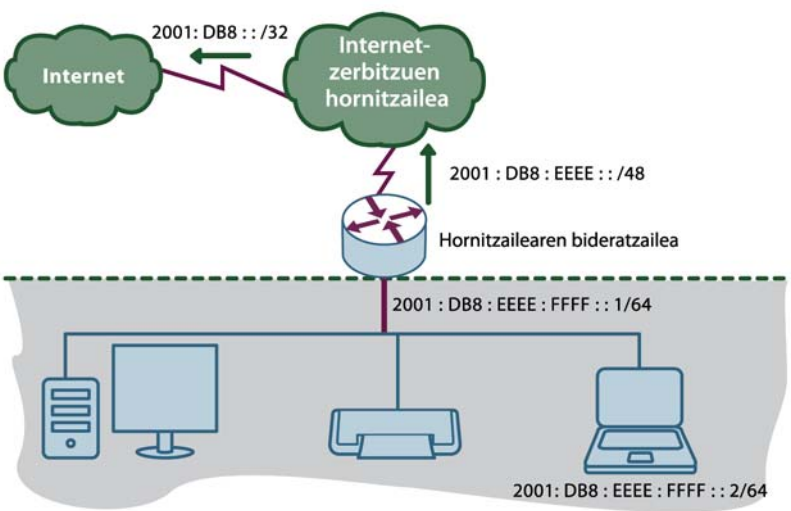
Atal honetan, gure sarean IPv6 bidezko kanpoko konexio bat konfiguratzeko dauden aukerak aztertuko ditugu.

Baliteke SOHO sareak lotura dedikatu bat izatea, eta, horretarako, Internet zerbitzu-hornitzaileak sarea kanpoarekin lotzen duen bideratzaile bat jarria izatea.

Dena den, bi aukera ditugu:

A) Hornitzaileak IPv6 bidezko Interneteko konexioaren zerbitzua ematen digu, IPv4 bidezko konexioaren zerbitzuaz gainera.
B) Hornitzaileak ezin digu eman IPv6 bidezko Interneteko konexio-zerbitzurik.

Gure kasua **A** bada, baliteke hornitzailea bere IPv6 aurrezenbakia jada jakinarazten aritzea; eta, bezeroei zerbitzua emanez gero, bere barrutiko aurrezenbaki bat ematea. Egoera hori izanik, hornitzaileak bere aurrezenbakia jakinarazten badu, gurea ere jakinarazten ari da, bere helbide multzoaren azpimultzo bat izaki. Aurrezenbakien esleipen eta jakinarazpen horren eskema da hau:



IPv6 nonahi baliatzeko gidaliburua

Egoera hori denean, gure hornitzaileak kanpoko konexioaren konfigurazioa nola egitea nahiago duen jakiteko, ez daukagu berarekin hitz egin beharrik (SOHO sarearekiko BGP saio baten bidez, gure bideratzailerantz zuzendutako bide estatikoen bidez, eta abar). Dena den, adosteko kontua besterik ez da. Adostasun horiek gure konektagarritasun-aukeren araberakoak dira, baina komeni izaten da RFC4779 begiratzea, eta gure egoerara hobekien egokitzen direnak zein diren ikustea.

B kasuan bagaude, ordea, hornitzailearen IPv4 sarea zeharkatu eta gure IPv6 paketeak interpreta ditzakeen beste sare batera iristeko modua bilatu behar dugu. Eta hori tunel-mekanismoren baten bidez egiten da.

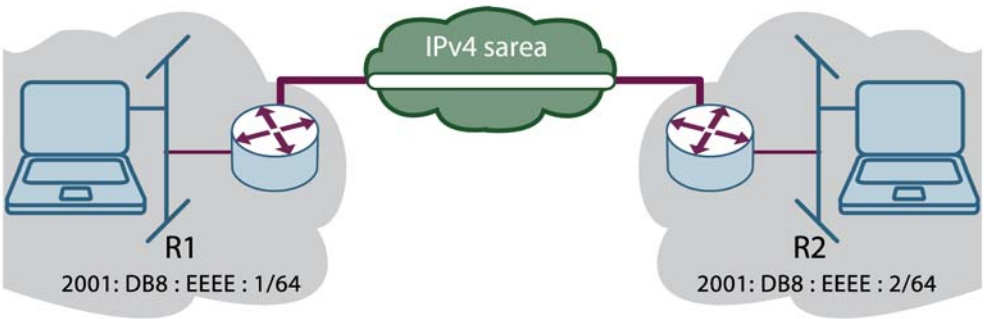
Tunelak (ikus 7. irudia) paketeak kapsulatzeko aukera ematen duten mekanismoak dira, eta paketeak halako moldez paketatzen dira, non ezaugarri nabarmen desberdinak dituzten sareak zeharkatu baititzakete. Bi talde handitan banatzen dira tunelak:

- Eskuzko tunelak. Izenak berak adierazten duenez, eskuz konfiguratzen dira, tunelaren bi aldeetan. Aukera hori eragingarria den arren, kanpoko IPv6 sareetarako konexioa emango digun urruneko gailu batekin tunel bat ezarri behar dugu modu estatikoan.
- Tunel automatikoak. Eskuzkoak ez bezala, bi muturrak ez dira eskuz konfiguratu behar; gutxieneko konfigurazio batekin, automatikoki ezartzen dira

4.2.1. Eskuzko tunelak

Honelako tunelak ez ditugu xehe aztertuko, erabiltzaileentzat praktikoenak diren kasuei ematen baitiegu garrantzi handiena, barneko sarearen konfigurazioan egin dugun bezala.

Eskuzko tunelak, dagoeneko esan dugunez, tunelaren bi muturretan konfiguratu behar dira. Hau da tunel horien funtzionamenduaren eskema:



7. IRUDIA. **IPv6 SAREAK ZEHARKATZEKO ESKUZKO TUNEL BATEN FUNTZIONAMENDUAREN ESKEMA**

Hau da, adibidez, irudiko tunela ezartzeko ohiko konfigurazio orokor bat:

R1-en:

```
interface TunnelAdibideaR1
no ip address
ipv6 address 2001:DB8:FFFF::1/64
tunnel source GigabitEthernet0/0
tunnel destination 1.1.1.1
tunnel mode ipv6ip
```

R2-n:

```
interface TunnelAdibideaR2
  no ip address
ipv6 address 2001:DB8:FFFF::2/64
tunnel source GigabitEthernet0/1
tunnel destination 2.2.2.2
tunnel mode ipv6ip
```

Komando horiek modu orokorrean eta laguntza gisa soilik azaldu ditugu, eta konfiguratzen ari garen gailuaren arabera aldatzen da beren sintaxia. Batetik, gailua askotarikoa izan liteke —bideratzaile batetik hasi eta bideratzaile-lana egiten duen ordenagailu bateraino—, eta, bestetik, sintaxia gailuaren markaren, sistema eragilearen, motaren eta abarren arabera aldatzen da.

4.2.2. Tunel automatikoak

Honelako tunel mota asko dago, baina horietako batzuk besterik ez ditugu aztertuko. Gure ustez, 6to4 eta Teredo tunelak egokiak dira SOHO sare baterako.

4.2.2.1. 6to4

6to4 tunelak mekanismo batzuk dira, IPv4 sareetara soilik konektatuak dauden IPv6 gailuei beste IPv6 sare batzuk atzitzeko aukera ematen dietenak. Horretarako, IANA[10] erakundeak 6to4 tunelentzat aurrez ezarritako helbide multzo batekin lan egiten dute; hain zuzen, 2002::/16 blokearekin.

6to4 tunelen mekanismoak honela lan egiten du: IPv6 helbide bat duen gailu batek haren saretik kanpora dagoen beste IPv6 helbide batekin komunikatu nahi du. Horretarako, 6to4 pseudointerfazeak onartzen dituen eta 2002::/16 aurrezenbakia bideratu dezakeen bideratzaile bat behar du sarean.

Gainera, IPv4 helbide publiko bat behar du gutxienez, helbide horretan oinarrituta bideratzailearen 6to4 helbidea kalkula dezan. Kalkulu hori honela egiten da:

10 http://www.iana.org/

1. IPv4 helbidea deskonposatu, eta nibble idazkeran jarri behar da. Adibidez:

192.0.2.1 IPv4 helbidea nibbleetan banatuz gero, hau lortzen dugu:

```
192 ---> C0
0 ---> 00
2 ---> 02
1 ---> 01
```

2. Erabiltzen ari garen bideratzailearen helbidearen lehen zatia eraikitzeko, 6to4 helbideentzat lehentxeago aipatutako aurrezenbakia erabili behar dugu, honela:

```
2002:C000:0201::/48
```

3. Dagoeneko badugu gure bideratzailearen aurrezenbakia. Orain, interfaze-identifikatzaile[11] bat, edozein, aukeratu behar dugu. Adibidez:

```
2002:C000:0201::1/128
```

6to4 tunelen funtzionamendua garatzen segitzeko, IPv6 sare batekin komunikatzen saiatzen ari den gailuaz eta 6to4 pseudointerfazea duen bideratzaileaz gainera (bideratzaile hori, normalean, irteerakoa izaten da), Interneten bideratzaile bat behar dugu, haren kontra tunela eraikitzeko. Baina, zer bideratzaile da hori? Interneten badira horrelako gailu batzuk anycast helbide mota dutenak; zehazki, 192.88.99.1[12] helbidea dute. Bestalde, helbide hori nibble idazkeran jartzen badugu, hau lortzen da: 2002:c058:6301::/128.

Hala, tunel bat izango dugu gure bideratzaileko IPv4 helbideen eta anycast helbidearen (192.88.99.1) artean. Horrekin, badugu 6to4-ren IPv6 aurrezenbaki bat (2002:C000:0201::/48) gure LAN sarean erabiltzeko, eta badugu, halaber, tunelaren bidez atzi daitekeen 2002:c058:6301::/128 helbidea. 2002::/16 aurrezenbakia interfaze horren bidez bideratu behar dugu.

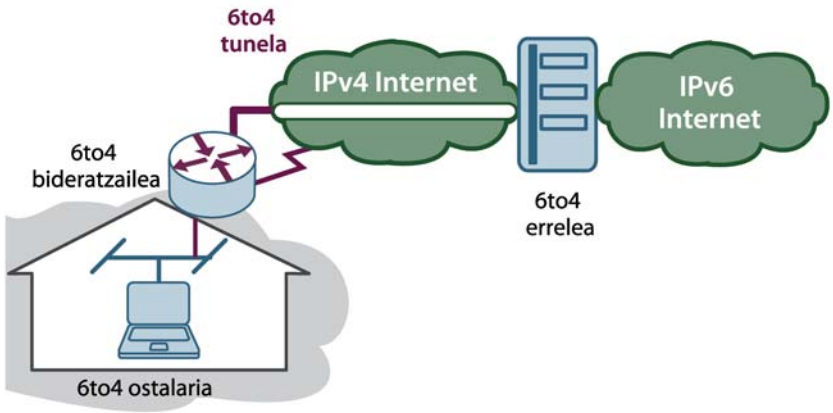
Cisco bideratzaile batean 6to4 tunel bat honela sortzen da, adibidez:

```
interface Tunnel2002
description Interneterako 6to4 tunela
no ip address
no ip redirects
ipv6 address 2002:C000:0201::/48
tunnel source GigabitEthernet0/0
tunnel mode ipv6ip 6to4

interface GigabitEthernet0/0
description 6to4-erako interfazea
ip address 192.0.2.1 255.255.255.0

ipv6 route 2002::/16 Tunnel2002
```

11 http://www.ietf.org/rfc/rfc3513.txt
12 http://www.ietf.org/rfc/rfc3068.txt



8. IRUDIA. **6TO4 TUNEL BATEN SORKUNTZA**

4.2.2.2. Teredo[13]

Teredo (edo, kode irekiko softwarean, Miredo) mekanismoak IPv6 sareak atzitzeko aukera ematen die gailuei, gailu horiek IPv4 motako NAT baten atzean daudenean.

Horretarako, zerbitzari bat behar da (adibidez, Linux edo BSD zerbitzari bat), eta zerbitzariak ematen ditu NAT itzultzailea zeharkatzeko IPv6 helbideak. Zerbitzariak Internetetik atzi daitekeen IPv4 helbide publiko bat eduki behar du.

Teredo zerbitzari horren zerbitzuekin Interneten sartu eta IPv6 helbideren batekin konektatu nahi duenari *Teredo bezero* deritzogu.

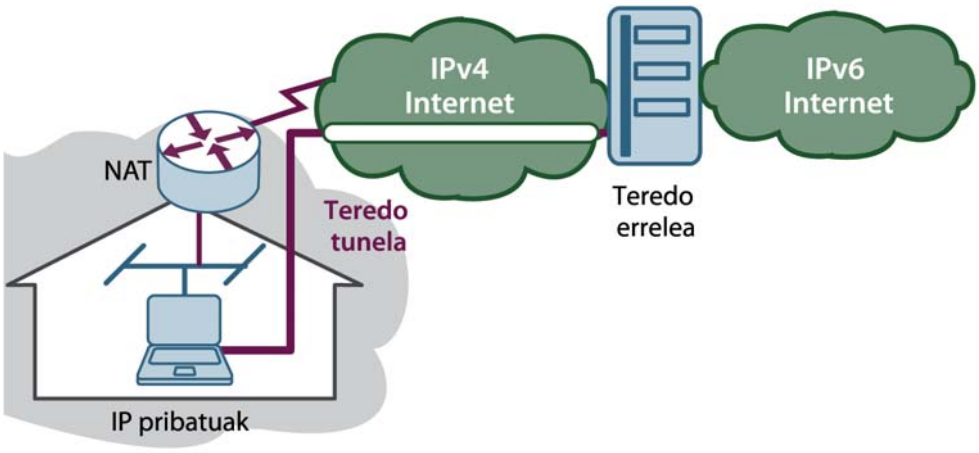
Teredo zerbitzariak Teredo bezeroaren eskariak jasotzen ditu UDP[14] protokoloko 3544 atakan, eta IPv6 helbide bat bidaltzen dio bezeroari, bere helburura iristeko erabil dezan.

Interneteko IPv6 helbideen eta gure Teredo bezeroaren artean trafikoa joan-etorrian ibiltzeko, Teredo errele baten bidez komunikatu behar dugu. Errele horrek Teredo bezeroaren IPv6 trafikoa jaso eta birbidali egiten du.

Bestalde, kontuan izan behar da Teredo zerbitzariak Interneten aldera Teredo aurrezenbakia jakinarazten duela (2001:0000::/32).

Honaino iritsi bagara, eta azaldutako urrats guztiak egin baditugu, IPv6 protokolora lotuak gaude, bai barnean, bai kanpoan. Beraz, gure egitekoa bete dugula esan genezake.

13 http://www.ietf.org/rfc/rfc4380.txt
14 http://www.ietf.org/rfc/rfc0768.txt



9. IRUDIA. **TEREDO/MIREDO TUNELEN FUNTZIONAMENDUAREN ESKEMA**

Bestalde, irakurleak kontuan izan behar du kapitulu honetan gure helburua dela bulego txiki bateko edo gure etxeko sarea IPv6-rekin aritzeko moduan jartzen laguntzeko tresna eta urrats batzuk jasotzea. Baina hemen jasotakoa ez da hori lortzeko modu bakarra. Aitzitik, IPv6-rako trantsizioko kontu praktiko guztietatik gutxi batzuk besterik ez ditugu azaldu.

5. Erreferentziak

http://portalipv6.lacnic.net/

http://www.ipv6tf.org

4. IPv6-rekin dabiltzan zerbitzuak

1. Sarrera

Kapitulu honetan, ikusiko dugu nola instalatu eta konfiguratu behar diren oinarrizko zerbitzu batzuk sistema eragile ohikoenetan, IPv6-rekin ibil daitezen. Gehien erabiltzen diren ia zerbitzu, aplikazio eta gailu guztiek onartzen dute IPv6 (zerrenda xehe bat dago *http://www.ipv6-to-standard.org* helbidean).

Argi izan behar dugu zerbitzu-aplikazioa edo zerbitzu-programa plataforma batean —alegia, zerbitzarian— exekutatzen dela, eta plataforma horrek bere sistema eragilea eta hardwarea dituela. Hori horrela, lehendabizi zerbitzariaren plataforman gaitu behar dugu IPv6, zerbitzaritik eta zerbitzarira datuak IPv6 protokoloaren arabera garraiatu ahal izateko. Sistema eragile desberdinetan IPv6 gaitzeko urratsak azken erabiltzaileari buruzko kapituluan (2. kapituluan) deskribatu ditugu. Ondoren, IPv6-rekin dabiltzan zerbitzuak martxan jartzeko, nahikoa da IPv6 onartzen duten programak instalatzea eta konfiguratzea; eta programa horiek, oro har, IPv4 onartzen duten programen bertsio hedatuak izaten dira.

2. Zerbitzuei buruz

Interneten eskaintzen diren zerbitzuak, edozein bezerok atzitzeko jartzen dira. Alegia, Interneteko zerbitzuetan, bezero-zerbitzari eredua bezero askok atzitzen duten zerbitzari batean oinarritzen da, eta bezeroak berak hasten du beti komunikazioa.

Zerbitzuak atzitzeko, zerbitzariaren sareko helbidea edo IP (Internet Protocol) helbidea zein den jakin behar da. Prozesu hori azken erabiltzaileentzat samurragoa izateko, DNS (Domain Name System) domeinu-izenen sistema sortu zen. Sistema horrek zerbitzari baten domeinu-izena haren IP helbidera itzultzen du. IP helbidea beharrean, izen hori erabiltzea komeni da.

Adibidez, web bezero batetik www.google.com helbidea atzitzean, Googleren orria bezeroari eskaintzen dion web-zerbitzari baten IP helbide bihurtzen da izen hori, erabiltzailea hortaz jabetu gabe.

DNSren bidez lortzen den IP helbidea honelakoa da: IPv4 soilik, IPv6 soilik, edo IPv4 eta IPv6. Horrela, IPv6-rekin dabiltzan zerbitzuak atzitzea erraza eta agerikoa da azken erabiltzailearentzat.

Ondoren, zerbitzu batzuk plataforma batzuetan nola instalatzen eta konfiguratzen diren aztertzen dugu.

3. Telnet

3.1. Zerbitzuaren deskribapena

Beste ekipo batekin komunikatzeko erabiltzen den aplikazio ezagun bat da Telnet; komando-interfaze baten bidez eta Telnet protokoloa eta TCP 23 ataka erabiliz egiten du komunikazioa. Bezero-zerbitzari ereduan oinarritzen denez, biak ala biak behar dira komunikaziorako. Telnet zerbitzaria *telnetd* programaren bidez instalatzen da.

3.2. Instalazioa eta konfigurazioa

Linuxen, badira banaketa desberdinentzako bertsioak. Ohikoenak honela instalatzen dira.

3.2.1. Debian

Instalatzeko, erabili hau:

```
# sudo apt-get install telnetd
```

Konfigurazio-fitxategia /etc/inetd.conf da.

Zerbitzua berrabiarazteko, erabili hau:

```
# sudo /etc/init.d/inetd restart
```

3.2.2. Fedora

Instalatzeko, erabili hau:

```
# yum install telnet-server telnet
```

Telnet instalatzen da, hain zuzen, xinetd prozesuak deitzen duen zerbitzu gisa. Telnet gaitzeko edo desgaitzeko, /etc/xinetd.d/telnet fitxategia aldatu behar da. Honela gaitzen da telnet: disable = no.

Bestalde, telnet berrabiarazteko, erabili hau:

```
# /etc/init.d/xinetd restart
```

3.2.3. Red Hat Enterprise

Instalatzeko, erabili hau:

```
# up2date telnet-server telnet
```

Telnet instalatzen da, hain zuzen, xinetd prozesuak deitzen duen zerbitzu gisa. Telnet gaitzeko edo desgaitzeko, /etc/xinetd.d/telnet fitxategia aldatu behar da. Honela gaitzen da telnet: disable = no.

Bestalde, telnet berrabiarazteko, erabili hau:

```
# /etc/init.d/xinetd restart
```

3.2.4. Ubuntu

Instalatzeko, erabili hau:

```
# sudo apt-get install telnetd
```


Konfigurazio-fitxategia /etc/inetd.conf da.

Zerbitzua berrabiarazteko, erabili hau:

```
# sudo /etc/init.d/openbsd-inetd restart
```

3.2.5. FreeBSD

FreeBSD bertsioan, telnet zerbitzariaren paketea lehenespenez instalatua dago, hemen: /usr/libexec/telnetd.

Konfigurazio-fitxategia /etc/inetd.conf da. Fitxategi horretan, telnet zerbitzaria gaitzeko, lerro honetako iruzkina (alegia, # ikurra) kendu behar da:

```
#telnet stream tcp nowait root /usr/libexec/telnetd telnetd
```

Ondoren, inetd zerbitzua gaitu behar da, telnet kargatzeko. Lerro hau gehitu behar da, /etc/rc.conf fitxategian:

```
inetd _ enable= "YES"
```

Azkenik, telnet zerbitzaria inetd zerbitzuaren bidez berrabiarazteko, erabili komando hau:

```
# /etc/rc.d/inetd restart
```

4. SSH

4.1. Zerbitzuaren deskribapena

Beste ekipo batekin komunikatzeko aukera ematen du SSHk; komando-interfaze baten bidez eta enkriptatzea darabilen kanal seguru bat eta TCP 22 ataka erabiliz egiten du komunikazioa. Normalean, telnet ordezten du, komunikazio seguru bat behar denetan. SSH ere bezero-zerbitzari ereduan oinarritzen denez, biak ala biak behar dira komunikaziorako. SSH zerbitzaria sshd programaren bidez instalatzen da.

4.2. Instalazioa eta konfigurazioa

Zenbait aplikazio daude SSH zerbitzarientzat. Linuxerako, Portable OpenSSH gailentzen da, eta BSDrako, berriz, Open SSH.

4.2.1. Debian/Ubuntu

Instalatzeko, erabili hau:

```
# sudo apt-get install openssh-server
```


Lehenespenez, instalatzean, SSH zerbitzaria gaitua gelditzen da. SSH zerbitzaria geldiarazteko, abiarazteko edo berrabiarazteko, erabili hauek:

```
# sudo /etc/init.d/ssh stop
# sudo /etc/init.d/ssh start
# sudo /etc/init.d/ssh restart
```

4.2.2. Red Hat Enterprise

Openssh-server-4.3p2-29.el5.i386.rpm paketeak eta berriagoek badute SSH zerbitzari bat (http://rpmfind.net). Exekutatzeko, erabili hau:

```
# rpm -ihv openssh-server-4.3p2-29.el5.i386.rpm
```

Zerbitzariak bi konfigurazio-fitxategi ditu: /etc/ssh/sshd_config eta /etc/ssh/ssh_host_key. Lehenengo fitxategia ezaugarri orokorrak konfiguratzeko erabiltzen da; fitxategi hori sistema jakin bakoitzari egokitzeko aldatu daitekeen arren, instalazioak lehenespenez dituen balioak nahikoak izaten dira SSH zerbitzaria erabiltzeko. Beste fitxategia, berriz, beste ostalariekiko komunikazioan erabilitako gakoak gordetzeko erabiltzen da.

Dena den, behar izanez gero, hau erabil daiteke sshd bat bilatu eta instalatzeko:

```
# up2date --showall | grep sshd
```

4.2.3. FreeBSD

OpenSSH sistema eragilearen parte da, eta ez da hura instalatzeko deus ere egin behar. Zerbitzua /etc/rc.conf fitxategian gaitzen da.

5. FTP

5.1. Zerbitzuaren deskribapena

FTP protokoloa urruneko ostalari bateko fitxategiak lortzeko edo urruneko fitxategi batera fitxategiak eramateko erabiltzen da. FTP protokoloak, normalean 20 eta 21 atakak erabiltzen ditu. Bezero-zerbitzari ereduan oinarritzen denez, biak ala biak behar dira komunikaziorako. FTP protokoloa ftpd programaren bidez instalatzen da.

5.2. Instalazioa eta konfigurazioa

FTP zerbitzariaren programa batek baino gehiagok onartzen du IPv6 (http://linuxmafia.com/faq/Network_Other/ftp-daemons.html). Ohiko batzuk honela instalatzen dira.

5.2.1. Red Hat

Pure-FTPd programa pure-ftpd-1.0.22.tar.gz bertsioan edo bertsio berriagoan instala daiteke (http://www.pureftpd.org). Instalatzeko, erabili hau:

```
# tar xzvf pure-ftpd-1.0.22.tar.gz
```

Sortutako karpetara joan, eta ohiko instalazio-komandoak exekutatu:

```
./configure
make
make install
```

5.2.2. Ubuntu

Proftpd programa instalatzeko, erabili hau:

```
# sudo apt-get install proftpd
```

6. Posta elektronikoa

6.1. Zerbitzuaren deskribapena

Posta elektronikoa gehien erabiltzen den zerbitzuetako bat da. Normalean, protokolo hauek erabiltzen dira: mezu elektronikoak bidaltzeko, SMTP (25 ataka); mezu elek-

tronikoak jasotzeko, POP3 (110 ataka) edo IMAP4 (143 ataka). Zerbitzua bezero-zerbitzari ereduan oinarritzen denez, biak ala biak behar dira komunikaziorako. Posta elektronikoaren zerbitzari eta bezero gehienek onartzen dute IPv6.

6.2. Instalazioa eta konfigurazioa

SMTPren, POP3ren eta IMAP4ren zerbitzari batek baino gehiagok onartzen du IPv6. Unix inguruneetarako, SMTP zerbitzari oso ezaguna da Sendmail (http://www.sendmail.org). Washingtongo Unibertsitatearen UW-IMAP programa, IMAP4 eta POP3 zerbitzarietarako dena, oso zabaldua dago (http://www.washington.edu/imap). Ondoren, programa horiek sistema eragile batzuetan nola instalatzen eta konfiguratzen diren azaltzen da.

6.2.1. Linux

Sendmail programa deskargatu eta instalatu behar da.

Sendmail programan, lehenespenez, IPv6 ez dago gaitua (8.12.x bertsiora arte, bederen, ez). IPv6 onartzea gaitzeko, devtools/Site/site.config.m4 konfigurazio-fitxategian lerro hau idatzi behar da:

```
APPENDDEF('confENVDEF', '-DNETINET6')
```


Eta Sendmail berreraiki (*rebuild*).

Ondoren, sendmail.mc fitxategian, lerro hau idatzi behar da:

```
DAEMON _ OPTIONS('Port=smtp, Name=MTA-v6, Family=inet6')dnl
```

Sendmail.cf berri bat egin, eta berrabiarazi Sendmail.

Errore-mezu bat jasoz gero, esleitutako liburutegiek IPv6 onartzen duten begiratu behar da, eta, onartzen ez badute, berreraiki egin behar dira IPv6 onar dezaten.

Bestalde, POP3/IMAP4 zerbitzari bat nahi izanez gero, UW-IMAP programa deskargatu eta instalatu behar da.

IPv6 onartzea gaitzeko, lerro hauek idatzi behar dira /etc/inetd.conf konfigurazio-fitxategian:

```
# IPv6 onartzen duen IMAP zerbitzaria
imap stream tcp6 nowait root /usr/sbin/tcpd imapd
# IPv6 onartzen duen POP3 zerbitzaria
pop-3 stream tcp6 nowait root /usr/sbin/tcpd ipop3d
```

UW-IMAP programa beharrean, Courier-IMAP programa erabiltzeko aukera ere badago. Horretarako, deskargatu eta instalatu Courier-IMAP programa (http://www.courier-mta.org/imap).

Courier-IMAP konpilatzean, sistema eragilean IPv6 onartzen dela hautematen bada, IPv6 automatikoki gaitzen da. Hori horrela, ez da beste urratsik egin behar.

6.2.2. FreeBSD

Deskargatu eta instalatu Sendmail.

IPv6 onartzea gaitzeko, etc/sendmail.ipv6.cf konfigurazio-fitxategian lerro hau idatzi behar da:

```
# SMTP daemonaren aukerak
O DaemonPortOptions= Port=smtp, Name=MTA-v6, Family=inet6,
Addr=[posta-zerbitzariaren IPv6 helbidea]
```

Sendmail zerbitzua abiarazteko, idatzi lerro hau /etc/rc.local fitxategian:

```
# IPv6 onartzen duen Sendmail SMTP zerbitzaria
/usr/sbin/sendmail -C/etc/sendmail.ipv6.cf -bd -q30m
```

Popper, bestalde, POP3 zerbitzari bat da. BSDn instalatzeko, erabili hau:

```
# cd /usr/ports/mail/popper
# make install
```


IPv6 onar dezan gaitzeko eta konfiguratzeko, /etc/inetd.conf fitxategian lerro hau idatzi behar da:

```
# IPv6 onartzen duen Popper POP3 zerbitzaria
pop3 stream tcp6 nowait root /usr/local/libexec/popper popper
```

6.2.3. Windows Server 2008

Windows Server 2008k sareko aplikazio guztietan eta zerbitzu nagusietan erabat onartzen du IPv6, Internet Information Services (IIS) aplikazioko SMTP zerbitzarietan izan ezik. Service Pack 1 duen Microsoft Exchange Server 2007n, ordea, SMTP zerbitzariak onartzen du IPv6. Exchange Serverren, IPv4-ren antzera instalatzen eta konfiguratzen da IPv6.

7. Multimedia-transmisioa

7.1. Zerbitzuaren deskribapena

Gero eta ohikoagoa da audioa eta bideoa Internet edo intranet bidez bidali behar izatea. Multimedia-transmisioa bezero-zerbitzari ereduan oinarritzen denez, biak ala biak behar dira komunikaziorako.

7.2. Instalazioa eta konfigurazioa

Multimediaren transmisioa egiten duten programa batek baino gehiagok onartzen du IPv6. Windows plataformetan, ohikoena Windows Media Services da. Honela instalatzen eta konfiguratzen da.

7.2.1. Windows Serverrak

Windows 2000, 2003 eta 2008 zerbitzarietan, Windows Media Services (WMS) aplikazioa erabil daiteke audioa eta bideoa zuzenean edo eskatu ahala transmititzeko. Windows Media Services aplikazioak iturburu kodetuen streaming-zerbitzari gisa jokatzen du, eta ataza hauek betetzen ditu, besteak beste: bezeroen eskaerei itxaron, erabiltzaile jakin baten konexioa baimendua dagoela egiaztatu, sare-konexioak kontrolatu, iturri kodetuak informazio erabilgarritzat hartuta streaming-paketeak eraiki, streaming-paketeak IPv4-rekin eta IPv6-rekin helburuei entregatu (helburuak unicast, anycast edo multicast izan daitezke, besteak beste).

- Windows Media Services aplikazioa Windows Server sistema eragileek jatorriz dakarten osagai bat da.
- Windows 2003 Serverren, behar izanez gero, honekin eguneratu daiteke: *http://download.microsoft.com/download/1/2/e/12e25064-8b99-4229-a554-acb67493742d/UpgradeWMS9S.exe*
- Windows 2008 Serverrek ere, sistemaren nukleoan, jatorriz dakar Windows Media Services 2008, edo, bestela, honekin instalatu daiteke: *http://www.microsoft.com/windows/windowsmedia/forpros/serve/prodinfo2008.aspx*

Multimedia-iturriak kodetzeko beharrezkoa izan liteke beste aplikazio bat ere: Windows Media Encoder (WME). Aplikazio horrek multimedia iturri batzuk kodetzen ditu (adibidez, DVD, audio- edo bideo-sarrera analogikoak, eta abar), eta transmisiorako erabil daitezkeen formatura bihurtzen ditu (adibidez, audioa mp3 bihurtzen du, edo bideoa, AVI). Windows Media Encoder aplikazioa multimedia transmititzeko ere erabil daiteke, baina bezero gutxi dagoenean besterik ez (bost bezero edo gutxiago). Aplikazio hori instalatzeko, erabili hau: *http://download.microsoft.com/download/8/1/f/81f9402f-efdd-439d-b2a4-089563199d47/WMEncoder.exe*

Windows Media Services aplikazioaren konfigurazio-interfazea honela atzitzen da: Programak > Administrazio-tresnak > Windows Media Services

Argitaratze-puntuak dira multimediaren transmisioaren oinarria.

7.2.1.1. Argitaratze-puntu berri baten sorrera

Bi eredu daude: **push** eta **pull**.

Push

Kodetzaileak abiarazten du multimedia-streamingaren transmisioa. Kodetzailean konfiguratzen da streaming-zerbitzaria zein den, eta, kodeketa abiarazten den aldiro, multimedia-fluxua zerbitzari horretara bidaltzen da. Hori da kudeaketa modu errazena, baina banda-zabalera handia behar dute kodetzaileak eta streaming-zerbitzariak, baita zerbitzarira konektatutako erabiltzailerik ez dagoenean ere.

Honela konfiguratzen da:

- Kodetzailean, Propietateak aukeran, sakatu Irteera, eta hautatu «Push to server (the connection is initiated by the encoder)».
  - Zerbitzariaren izena: streaming.adibidea.com:8100 (8100 atakako streaming-zerbitzaria da hori, balitekeelako 80 ataka web-zerbitzari batek hartua izatea).
  - Argitaratze-puntua. Publishing point: igorri_beharreko_gertaeraren_izena (hori izango da erabiltzaileen konexioaren argitaratze-puntua).
  - Kopiatu setting: push_test (streaming-zerbitzariaren konfigurazio hori «igorri_beharreko_gertaeraren_izena» argitaratze-puntua sortzeko kopiatzen da. Konfigurazio horrek streaminga kodetzailetik atera eta push:* jartzen du streaming motan).
- Konpresioa doitu daiteke: Propietateak > Konpresioa. Probak egiteko, komeni da streaming osoan gehienez 150 kbps izatea. Transmisioa egingo den tokian erabilgarri dauden sareen arabera, banda zabalagoak ere erabil daitezke.
- Hori egin eta gero, kodeketa abiarazten da Start Encoding-ekin, eta kodetzaileak streming-zerbitzarira bidaltzen du fluxua. Baliteke ohar bat agertzea, azaltzen duena argitaratze-puntua multicast erakoa bada zer urrats egin behar diren. Ez ikusi egin.
- Momentu jakin batean, kodetzaileak erabiltzaile-izena eta pasahitza eskatzen ditu, gure streaming-zerbitzarian argitaratzeko. Erabili *proba* erabiltzaile-izena, eta *4321* pasahitza.
- Erabiltzaile horrek WMSn idazteko baimena izan behar du, eta baimen hori streaming-zerbitzariaren propietateetan konfiguratzen da: propietateak > baimena > WMSko argitaratze-puntuen atzipen-kontroleko zerrenda.
- Streaming-zerbitzariaren propietateak ere gaitu behar dira: autentifikazioa > WMS -negoziazioaren autentifikazioa.
- Hala, zerbitzariak argitaratze-puntua automatikoki sortuko du, eta erabiltzaileak URL hauen bidez konektatu ahal izango dira puntu horretara:
  - *http://streaming.adibidea.com:8100/igorri_beharreko_gertaeraren_izena*
  - *mms://streaming.adibidea.com/igorri_beharreko_adibidearen_izena*
- Argitaratze-puntua banaketakoa da (ez eskaripekoa), eta interfaze grafiko berdea ageri da, urdina beharrean.

Pull

Honela konfiguratzen da:

- Kodetzailean, Propietateak aukeran, sakatu Irteera, eta hautatu Pull.

- WM Serverren, «atera» motako argitaratze-puntu bat konfiguratzen da, honelako URL batekin (adibidez):
  - *http://zerbitzariaren_Izena:zerbitzariaren_ataka*
- WM Serverren erabiltzaile baten konexio-eskaera bat jasotzen denean, Serverra kodetzailera konektatzen da, eta streaminga egiten du.

7.2.1.1. Gertaera baten transmisioa/grabazioa

Normalean, ezaugarri teknikoak direla eta, ordenagailu dedikatu bat behar izaten da (Windows 2003), eta Windows Media Encoder (WME) instalatzen zaio.

Kanpoko bideokamera bat erabiltzen bada, ordenagailu dedikatu bat izateaz gainera, bideoa kapturatzeko txartel bat instalatu behar da zerbitzari horretan, bideokamera konektatu ahal izateko. Dena den, USB-kamera bat erabil daiteke, eta orduan ez da bideoa kapturatzeko txartelik behar.

WME konfiguratu daiteke bai kamerako audioa edo bideoa kodetzeko, bai streamingaren transmisioa egiteko, eta bai disko gogor lokalean grabatzeko. Streamingeko bost konexio baino gehiago izatea espero bada, ezin da dena ordenagailu bakar batekin egin; ordenagailu bat behar da WMSrentzat eta beste bat WMErentzat. Dena den, saioa grabatzen duen zerbitzariaren prozesadorearen ahalmenaren araberakoa da muga hori. Streaming-zerbitzari eta kodetzaile bat erabiltzeko, lehentxeago azaldutako pull ereduaren argibideei jarraitu behar zaie.

8. Weba

8.1. Zerbitzuaren deskribapena

Web-nabigazioak HTTP protokoloa erabiltzen du hipertestuen, web-orrien eta HTML orrien transferentzia egiteko; eta web-nabigaziorako, normalean, 80 ataka erabiltzen da. Bezero-zerbitzari ereduan oinarritzen denez, biak ala biak behar dira komunikaziorako. Web-zerbitzaria edo HTTP instalatzeko, httpd programa erabiltzen da.

8.2. Instalazioa eta konfigurazioa

Gehien erabiltzen den zerbitzua da hau. Eta zerbitzu hau eskaintzeko, hainbat programa erabiltzen dira, baina Apache eta IIS erabiltzen dira gehien. Biak ala biak nola instalatu eta konfiguratu behar diren ikusiko dugu, IPv6-n oinarritutako eskaerei erantzun diezaieten.

8.2.1. Apache

Gaur egun, web-zerbitzari hedatuena da Apache, eta haren exekuzio-ingurune naturala Linux plataformak dira. IPv6 onartzeko, 2.x bertsioak erabili behar dira. Hemengo adibideak 2.0.63 bertsioan oinarritzen dira.

Instalatzeko, banaketa bakoitzaren ohiko sistemak erabil daitezke (apt-get install apache2, yum, up2date, rpm, eta abar), edo, bestela, http://httpd.apache.org helbidetik iturburu-fitxategiak deskargatu, eta konpilatu:

```
#>cd /usr/local/src
#>tar -xzvf httpd-2.0.63.tar.gz
#>cd httpd-2.0.63
#>./configure --prefix=/usr/local/apache2 --enable-module=so
#>make
#>make install
```

Instalazioa zer karpetatan egin behar den adierazten du --prefix parametroak. Eta --enable-module=so parametroak, berriz, Dynamic Shared Object (DSO) onartzea gaitzen du, moduluak dinamikoki kargatu ahal izateko (adibidez, PHP).

8.2.1.1. IPv6 entzutea

Apacheren 2.0.x bertsiotik aurrera, lehenespenez gaitua dago IPv6 onartzea. Hala, instalatu ondoren, abiarazi besterik ez da egin behar, IPv6-ren bidez entzun dezan. Ez ahaztu Linux zerbitzaria IPv6 onartzeko konfiguratu behar dela lehenik eta behin.

Listen aginduak kontrolatzen ditu Web-zerbitzariak entzuteko erabiltzen dituen IPak eta atakak, eta httpd.conf konfigurazio-fitxategi nagusian aurkitzen da. Lehenespenez, zerbitzariak IP guztien bidez eta 80 atakaren bidez (http) entzuten du:

```
Listen 80
```

Zerbitzariak 80 atakan IPv6-ren bidez entzuten duela egiaztatzeko, netstat komandoa erabil daiteke, honela:

```
[root]# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
...
tcp 0    0  :::80     :::*       LISTEN
...
```

Horrek adierazten du 80 atakatik (:80) zerbitzariaren edozein helbidetan (::) entzuten (LISTEN) ari dela (izan IPv4, izan IPv6).

8.2.1.2. Ostalari birtualak

IPv6 ostalari birtualak konfiguratzeko, IPv6 helbidea kako zuzenen artean ([]) bildu behar da. Adibidez:

```
NameVirtualHost [2001:db8:1::1000:1234]
NameVirtualHost 10.0.0.3

<VirtualHost [2001:db8:1::1000:1234]>
DocumentRoot /adibidea/htdocs/web-v4-v6
ServerName www.adibidea.com
</VirtualHost>

<VirtualHost 10.0.0.3>
DocumentRoot /adibidea/htdocs/web-v4-v6
ServerName www.adibidea.com
</VirtualHost>

<VirtualHost [2001:db8:1::1000:1234]>
DocumentRoot /adibidea/htdocs/web-soilik-v6
ServerName ipv6.adibidea.com
</VirtualHost>
```


Konfigurazio horren bidez, hau egin dezake zerbitzariak:

- IPv4 bidez 10.0.03 helbideari egindako eskaerei eta IPv6 bidez 2001:db8:1::1000:1234 helbideari egindako eskaerei erantzun
- Helbide horietan jasotako eskaerak URL desberdinei zuzenduak daude, eta horregatik bereizten dira. Horregatik,
- www.adibidea.com helbidera egindako eskaerei bai IPv4 eta bai IPv6 bidez erantzuten zaie, eta, horretarako, /adibidea/htdocs/web-v4-v6 fitxategiko edukia erabiltzen da.
- ipv6.adibidea.com helbidera egindako eskaerei IPv6 bidez soilik erantzuten zaie, eta horretarako, /adibidea/htdocs/web-soilik-v6 fitxategiko edukia erabiltzen da.

OHARRA: aurreko adibidean, ohikoena da www.adibidea.com-ek IPv4 eta IPv6 helbideak, biak, DNS bidez ebaztea. Halaber, ipv6.adibidea.com-ek IPv6 helbidea soilik ebatzi beharko luke. Gai horri buruz gehiago jakin nahi izanez gero, ikus DNSri buruzko atala, aurreraxeago.

8.2.1.3. Trikimailua: bezeroaren IPv6/IPv4 helbidea bistaraztea

Interesgarria izan liteke gure zerbitzariaren web-orrian bezeroak hura atzitzeko erabiltzen duen IP helbidea bistaraztea. Hori egiteko era bat baino gehiago dago, baina Li-

nux/Apache inguruneetan hedatuena PHP programazio-hizkuntza denez, hizkuntzahori erabiliz helbidea nola bistaraz daitekeen ikusiko dugu (adibide bat da).

Hasierako orrian (adibidez, index.php), kode hau idatzi behar da:

```
<?php if(strpos($ _ SERVER['REMOTE _ ADDR'],".")===false)
 {
 echo "<font color='#FF0000' size=2 face='verdana'>IPv6 erabiltzen
ari da (".$ _ SERVER['REMOTE _ ADDR']).</font><br><br>";
 }else{
 $DIRv4=str _ replace("::ffff:","",$REMOTE _ ADDR);
 echo "<font color='#FF0000' size=2 face='verdana'>IPv4 erabiltzen
ari da (".$ _ SERVER['REMOTE _ ADDR']).</font><br><br>";
 }
?>
```

8.2.1.4. Trikimailua: sendfile desgaitzea

Apache 2-k sendfile izeneko metodo bat onartzen du, sistema eragileak dakarrena, datuak zerbitzatzeko abiadura bizkortzeko. Sareko txartel-kontrolagailu batzuek ere TCP-checksum eragiketak lineaz kanpo egitea onartzen dute. Batzuetan, IPv6 bidezko trafikoarentzat, konexio-arazoak eta TCP-checksum okerrak sortzen ditu lineaz kanpo lan egiteak.

Horrelakoetan, sendfile desgaitu egin behar da, edo, bestela, zerbitzaria berriro konfiguratu, hain zuen, **--without-sendfile** konfigurazio-aukera erabiliz, edo Apacheren konfigurazio-fitxategian (httpd.com) **EnableSendfile off** agindua erabiliz.

EnableSendfile agindua 2.0.44 bertsiotik aurrera soilik onartzen da.

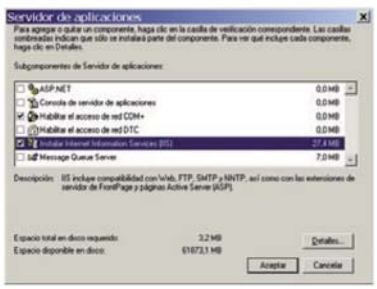
8.2.1.5. Badabilela egiaztatzea

Atzitzeko erabiltzen dugun helbidea bistarazteko amarruaz baliatuz, IPv4 bidez eta IPv6 bidez zerbitzaria atzi dezakegun ikus dezakegu zerbitzarian bertan dagoen nabigatzaile batekin. Horretarako, localhost IPv4 (127.0.0.1) eta IPv6 (::1) helbideak erabil daitezke.

8.2.2. IIS

Microsoften IIS (Internet Information Services) aplikazioaren ingurune naturala Windows zerbitzariak dira. Horregatik, hemen azaltzeko, Windows Server 2003 R2 SP2 Standard Edition eguneratua hartuko dugu plataformatzat. Plataforma horrek IISren 6.0 bertsioa dakar.

Instalatzeko eta desinstalatzeko, kontrol-paneleko **Gehitu edo kendu programak** erabili behar da. Egin klik **Gehitu/Kendu Windows osagaiak** aukeran, Windowsen osagaien morroia atzitzeko.



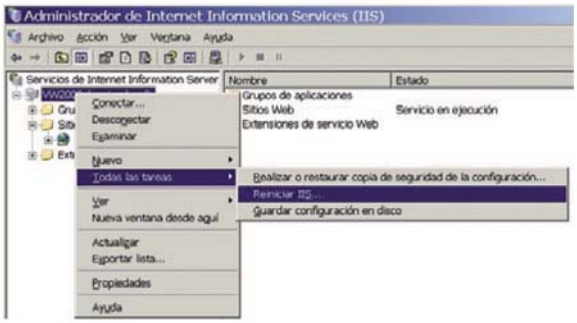
Windowsen osagaien morroian, hautatu **Aplikazio-zerbitzaria**, eta egin klik **Xehetasunak...** aukeran. Hautatu **Internet Information Services (IIS)** instalatzeko aukera, eta sakatu **Xehetasunak...**

Web-zerbitzaria ondo instalatzeko, osagai hauek gaitu behar dira: **Internet Information Services-eko (IIS) kudeatzailea, Fitxategi arruntak** eta **World Wide Web zerbitzua**.

OHARRA: Windows Server 2003ren instalazio-CDa behar da horretarako.

8.2.2.1. IPv6 entzutea

Zerbitzarian IIS-zerbitzaria eta IPv6 instalatu ondoren (*C:\netsh interface ipv6 install*), IIS-zerbitzaria berrabiaraztea komeni da, IPv6 bidez entzun dezan. Horretarako, Administrazio-tresnak aukerako **IIS-administratzailea** erabiltzen da. IIS exekutatzen den zerbitzaria hautatu behar da. Ondoren, eskuin botoiarekin klik eginez, Zeregin guztiak aukeraren barruan, IIS berrabiarazteko aukera agertzen da:



80 atakatik (http) IPv6 bidez entzuten dela egiazta dezakegu, honela:

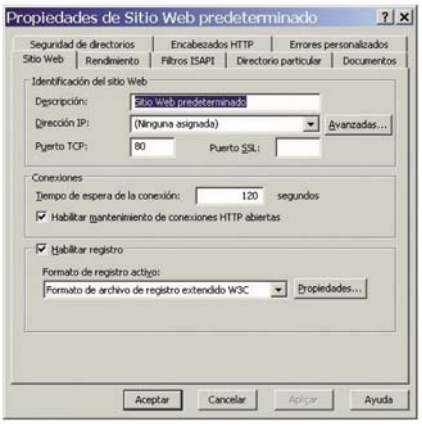
```
C:\>netstat -an -p tcpv6
Conexiones activas

Proto Dirección local  Dirección remota  Estado
TCP   [::]:80          [::]:0           LISTENING  0
...
```


8.2.2.2. IIS konfiguratzea

IIS, IPv6 bidezko web-orriak eman ditzan, web bakoitzerako konfiguratzen da. Horretarako, Administrazio-tresnak aukerako **IIS-administratzailea** erabiltzen da.

Web-orri baten ezaugarriak konfiguratzeko, egin klik eskuin-botoiarekin konfiguratu nahi den web-orriaren gainean, eta hautatu Propietateak:



Webgunearen fitxan, IP-helbidean, bat ere esleitu gabe utzi behar da. Hala, 80 atakatik eta IPv4 eta IPv6 helbide guztien bidez entzuten da. Xehetasunak gehitu daitezke, Aurreratuak... aukeran sartuta.

Beheko irudiko adibidean, webgune bat atzitzeko hiru era hauek ageri dira:

- **IPv4 soilik:** *ipv4.adibidea.com*, 192.168.1.101 IPv4-ra ebazten duena.
- **IPv4 eta IPv6:** *www.adibidea.com*, zerbitzariaren IPv4 eta IPv6 helbideetara ebazten duena.
- **IPv6 soilik:** *ipv6.adibidea.com*, zerbitzariaren IPv6 helbidera ebazten duena.

Beste adibide hau sinpleagoa da; atzipena edozein IP erabiliz eta edozein domeinu-izenekin egiten uzten du:

8.2.2.3. Trikimailua: bezeroaren IPv6/IPv4 helbidea bistaraztea

Interesgarria izan liteke gure zerbitzariaren web-orrian bezeroak hura atzitzeko erabiltzen duen IP helbidea bistaraztea. Hori egiteko modu bat erakutsiko dugu, ASP programazio-hizkuntzan oinarritutakoa, hori baita Windows/IIS inguruneetan gehien erabiltzen dena.

Hasierako orrian (adibidez, default.asp), kode hau idatzi behar da:

```
<%
 if InStr(Request.ServerVariables("REMOTE _ ADDR"),".") = 0 then
   response.Write( "<font color='#154983' size=2 face='verdana'>
IPv6 erabiltzen ari da.<br><br>")
 else
   response.Write ("<font color='#FF0000' size=2 face='verdana'>
IPv4 erabiltzen ari da.<br><br>")
 end if

   response.Write ("(" &Request.ServerVariables("REMOTE _ ADDR")
& ")</font><br><br>")
%>
```

OHARRA: ASP orriak, behar bezala funtzionatzeko, IIS-administratzaileko web-zerbitzuen luzapenetan onartu behar dira, honela:

8.2.2.4. Badabilela egiaztatzea

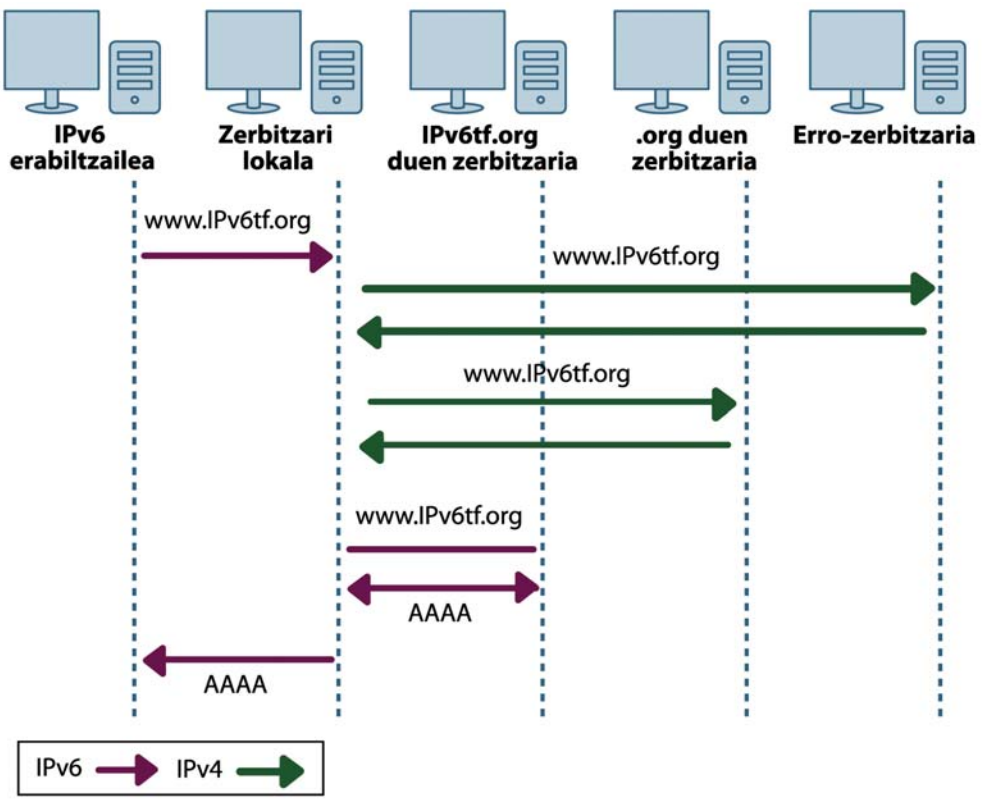
Atzipen-helbidea bistarazteko amarruaz baliatuz, zerbitzarian bertan dagoen nabigatzaile batekin ikus dezakegu IPv4 bidez eta IPv6 bidez zerbitzaria atzi dezakegun. Horretarako, localhost IPv4 (127.0.0.1) eta IPv6 (::1) helbideak erabil daitezke.

9. DNS

9.1. Zerbitzuaren deskribapena

Domeinu-izenak sareko (bai IPv4-ko, bai IPv6-ko) helbide bihurtzen ditu DNS sistemak, eta oinarrizko funtzioa betetzen du gaur egungo Interneten.

Ez dugu DNSren erabilera xehe azalduko, baina argi izan behar dugu gauza bat dela DNS trafikoaren garraioa (IPv4 eta/edo IPv6 sare baten bidez), eta beste gauza bat direla DNS zerbitzarietako datuak (IPv4-rako A erregistroak eta IPv6-rako AAAA erregistroak). Eta hori horrela da, garraiorako erabiltzen den IP protokoloa erabiltzen dela. Irudi honetan ikusten da, hain zuzen, nola, IPv6 (AAAA) helbide bat ebazteko, IPv4 eta IPv6 garraioak desberdin erabiltzen diren.



1. IRUDIA. **GARRAIOAREN ETA EDUKIAREN ARTEKO DIFERENTZIA, DNSN**

Horregatik ikusiko dugu, batetik, zerbitzaria nola konfiguratzen den IPv6 eskaerei erantzun diezaien (garraioa), eta, bestetik, IPv6-rekin erlazionatutako datuak zerbitzariak emandako edukietan nola sartzen diren (datuak).

Gaur egun, DNS zerbitzari guztiak pila bikoitzekoak izatea komeni da, alegia, bai IPv4 eta bai IPv6 bidezko eskaerak onartzeko gai izatea, DNSren azpiegitura guztiak ez duelako IPv6 onartzen. Gainera, lehendik dauden zerbitzariekin bateragarria izatea bermatzen da horrela.

Kontuan hartu beharreko kontzeptuak dira, halaber, domeinu baten zerbitzari maisu edo primarioa eta zerbitzari sekundario edo morroia. Hitz gutxitan esateko, zerbitzari maisuan sortzen eta eguneratzen dira DNSren datuak, ondoren zerbitzari morroietara automatikoki hedatzeko.

9.2. Instalazioa eta konfigurazioa

DNSren zerbitzari-programa batzuek onartzen dute IPv6. Bai IPv4-n bai IPv6-n, BIND eta Windows DNS Server erabiltzen dira gehien (UNIX motako eta Windows plataformetarako, hurrenez hurren), eta horiek biak nola instalatzen diren ikusiko dugu.

9.2.1. BIND

BIND (Berkeley Internet Name Domain) da, gaur egun, DNS zerbitzari hedatuena, eta haren exekuzio-ingurune naturala Linux plataformak dira. Konfiguratzeko, testu-fitxategiak editatu behar dira.

Instalatzeko, banaketa bakoitzaren ohiko sistemak erabil daitezke (apt-get, yum, up2date, rpm, eta abar), edo, bestela, *https://www.isc.org/software/bind* helbidetik iturburu-fitxategiak deskargatu, eta konpilatu:

```
# tar -xzvf bind-9.4.2-P2.tar.gz
# cd bind-9.4.2-P2
# ./configure
# make
# make install
```

Lehendik dagoen instalazio bat oinarri hartuta (BIND 9.4.2-P2), hauek nola egin ikusiko dugu:

- IPv6 bidezko eskaerei erantzutea gaitu (IPv6 entzun).
- IPv6 helbideak domeinu-izenei esleitu (AAAA erregistroak).
- IPv6 helbidetik domeinu izenerako alderantzizko ebazpena (PTR erregistroa).

9.2.1.1. IPv6 entzutea

DNS zerbitzariaren konfigurazioa duen fitxategi nagusia, gure kasuan, /etc/named.conf da, eta han egin behar dira egin beharreko aldaketak.

Zerbitzarian IPv6 bidez entzutea gaitzeko, options atalean listen-on-v6 {}; agindua gehitu behar da, halako moldez, non named.conf-en hasieran gelditzen baita, honela edo antzera:

```
options {
    directory "/var/named/";
    listen-on-v6 { any; };
};
```

Hala, zerbitzariak dituen IPv6 helbide guztietan entzuten du DNS zerbitzariak.

9.2.1.2. AAAA erregistroak

IPv6 helbideak AAAA motako erregistrotan gordetzen dira DNSn. DNS zerbitzari guztiek badituzte zona-fitxategi deritzenak, zeinetan DNSren informazioa, azpidomeinu batekin erlazionatutakoa, baitago. Guk adibidea.com azpidomeinua erabiliko dugu.

BINDen, zerbitzariak bere gain dituen zonak /etc/named.conf-en konfiguratzen dira. Adibidez, /var/named/adibidea.com.zone fitxategian dagoen zona adibidea.com azpidomeinuaren zerbitzari maisu edo primarioa[1] abiatzean kargatu behar dela adierazten da:

```
zone "adibidea.com" {
    type master;
    file "adibidea.com.zone";
};
```

Zuzenean ebazteko zonako fitxategietako erregistroen helbideak IPv4, IPv6 nahiz biak batera izan daitezke. Lehengo adibidearekin jarraituz, /var/named/adibidea.com.zone editatu, eta hau erantsiko diogu:

```
ipv4-ipv6 IN   A    10.0.0.3
   IN   AAAA  2001:db8:1:0:0:0:1234:5678

ipv6    IN   AAAA  2001:db8:1:0:0:0:1234:5678

ipv4         IN  A    10.0.0.3
```


Hala, hau egiteko konfiguratu dugu:

- ipv4.adibidea.com-ek IPv4 helbide batera soilik ebazten du (10.0.0.3).
- ipv6.adibidea.com-ek IPv6 helbide batera soilik ebazten du (2001:db8:1:0:0:0:1234:5678).
- ipv4-ipv6.adibidea.com-ek IPv4 helbide batera eta IPv6 helbide batera ebazten du, aldi berean (sistema eragileak eta/edo aplikazioak erabakitzen du helbide bata ala bestea erabili).

9.2.1.3. PTR erregistroak

Mota horretako PTR erregistroak ez dira berriak; horrelakoak erabiltzen dira IPv4 helbidetik domeinu-izenerako alderantzizko ebazpenean. IPv6 helbideak adierazteko erabilitako notazioan (nibbleen bidezko idazkera[2]) eta horretarako erabilitako domeinuaren izenean (IP6.ARPA) datza aldea. IPv6 helbideen alderantzizko ebazpena egiteko zona-fitxategiek IPv6 helbideak soilik izango dituzte.

Ikus dezagun adibide bat, IPv6-rekin:

Gure sareentzat eman diguten 2001:db8:1::/48 aurrezenbakiari dagokion alderantzizko ebazpenaren zona adierazten da /etc/named.conf-en:

1 Sekundarioa edo morroia izateko, erabili type slave;
2 Nibble bat lau bit dira; horregatik, oinarri hamaseitarrean idazten da.

```
zone "1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
type master;
file "2001 _ 0db8 _ 0001.zone";
};
```

Aurrezenbakia nibbletan banatzen da, eta nibbleak ip6.arpa domeinuaren alderantzizko ordenan lotzen dira.

2001_0db8_0001.zone fitxategiak hau edukiko du:

```
$TTL 86400
@ IN SOA ns1.adibidea.com. dnsadmin.adibidea.com (
  2002071901 ; serial
  28800 ; refresh
  7200 ; retry
  604800 ; expire
  86400 ; ttk
  )
IN NS ns1.adibidea.com.

4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR www.adibidea.com.
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR ipv6.adibidea.com.
```

Alegia:

- 2001:db8:1::1000:1234 helbideak *www.adibidea.com* domeinu-izenera ebatziko du.
- 2001:db8:1::1234:5678 helbideak *ipv6.adibidea.com* domeinu-izenera ebatziko du.

Kontuan izan behar da IPv6 helbide batek 32 nibble dituela. Hori horrela, named.conf-en adierazitako nibbleek (gure adibidean, 12) eta zona-fitxategiko helbide bakoitzaren nibbleek (gure adibidean, 20), guztira, 32 izan behar dute.

9.2.1.4. Konfigurazioa probatzea

Aldaketak aplikatu diren ikusteko, DNS zerbitzaria berrabiarazi behar da (gure adibideko sisteman, /etc/init.d/named restart erabiliz).

Zerbitzaria DNS atakan (53 atakan) IPv6 eta IPv6 helbideetan entzuten ari dela ikus daiteke:

```
# netstat -tan
Proto Recv-Q Send-Q Local Address    Foreign Address  State
...
tcp  0  0 ::1:53          :::*    LISTEN
tcp  0  0 2001:db8:1:0:0:0:1234:5678:53 :::*     LISTEN
tcp  0  0 10.0.0.3:53        0.0.0.0:* LISTEN
tcp  0  0 127.0.0.1:53        0.0.0.0:*  LISTEN
...
```

Zerbitzarian bertan, dig aplikazio bezeroa erabil daiteke; aplikazio horrek gure zerbitzariari kontsultak egiteko aukera ematen du.

Adibidez, *ipv6.adibidea.com* ebazteko:

```
# dig any ipv6.adibidea.com

; <<>> DiG 9.4.2-P2 <<>> any ipv6.adibidea.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48527
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
; ipv6.adibidea.com.          IN   ANY

;; ANSWER SECTION:
ipv6.adibidea.com.   172800  IN  AAAA  2001:db8:1:0:0:0:1234:5678
...
;; Query time: 4 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Jun 17 17:23:48 2009
;; MSG SIZE rcvd: 296
```


Eta *ipv4.adibidea.com* ebazteko:

```
# dig any ipv4-ipv6.adibidea.com

...
;; QUESTION SECTION:
; ipv4-ipv6.adibidea.com.          IN   ANY

;; ANSWER SECTION:
ipv4-ipv6.adibidea.com. 172800 IN A  10.0.0.3
ipv4-ipv6.adibidea.com. 172800 IN AAAA 2001:db8:1:0:0:0:1234:5678
...
```

Azkenik, 2001:db8::1000:1234-ren alderantzizko ebazpena egiteko:

```
# dig -x 2001:db8::1000:1234

; <<>> DiG 9.4.2-P2 <<>> -x 2001:db8::1000:1234
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1333
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.
arpa. IN PTR
```

```
;; ANSWER SECTION:
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
172800 IN PTR www.adibidea.com.

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Jun 17 17:37:02 2009
;; MSG SIZE rcvd: 270
```

9.2.1.5. Aztarna-fitxategia (aparteko atala)

Aztarna-fitxategi baten erabilera /etc/named.conf-en konfiguratzen da. Aztarnen (hints) fitxategiek DNSren erro-zerbitzarien IP helbideak dauzkate.

```
zone "." {
    type hint;
    file "named.root";
};
```

Ez gara xehetasunetan sartuko, baina zerbitzari horiek orain dela gutxitik dira IPv6 bidez atzigarriak (2008ko otsailaren 4tik aurrera, hain zuzen), eta aztarna-fitxategia behar bezala eguneratu da.

Horregatik, DNS zerbitzarian IPv6-ren konfigurazioa osatzeko, aztarna-fitxategia eguneratu behar da, erro-zerbitzarien IPv6 helbideak eduki ditzan (halako helbideak badauzkate, noski). Adibidez, http://www.internic.net/zones/named.root-en erabilgarri dagoen azkena 2008ko abenduaren 12koa da; han, hamahiru erro-zerbitzarietatik zazpik badute IPv6 helbide bat esleitua.

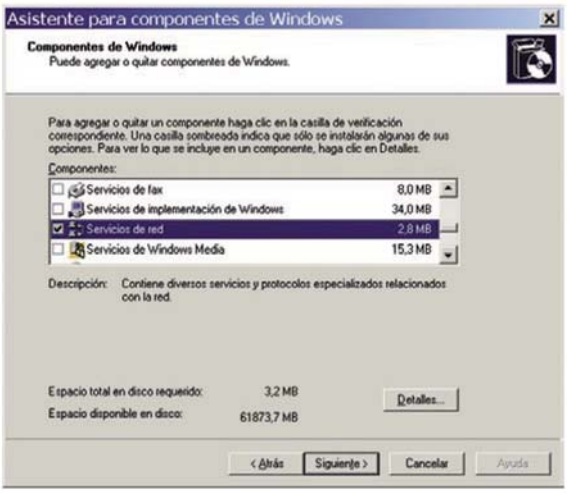
Hau da, adibidez, named.root fitxategiaren edukia:

```
.          3600000  IN NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.    3600000   A   198.41.0.4
A.ROOT-SERVERS.NET.    3600000   AAAA 2001:503:BA3E::2:30
```

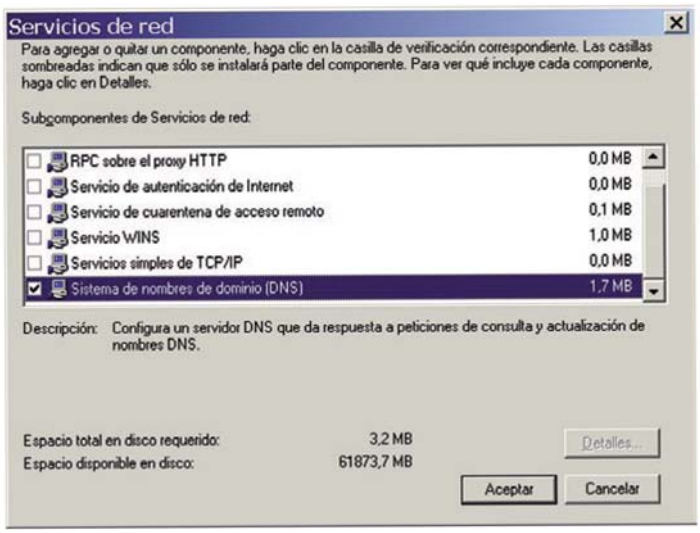
9.2.2. Windows DNS Server

Microsoften Windows DNS Server aplikazioaren ingurune naturala Windows zerbitzariak dira. Horregatik, hemen azaltzeko, Windows Server 2003 R2 SP2 Standard Edition eguneratua hartuko dugu plataformatzat.

Instalatzeko eta desinstalatzeko, kontrol-paneleko **Gehitu edo kendu programak** erabili behar da. Egin klik **Gehitu/Kendu Windows osagaiak** aukeran, Windowsen osagaien morroia atzitzeko.



Windowsen osagaien morroian, hautatu sareko zerbitzuak, eta egin klik Xehetasunak... aukeran. DNS zerbitzariari Domeinu-izenen sistema (DNS) deritzo:



OHARRA: Windows Server 2003ren instalazio-CDa behar da horretarako.

9.2.2.1. IPv6 entzutea

Zerbitzarian DNS zerbitzaria eta IPv6 instalatu ondoren (C:\>netsh interface ipv6 install), DNS zerbitzariak IPv6 bidez entzutea lortu behar da. Horretarako, hau erabili behar da:

```
C:\>dnscmd /config /EnableIPv6 1
Registry property EnableIPv6 successfully reset.
Command completed successfully.
```

OHARRA: Windows Server 2003 Support Toolsen parte da dnscmd.exe, eta Windows Server 2003ren CDko Support\Tools karpetan aurkitzen da. Instalatzeko, karpeta horretako suptools.msi exekutatu behar da.

IPv6 bidez entzuten hasteko, zerbitzaria edo DNS zerbitzaria berrabiarazi behar da. Horretarako, joan Administrazio-tresnak aukerara, eta exekutatu zerbitzuen kudeaketako aplikazioa. Bilatu DNS zerbitzaria, eta berrabiarazi.

DNS zerbitzariak (53 ataka) IPv6-ren bidez entzuten duela egiaztatzeko, netstat komandoa erabil daiteke, honela:

```
C:\>netstat -a -n -p udpv6
Conexiones activas
  Proto  Dirección local      Dirección remota  Estado
  UDP    [::]:53          [::]:0       LISTENING  0
  …
  UDP    [2001:db8:1::1000:1234]:53  [::]:0        LISTENING  0
  UDP    [fe80::1%1]:53      [::]:0         LISTENING  0
  UDP    [fe80::ffff:ffff:fffd%6]:53 [::]:0   LISTENING  0
  UDP    [fe80::200:1cff:feb5:5a88%5]:53  [::]:0    LISTENING  0
```

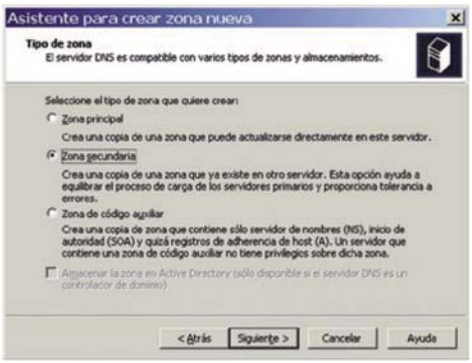
9.2.2.2. AAAA erregistroak

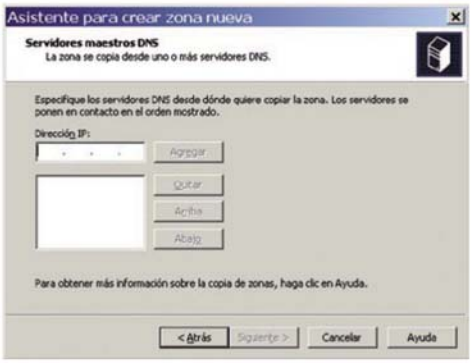
Zerbitzaria IPv6 helbideekiko AAAA erregistroak dauzkan zona baterako morroia edo sekundarioa bada, konfiguratzeko, interfaze grafikoa erabil daiteke. Hori, baldin eta zonako zerbitzari maisuak eta gainerako morroiek IPv4 helbide erabilgarri bat badute, interfaze grafikoak ez baitu uzten haientzat IPv6 helbideak sartzen.

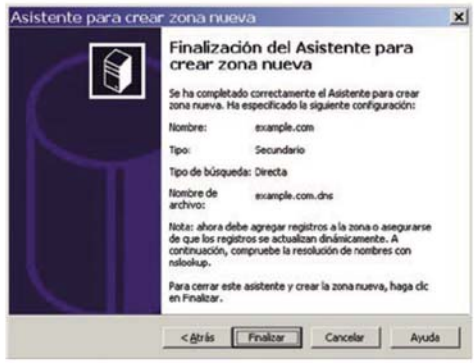
Domeinu berri bat, zerbitzaria morroi edo sekundario duela konfiguratzeko, konfigurazioaren interfaze grafikoa erabili behar da; alegia, Administrazio-tresnak aukeraren barruan dagoen DNS tresna.

Horretarako, domeinu-izenetik IPrako ebazpen-zona bati dagokionez, egin klik eskuin-botoiarekin bilaketa zuzeneko zonetan. Hautatu Zona berria, eta zona berri bat sortzeko morroia irekitzen da:

Hautatu zona sekundarioa zona mota gisa, jarri zona-izena (adibidez, adibidea.com), eta konfiguratu zerbitzari maisuen IPv4 helbideak (zerbitzari primarioarena eta, baleude, beste sekundarioenak).







Zerbitzaria IPv6 helbideekiko AAAA erregistroak dauzkan zona baten zerbitzari maisu edo primarioa bada, konfiguratzeko[3], komando-interfazea erabili behar da, hain zuzen, dnscmd komando-interfazea. Komando hauek daude erabilgarri, besteak beste[4]:

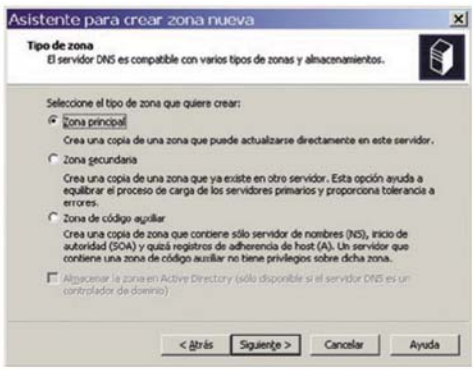
- **Zona bat gehitzeko**: dnscmd serverName /ZoneAdd zoneName zoneType [options]
- **Zona bat ezabatzeko:** dnsdmd serverName /ZoneDelete zoneName [/DsDel] [/f]
- **Erregistro bat gehitzeko:** dnscmd serverName /RecordAdd zoneName nodeName [/Aging] [/OpenAcl] [Ttl] typeRR dataRR
- **Erregistro bat ezabatzeko:** dnscmd serverName /RecordDelete zoneName nodeName typeRR dataRR [/f]
- **Zerbitzariaren zonak ikusteko:** dnscmd serverName /Enumzones
- **Zona baten edukia ikusteko:** dnscmd serverName /ZonePrint zoneName
- **Domeinu-izen bati lotutako erregistroak ikusteko:** dnscmd serverName> / EnumRecords <ZoneName> <NodeName>

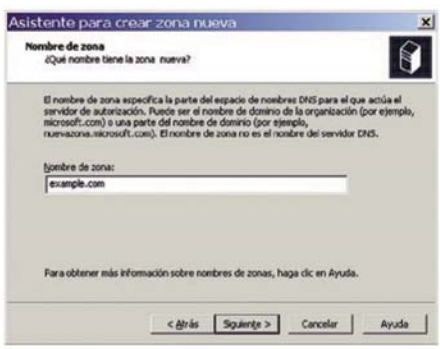
3 Zerbitzari sekundarioa edo morroia balitz eta IPv4 bidez atzi litekeen beste zerbitzaririk ez balego ere, komandoak erabiliko genituzke.
4 Erabili dnscmd /? erabilgarri dauden komandoei buruzko informazioa lortzeko. Erabili dnscmd <komandoa> /? komando jakin bati buruzko laguntza lortzeko.

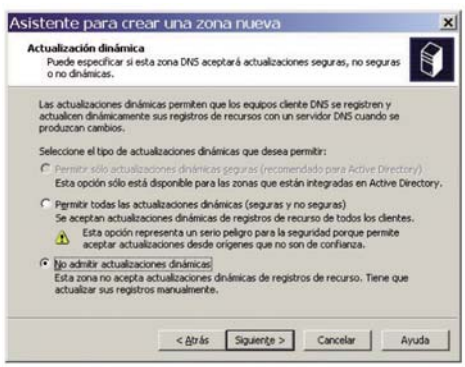
Ikus dezagun, adibide batean, zerbitzaria primariotzat duen adibidea.com zona bat nola sortzen den. Zona horrek, gainera, ezaugarri hauek ditu:

- ipv4.adibidea.com-ek IPv4 helbide batera soilik ebazten du (10.0.0.3).
- ipv6.adibidea.com-ek IPv6 helbide batera soilik ebazten du (2001:db8:1:0:0:0:1234:5678).
- ipv4-ipv6.adibidea.com-ek IPv4 helbide batera eta IPv6 helbide batera ebazten du, aldi berean (aplikazioak erabakitzen du helbide bata ala bestea erabili).

Lehenbizi, interfaze grafikoan, zona sortu behar da. Horretarako, domeinu-izenetik IPrako ebazpen-zona bati dagokionez, egin klik eskuin-botoiarekin bilaketa zuzeneko zonetan. Hautatu Zona berria, eta zona berri bat sortzeko morroia irekitzen da:







Ondoren, sartu erregistroak, komando-lerroaren bidez:

```
C:\>dnscmd ::1 /RecordAdd adibidea.com ipv4 A  10.0.0.3
Add A Record for ipv4.adibidea.com at adibidea.com
Command completed successfully.

C:\>dnscmd ::1 /RecordAdd adibidea.com ipv6 AAAA 2001:
 db8:1:0:0:0:1234:5678
Add AAAA Record for ipv6.adibidea.com at adibidea.com
Command completed successfully.

C:\>dnscmd ::1 /RecordAdd adibidea.com ipv4-ipv6 A 10.0.0.3
Add A Record for ipv4-ipv6.adibidea.com at adibidea.com
Command completed successfully.

C:\>dnscmd ::1 /RecordAdd adibidea.com ipv4-ipv6 AAAA 2001:
 db8:1:0:0:0:1234:5678
Add AAAA Record for ipv4-ipv6.adibidea.com at adibidea.com
Command completed successfully.
```

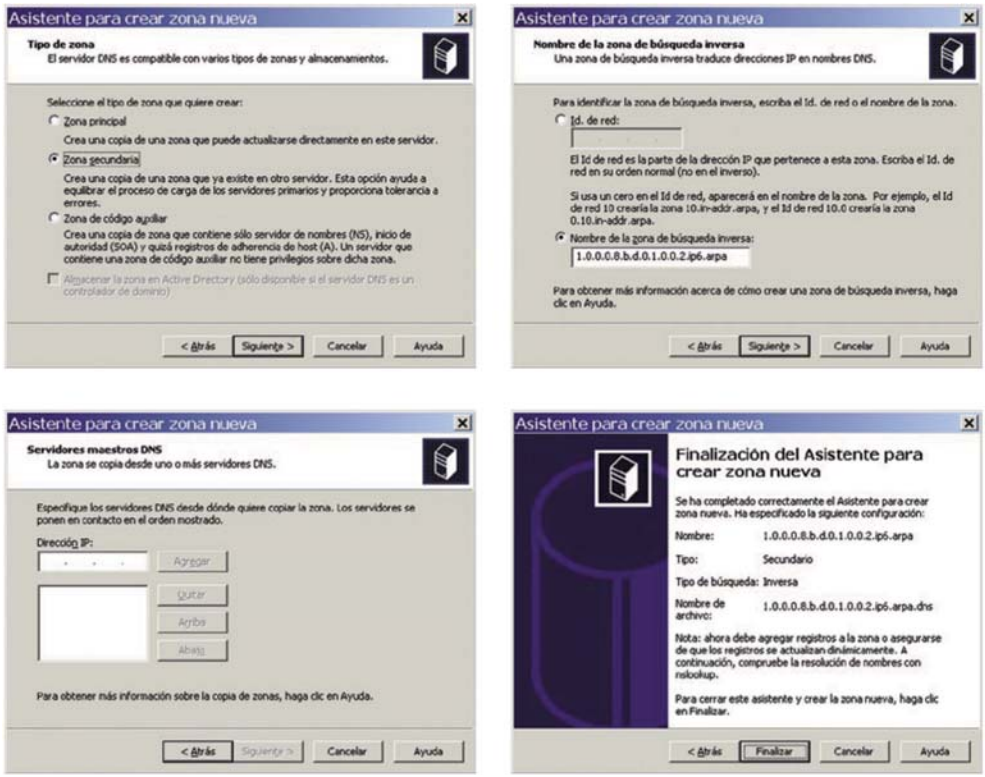
9.2.2.3. PTR erregistroak

Zerbitzaria domeinu-izenekiko PTR erregistroak dauzkan zona batentzat morroia edo sekundarioa bada, orduan, konfiguratzeko, interfaze grafikoa erabil daiteke. Hori, baldin eta zonako zerbitzari maisuak eta gainerako morroiek IPv4 helbide erabilgarri bat badute, interfaze grafikoak ez baitu uzten haientzat IPv6 helbideak sartzen.

Domeinu berri bat zerbitzaria morroi edo sekundario duela konfiguratzeko, konfigurazioaren interfaze grafikoa erabili behar da; alegia, Administrazio-tresnak aukeraren barruan dagoen DNS tresna.

Horretarako, egin klik eskuin-botoiarekin alderantzizko bilaketako zonetan, IPv6 helbideetatik domeinu-izenerako ebazpen-zona baterako. Hautatu Zona berria aukera, eta zona berri bat sortzeko morroia irekitzen da:

Hautatu zona sekundarioa zona mota gisa, jarri zona-izena (adibidez, 2001:db8:1::/48 aurrezenbakiaren alderantzizko ebazpenerako, 1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa), eta konfiguratu zerbitzari maisuen IPv4 helbideak (zerbitzari primarioarena eta, baleude, beste sekundarioenak).



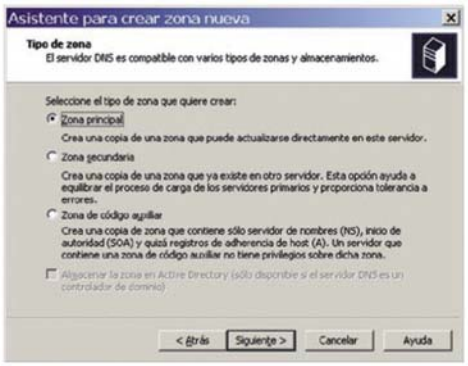
Zerbitzaria IPv6 helbideak ematen dituzten PTR erregistroak dauzkan zona baten zerbitzari maisu edo primarioa bada, konfiguratzeko[5], komando-interfazea erabili behar da, hain zuzen, dnscmd komando-interfazea. Aurreko atalean, maizen erabiltzen diren komandoei buruzko xehetasunak eman ditugu.

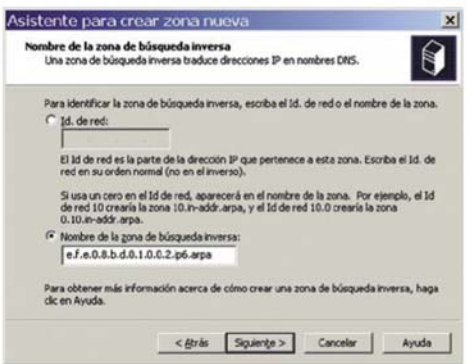
Ikus dezagun, adibide batean, zerbitzaria primariotzat duen zona bat (e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa) nola sortzen den. Zona hori 2001:db8:efe::/48 aurrezenbakiari dagokio, eta, gainera, han:

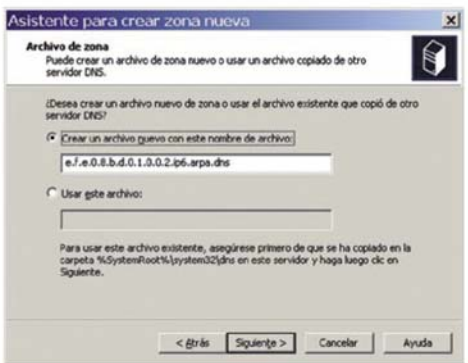
- 2001:db8:efe::1000:1234 aurrezenbakiak, ebaztean, www.adibidea.com ematen du.
- 2001:db8:efe::1234:5678 aurrezenbakiak, ebaztean, ipv6.adibidea.com ematen du.

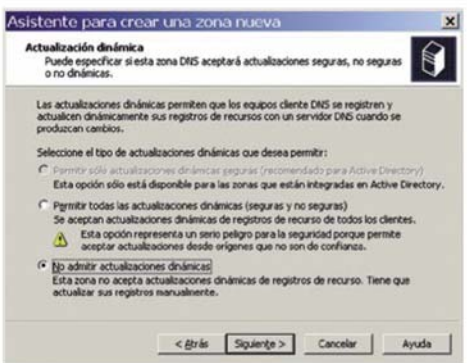
5 Zerbitzari sekundarioa edo morroia balitz eta IPv4 bidez atzi litekeen beste zerbitzaririk ez balego ere, komandoak erabiliko genituzke.

Lehenbizi, zona sortu behar da interfaze grafikoan. Horretarako, egin klik eskuinbotoiarekin alderantzizko bilaketako zonetan, IPv6 helbidetik domeinu-izenerako ebazpen-zona bati dagokionez. Hautatu Zona berria, eta zona berri bat sortzeko morroia irekitzen da:









Ondoren, sartu erregistroak, komando-lerroaren bidez:

```
C:\>dnscmd ::1 /RecordAdde.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa4.3.2.1.0
  .0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR www.adibidea.com.
Add PTR Record for 4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d
  .0.1.0.0
.2.ip6.arpa at e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
Command completed successfully.
```

```
C:\>dnscmd ::1 /RecordAdd e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa 8.7.6.5.4
 .3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR ipv6.adibidea.com.
Add PTR Record for 8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d
 .0.1.0.0
.2.ip6.arpa at e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
Command completed successfully.
```

9.2.2.4. Konfigurazioa probatzea

Interfaze grafikoan errazago ikusten da informazioa, baina, horrez gainera, badaude zenbait komando baliagarri ere. Hemen, lehenago landu ditugun adibideei dagozkien zenbait komando jarri ditugu, adibide gisa.

Sortu ditugun zuzeneko ebazpeneko AAAA eta A erregistroak ikusteko, komando hauek erabiltzen dira:

```
C:\>dnscmd ::1 /Enumrecords adibidea.com ipv4
Returned records:
@ 3600 A       10.0.0.3
Command completed successfully.

C:\>dnscmd ::1 /Enumrecords adibidea.com ipv4-ipv6
Returned records:
@ 3600 A       10.0.0.3
3600 AAAA      2001:db8:1::1234:5678
Command completed successfully.

C:\>dnscmd ::1 /Enumrecords adibidea.com ipv6
Returned records:
@ 3600 AAAA      2001:db8:1::1234:5678
Command completed successfully.
```

Eta adibidea.com zonaren eduki osoa ikusteko, berriz:

```
C:\>dnscmd ::1 /zonePrint adibidea.com
;
; Zone:    adibidea.com
; Server: ::1
; Time:    Thu Jun 18 16:48:45 2009 UTC
;
@ 3600 NS    vw2003.
       3600 SOA     vw2003. hostmaster. 5 900 600 86400 3600
ipv4   3600 A   10.0.0.3
ipv4-ipv6 3600 A   10.0.0.3
     3600 AAAA  2001:db8:1::1234:5678
ipv6    3600 AAAA  2001:db8:1::1234:5678
```

```
;
; Finished zone: 4 nodes and 6 records in 0 seconds
;
```

Alderantzizko ebazpeneko zona sekundario bat ondo konfiguratu dugun ikusteko, eta zona horren edukia ikusteko:

```
C:\>dnscmd ::1 /Enumzones
Enumerated zone list:
    Zone count = 5

Zone name                Type     Storage     Properties
...
1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa Secondary File     Rev
...

C:\>dnscmd ::1 /Zoneprint 1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
;
; Zone:    1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
; Server: ::1
; Time:    Thu Jun 18 16:20:30 2009 UTC
;
@ 172800 NS     dns1.novagnet.com.
      172800 SOA    ns1.adibidea.com. dnsadmin.adibidea.com.
200906 1802 36000 7200 1814400 7200
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 172800 PTR  www.adibidea.com.
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 172800 PTR  ipv6.adibidea.com.
```


Alderantzizko ebazpeneko zona primario bat ondo konfiguratu dugun ikusteko, eta zona horren edukia ikusteko:

```
C:\>dnscmd ::1 /Enumzones
Enumerated zone list:
    Zone count = 3
Zone name                    Type    Storage       Properties
...
e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa Primary  File       Rev
...

C:\>dnscmd ::1 /Zoneprint e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
;
; Zone:    e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
; Server: ::1
; Time:    Thu Jun 18 17:09:41 2009 UTC
;
@ 3600 NS       vw2003.
        3600 SOA       vw2003. hostmaster. 3 900 600 86400 3600
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 3600 PTR   www.adibidea.com.
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 3600 PTR   ipv6.adibidea.com.
```

Windows ingurunean, DNS bezero gisa gehien erabiltzen den tresna nslookup da; hain zuzen, Linuxen erabiltzen den dig tresnaren baliokidea. Ikus ditzagun tresna horren erabileraren adibide batzuk, lehengo adibideetan konfiguratutakoa probatzeko. Zuzeneko ebazpenerako:

```
C:\>nslookup
> server 127.0.0.1
Servidor predeterminado: localhost
Address: 127.0.0.1

> set type=ANY

> ipv4.adibidea.com
ipv4.adibidea.com      Internet address = 10.0.0.3

> ipv6.adibidea.com
ipv6.adibidea.com      AAAA IPv6 address = 2001:db8:1::1234:5678

> ipv4-ipv6.adibidea.com
ipv4-ipv6.adibidea.com  Internet address = 10.0.0.3
ipv4-ipv6.adibidea.com  AAAA IPv6 address = 2001:db8:1::1234:5678
```

Alderantzizko ebazpenerako:

```
C:\>nslookup
> server 127.0.0.1
Servidor predeterminado: localhost
Address: 127.0.0.1

> set type=PTR

>4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa

4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
name = www.adibidea.com

>8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa

8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.e.0.8.b.d.0.1.0.0.2.ip6.arpa
name = ipv6.adibidea.com
```


10. Bezeroak

Gaur egungo ia sistema eragile guztiek (zehazki esateko, sistema eragile horien azken bertsioek) lehenago deskribatutako zerbitzuen bezeroak lehenespenez instalatuak izaten dituzte, edo oso erraz lortzeko eta instalatzeko moduan.

Sistema eragilea / Zerbitzua	BSD	Linux	Mac OS X	Windows XP SP1 eta berriagoak, Vista, 7, 2003, 2008
Telnet	Komando-lerroa	Komando-lerroa	Komando-lerroa	Komando-lerroa, PuTTY
SSH	Komando-lerroa, OpenSSH	Komando-lerroa, OpenSSH	Komando-lerroa	PuTTY, SecureCRT SSH
FTP	Komando-lerroa	Komando-lerroa	Komando-lerroa	SmartFTP
Posta elektronikoa	Thunderbird	Thunderbird	Apple Mail, Thunderbird	Outlook
Multimedia-erreproduzitzailea	VLC	VLC	VLC, iTunes	Windows Media Player, VLC, Winamp
Web-arakatzailea	Firefox, Opera, Chrome, eta abar	Firefox, Opera, Chrome, eta abar	Safari, Firefox, Opera, Chrome, eta abar	Internet Explorer, Firefox, Opera, Chrome, eta abar
DNS	Onartzen du	Onartzen du	Onartzen du	Onartzen du

11. Erreferentziak

DAVIES, J. (2008). *Understanding IPv6*, bigarren argitalpena, Estatu Batuak: Microsoft Press.

MALONE, D., MURPHY, N. (2005). *IPv6 Network Administration*, Estatu Batuak: O'Reilly.

VAN BEIJNUM, I. (2006). *Running IPv6*, Estatu Batuak: Apress.

Apache HTTP Server Project. <http://httpd.apache.org> webgunean ikusia, 2009ko ekainaren 15ean.

Comparison of IPv6 application support. <http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support> web-orrian ikusia, 2009ko ekainaren 15ean.

Internet Information Services. <http://www.microsoft.com/windowsserver2003/iis/default.mspx> web-orrian ikusia, 2009ko ekainaren 15ean.

IPv6 to Standard. <http://www.ipv6-to-standard.org> webgunean ikusia, 2009ko ekainaren 15ean.

ISC BIND. <https://www.isc.org/software/bind> web-orrian ikusia, 2009ko ekainaren 15ean.

5. Enpresa

1. Enpresetako sareen atarikoa

Enpresa-sare baten eta etxeko sare baten arteko muga non dagoen esatea ez da erraza; askotan nahasten dira bi kontzeptuak, enpresa-sare askok bizitokietarako zerbitzuak erabiltzen dituztelako Internet atzitzeko. Kapitulu honetan, enpresa-saretzat hartuko dugu zerbitzu-hornitzailearekin interfaze argi bat duena —gehienetan, suebaki bat—, eta barneko eta kanpoko zerbitzuak ematen dituena.

Enpresa-sare baten barruko helbideratze bat aipatzen dugun aldiro, NAT (Network Address Translation edo Sareko Helbideen Itzulpena) dugu gogoan. IPv4 helbideratzeko, ia enpresa-sare guztiek erabiltzen dute NAT; alegia, muga argi bat jartzen dute enpresaren barruko sarearen eta kanpoaren artean. Enpresetan, zerbitzu-hornitzaileetan baino garrantzi handiagoa du IPv4-ren NATek, ia edozein inplementaziorako behar beste helbide ematen duelako. Baina, zer galtzen da NATv4 (IPv4-rako NAT) erabiltzean? Muturretik muturrerako konexioari buruz zer edo zer entzun izan dugu, baita NATek eten egiten duela ere; entzun dugu, halaber, aplikazio batzuetarako NATek arazoak sortzen dituela (hala nola IP gaineko ahotserako). Hala eta guztiz ere, enpresa askotan, erabiltzaile gehien-gehienek kanpoko zerbitzu bakarra erabiltzen dute —web-zerbitzua—, eta gainerakoa enpresa barruko zerbitzuen bidez bideratzen da. Enpresako erabiltzaileen eta kanpokoen artean interaktibitate handia duten enpresak bereziak dira; enpresa horietan NATv4 erabiltzeak eragozpenak sortzen ditu.

Bestalde, IPv4 helbideak agortzear daudela azaldu dugu liburuaren sarreran, eta, horregatik, begien bistakoa da enpresa-sareek prestatu egin behar dutela IPv6 ezartzeko. Baina nire enpresan NAT egiteko behar beste IPv4 helbide badut, zergatik behar dut IPv6?

Oro har, hauek dira horretarako arrazoiak:

- Baliteke enpresa-sare baten barruko erabiltzaileek IPv6 protokoloa soilik darabilen edukia atzitu behar izatea.
- Baliteke kanpoko bezeroren batek IPv6 helbideak besterik ez izatea; horregatik, enpresa-sareak kanpora ematen dituen zerbitzuek IPv6 bidez atzitzeko modukoak izan behar dute.

Enpresa-sare berriek erronka are handiagoari egin behar diote aurre, baldin eta NATv4 egiteko IPv4 helbide bat bera ere ez badute. Sare horiei IPv6-ra aldatzen laguntzeko itzulpen-mekanismoak definitzen ari da IETF erakundea, batez ere RFC4966 dokumentuak NAT-PT zaharkitutzat jo duenetik.

Teknologia berri bat ezarri aurretik, aurreproiektu bat egin behar da beti; aurreproiektu hori garatzeko eta ezartzeko behar den denbora, sarearen tamainaren araberakoa da. IPv6 ezartzearen eragina benetan zenbatekoa den jakiteko, enpresako ekipoak eta aplikazioak xehe ezagutu behar dira, eta, segur aski, hori da IPv6-ren erronka handienetako bat. Tamalez, askotan ez da informazio hori izaten, eta IPv6-k martxan dagoen instalazio batean zer eragin izan dezakeen baloratzea zaila izaten da.

Kapitulu hau osatzen duten ataletan, IPv6 enpresan ezartzeko plana egin aurretiko lanak eta ezarpen-plana osatzen duten zenbait alderdi biltzen dira, besteak beste.

2. IPv6 ezarri aurretik egin beharreko lanak

Enpresan IPv6 ondo ezartzeko, aldez aurretik (aurreproiektua egiteko), lan hauek egin behar dira, besteak beste: informazioa bildu, eragina neurtu, probako esperientzia bat egin, eta aurreproiektua egin.

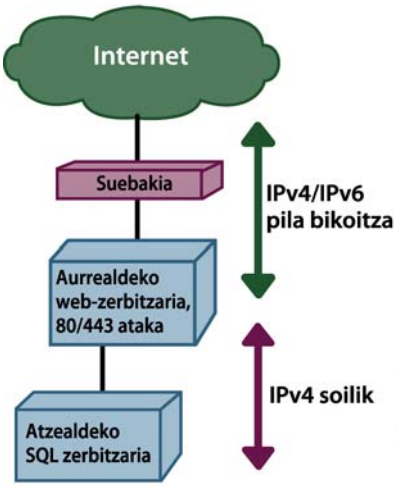
Edozein teknologia berriren azterketa behar bezala egiteko, informazioa ezinbestekoa da; eta IPv6 ez da salbuespen bat. Askotariko informazio-iturriak daude: liburuak, aplikazioen eta ekipoen eskuliburuak, arauak eta ereduak, hitzaldiak, eta ikastaroak. Informazioa bildu ondoren, sare-administratzaileak begiratu behar du, batetik, IPv6-k eragiten dion edo ez (normalean, eragin egingo dio), eta, bestetik, IPv6-k azpiegituran izango duen eragina aztertzeko gai den edo laguntza behar duen.

IPv6-k egiturari eragiten diola egiaztatu ondoren, IPv6-k azpiegiturari non eragiten dion aztertu behar da (eragina, ekipoetan ez ezik, negozioan ere izan dezake, eta izango du, segur aski).

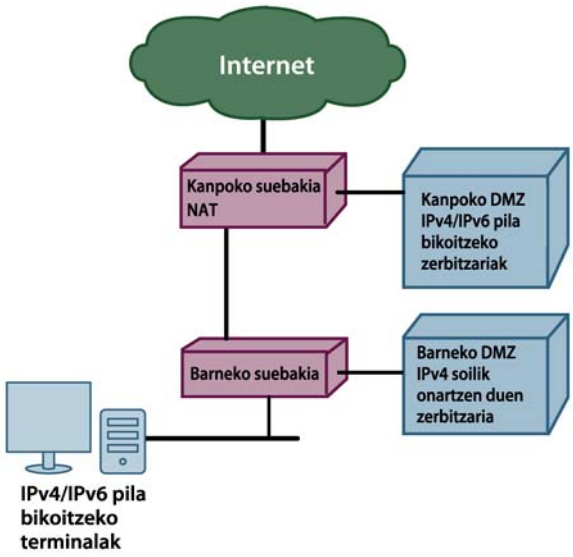
Horrelako proiektu konplexuei ekiteko era egokiena izaten da helburu jakin bat ezartzea eta hartan oinarrituta aurrera egitea. Har ditzagun bi adibide zehatz: batetik, Internet ostatatze-zerbitzua (*hosting*) ematen duen enpresa bat, eta, bestetik, Interneten nabigatzeko terminalak dituen enpresa txiki bat.

Ostatatze-enpresari dagokionez (1. irudia), IPv6-ren inguruko helburua da eduki guztia IPv6-ren bidez atzigarria izatea. IPv6-ren eraginaren azterketaren ondorioa izan liteke, adibidez, barneko komunikazioek (adibidez, SQL konexioek, aplikazio-zerbitzarietarako sarbideek eta abarrek) ez dutela IPv6 onartu beharrik helburua lortzeko. Ondorioz, IPv6 -ren ezarpenak sarerako sarbideari eta webgunearen interfazeari soilik eragiten die. Hala, egin beharreko lana erraztu egiten da, eta kostuak murriztu.

Bigarren kasuan, terminalak dituen enpresa bat dugu (2. irudia). Azterketa egindakoan ondorioztatzen da terminaletan pila bikoitza ezarri behar dela, IPv6 darabilen edukia atzitu ahal izan dezaten. Bestalde, kanpoarekin harremanak dituzten zerbitzariek ere pila bikoitza behar dute, IPv6 soilik duten SMTP zerbitzarietara mezu elektronikoak bidali ahal izateko.



1. IRUDIA. **OSTATATZE-ENPRESA**

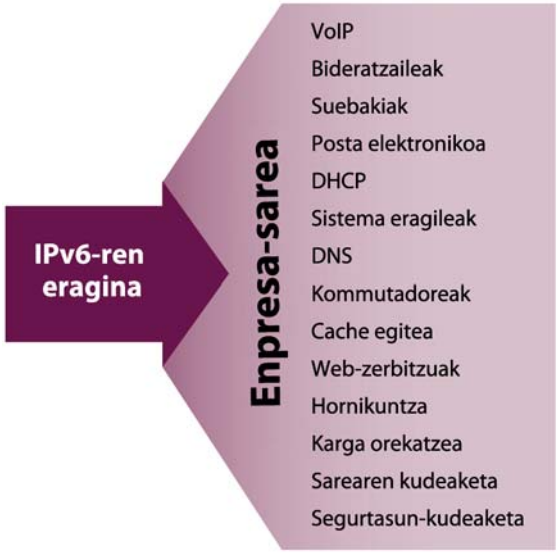


2. IRUDIA. **NABIGATZEKO TERMINALAK DITUEN ENPRESA**

Kontuz! Egokia da IPv6 sareko azken zokoraino helarazi nahi izatea, baina administratzaileak berariaz hartu beharreko erabakia da hori.

IPv6 ezartzean eraginen bat jasan lezaketen elementu batzuk ageri dira 3. irudian. Komeni da administratzaileak elementu horiek aztertzea.

Lan-helburu bat ezarritakoan, eta IPv6-ren eragina zenbaterainokoa izango den ikusitakoan, kostuak zenbatetsi behar dira, eta plangintza-fasera pasatu.



3. IRUDIA. **IPV6-REN ERAGINA AZTERTZEKO KONTUAN HARTU BEHAR DIREN ZENBAIT ELEMENTU**

Enpresa batean IPv6 ezartzeak izango duen eragina aztertzeko, elementu hauek hartu behar dira kontuan, besteak beste: sarearen helbideratzea, bideratzea, aplikazioak eta segurtasun-prozesuak. 3. irudian, enpresa-sare batean IPv6 ezartzeak duen eraginaren azterketan kontuan hartu beharreko zenbait elementu ageri dira.

3. Enpresa-sareetan IPv6 ezartzeko plana egitea

IPv6 ezartzeko planean, elementu hauek hartu behar dira kontuan, besteak beste:

- Helbideratzea.
- Bideratzea.
- Segurtasuna.
- Zerbitzuak.

Oro har, IPv6 ezartzeko plana egitean, ondorio onak ematen ditu IPv4-rako egina dagoenari jarraitzeak.

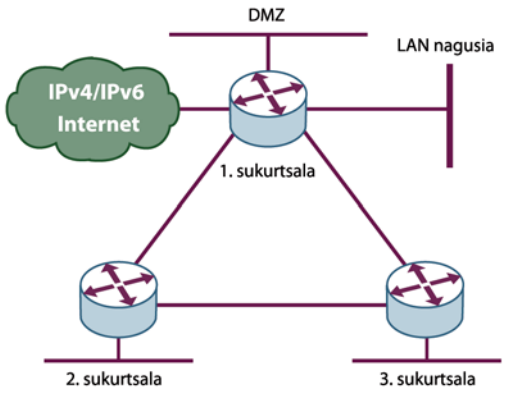
Enpresa-sare gehienak pila bikoitzekoak dira (segur aski, IPv4 helbide pribatuak dituztenak); beraz, IPv4 eta IPv6 aldi berean ibiliko dira. Hala eta guztiz ere, IPv6-ren ezarpena egitean, berriro hasteko aukera dute administratzaileek, alegia, azpiegituran aldaketak egiteko aukera dute.

3.1. Helbideratze-plana

Enpresa baten barruko helbideratze-plana nahiko erraza da. Oro har, /64 bloke bat erabiltzen da unitate gisa, difusio-bloke guztietarako. Hala, /64 blokeak erabiltzen dira sare lokaletarako (LAN), hedadura zabaleko sareetarako (WAN) eta *loopback*etarako. Enpresek, duten tamaina dutela, /48 bloke bat jasotzen dute normalean beren hornitzailearengandik, alegia, 65.535 /64 sareren baliokidea jasotzen dute. Baina enpresa batek —haren sare guztiak (LAN, WAN eta *loopback*ak) kontuan hartuta eta % 300 haziko dela jota— /48 bat baino gehiago behar badu, bloke handiago bat eskatu behar dio hornitzaileari edo, erabiltzen dituen helbideak hornitzailearenak ez badira, helbide-erregistroari.

IPv6-n, bada nahikoa unicast helbide global edozein enpresatarako. Orduan, nahikoa helbide izanik, zergatik erabili NAT? Irakurleari dagokio galdera horren erantzuna bilatzea; guk unicast helbide globalak soilik erabiliz ekingo diogu azterketari.

Adibide batez baliatuko gara, enpresa batean helbideratzea nola egin ikusteko. 4. irudian, ohiko enpresa bat ageri da: DMZ bat du egoitza nagusian (1. sukurtsalean), eta bi sukurtsal ditu (2. eta 3. sukurtsal izendatu ditugunak).



4. IRUDIA. **EGOITZA NAGUSI BAT ETA BI SUKURTSAL DITUEN ENPRESA BATEN SAREA (ADIBIDEA)**

Baliteke enpresari helbideak konexio-hornitzaileak ematea, eta baliteke enpresak helbideak erregistro nazionalean edo eskualdeko erregistroan (adibidez, LACNICen) lortzea. Kasu batean zein bestean, normalean, /48 bloke bat lortzen du enpresak, barne-helbideratzerako. Demagun, orduan, 2001:DB8::/48 dokumentazio-blokea jasotzen duela, zeina enpresako sare guztiak har ditzan zatitu behar baita. IPv6-n ez dira LAN bateko terminalak kontuan hartzen, horietako bakoitzari /64 bat esleitzen baitzaio, halako moldez, non aukera izango baita nahi beste terminal helbideratzeko. Horren ordez, zenbakitu beharreko sare eta azpisare kopurua hartzen da kontuan.

IPv6 helbide guztiek hiru zati dituzte: globalki bideratutako aurrezenbakia, azpisarearen identifikatzailea eta interfaze-identifikatzailea (5. irudia).

n bit	m bit	(128 – n – m) bit
Unicast aurrezenbaki globala	**Azpisare-identifikatzailea**	**Interfaze-identifikatzailea**

5. IRUDIA. **IPV6 HELBIDE BATEN HIRU ELEMENTUAK**

Enpresa-sare batean, oro har, unicast aurrezenbaki globalaren luzera hornitzailearen araberakoa da (gure kasuan, n = 48). Normalean, gainera, interfaze-identifikatzailea /64 izatea aukeratuko dugu, bi arrazoirengatik: sare lokaletan konfigurazio automatikoa errazago egin ahal izateko, eta askotan ekipoak luzera horretako IPv6 helbideekin lan egiteko prestatuak daudelako. Hala, azpisare-identifikatzailearen luzera m = 16 da. Sarearen barruan agregazio geografikoa egin nahi izanez gero (hala egitea komeni da, barruko bideratzean sare bat baino gehiago ager ez daitezen), azpisareari dagozkion 16 bitetan bi elementu identifikatu beha dira: enpresaren barruko sukurtsala, eta sukurtsal bakoitzaren barruko sarea.

1. taulan, jasotako /48 blokea banatzeko zenbait aukera posible ageri dira, 2ren multiploak diren **m** batzuk oinarri hartuta kalkulatuak. Lehen zutabean, azpisare-identifikatzailearen tartea ageri da, pisu handieneko bitetik hasita (ezkerren dagoenetik, alegia).

Banaketa	Sukurtsal kopurua	Sukurtsal bakoitzeko sare kopurua
/50	4	16.384
/52	16	4.096
/56	256	256
/58	1.024	64
/60	4.096	16
/62	16.384	4

1. TAULA. **/48 BAT ENPRESA BATEAN BANATZEKO ZENBAIT AUKERA**

Demagun, gure adibidean, /56 hartzen dugula barneko banaketaren mugatzat, hori baita sukurtsal bakoitzean espero dugun hazkundearen eta sukurtsal kopuruaren gehikuntzaren arteko oreka onena. Baditugu /56 motako 256 bloke, eta horietako bat aukeratu behar dugu sukurtsal bakoitzarentzat, bat kanpoko sarearentzat (1. sukurtsaletik bereizia badago), bat enpresaren WANarentzat eta beste bat ekipoetako *loopback*entzat. Geroago enpresa hazten bada agregazioa errazago egin ahal izateko, komeni da helbideratzea ez sekuentziala izatea, baizik eta sukurtsal bakoitzari hazteko aukera ematea. Esleipen binomiala egitea da errazena. Horretarako, lehendabizi lehen blokearen esleipenak egiten dira, ondoren azkenarenak, eta, ondoren, urrunen dauden bi blokeen erdiko bat. Kasu honetan, ordena honi jarraituz egiten dira esleipenak:

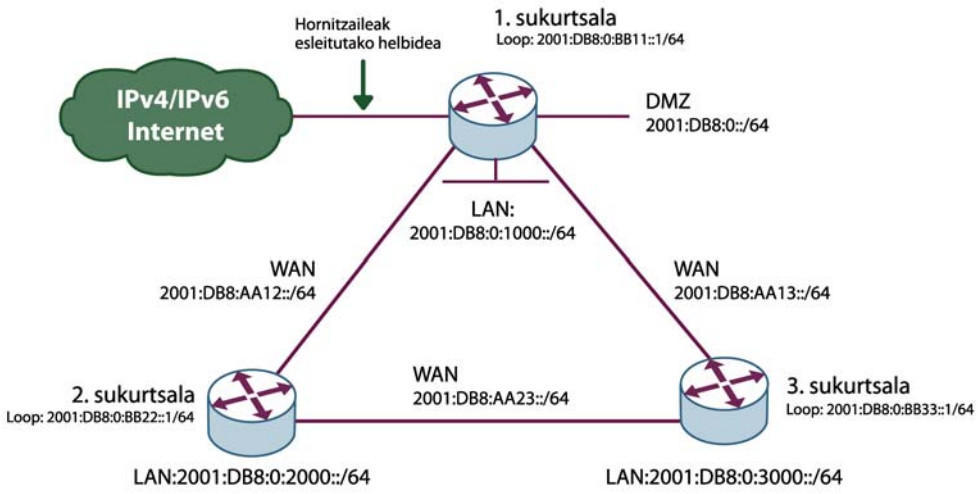
1- 2001:DB8::/56
2- 2001:DB8:0:FF::/56
3- 2001:DB8:0:7F::/56
4- 2001:DB8:0:3F::/56
5- 2001:DB8:0:B0::/56
6- ...

Metodo honek badu arazo bat. Hain zuzen, blokeen identifikazioek ez dute esanahi berezirik, eta gogoratzeko zailak izaten dira. Bada helbideak esleitzeko beste era bat ere, ez hain eraginkorra: esleipena era adimentsuan egitea, ahal den neurrian sukurtsalaren zenbakia dagokion helbide-blokean agerraraziz. Hala egina dago hurrengo adibidea. 2. taulan, helbideekin lana errazago egiteko proposatutako helbide-banaketa ageri da.

/56 helbideen blokeak	Helburua
2001:DB8::/56	**Kanpoko sareak (DMZ)**
2001:DB8:0:1000::/56	**1. sukurtsala**
2001:DB8:0:2000::/56	**2. sukurtsala**
2001:DB8:0:3000::/56	**3. sukurtsala**
2001:DB8:0:AA00::/56	**WAN sareak hautatzeko 2001:DB8:0:AAXY::/64 X sukurtsaletik Y-rako konexioetarako.**
2001:DB8:0:BB00::/56	***Loopback*ak hautatzeko 2001:DB8:0:BBXX::1/64 X sukurtsaleko bideratzailearentzat.**

2. TAULA. **ADIBIDEKO SAREARENTZAT HELBIDERATZE-PROPOSAMENA**

Adibideko sarearen helbideratze-planaren emaitza 6. irudian ageri da, erabili beharreko sare guztien xehetasunekin batera.



6. IRUDIA. **ADIBIDEKO ENPRESA-SAREA**

Onartu egin behar da IPv6 helbide batzuk alferrik galtzen direla. Enpresa-sareak diseinatzen dituenak ez du hori dela-eta gehiegi kezkatu behar, hornitzaileak behar baino askoz helbide gehiago ematen baitizkio, horri buruz deus ere galdetu gabe.

3.1.1. Zerbitzarien helbideratzea

LAN bakoitzean, zerbitzari bakoitzari dagokion interfaze-identifikatzailea aukeratzeko, helbideratze estatikoa erabiltzen da normalean, ahalik eta erabilgarritasun handiena lor dezagun eta sarearen helbidearekin arazoak izanez gero aldaketarik egin behar izan ez dezagun. Zerbitzari baterako erabili beharreko IPv6 helbide estatikoa aukeratzeko orduan, bi puntu hauetako baten alde egin behar dugu:

- Gogoratzeko erraza den helbide bat aukeratu (adibidez, 2001:DB8::1). Hala, problemak errazago aztertzen dira, eta, ondorioz, eragiketak egitea errazagoa da.
- Zorizko helbide bat aukeratu (adibidez, 2001:DB8::ACF:2311:FFED:CAFE). Hala, zailagoa da arazoei antzemateko analisia egitea, baina, inork indarrez eraso egin nahi izanez gero (*port scanning*), ausaz aukeratutako helbideen arrastoari segitzea ere zailagoa dela uste da.

Aukera egiteko orduan, kontuan izan IPv6 oso zabala dela, eta, DNS-erregistroak eskura izan ezean, denbora luzea behar izaten dela baliozko helbideen bila ekorketak gordinki nahiz ordena bati jarraituz egiteko. Beraz, zerbitzari baten DNS-erregistroa publikoki atzigarria bada, zorizko helbideak erabiltzea ez da hain garrantzitsua.

Helbideratze estatikoaren adibide bat (FreeBSD-n, ***ifconfig***):

```
bge0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST>
    mtu 1500
    options=1b<RXCSUM,TXCSUM,VLAN _ MTU,VLAN _ HWTAGGING>
    inet6 fe80::21a:64ff:fe6d:367e%bge0 prefixlen 64 scopeid 0x3
    inet 192.0.2.2 netmask 0xffffff00 broadcast 192.0.2.255
    inet6 2001:DB8::2 prefixlen 64
    ether 00:1a:64:6d:36:7e
    media: Ethernet autoselect (100baseTX <full-duplex>)
    status: active
```

3.1.2. Terminalen helbideratze

Terminalak helbideratzeko hiru aukera hartu behar ditu kontuan sare-administratzaileak:

- Eskuz helbideratzea. Kasu horretan, terminal guztiak banaka zenbakitu behar dira.
- Helbideratze automatikoa, egoerarik edo zerbitzaririk gabe (*stateless* edo *serverless*), bideratze-iragarkien mekanismoa erabiliz (*route advertisements*). Mekanismo horrek ICMPv6 paketeak eta interfazearekiko lokalak diren multicast taldeak erabiltzen ditu. Mekanismo horren bidez, IPv6 helbidea, aurrezenbakiaren luzera eta bide lehenetsia konfiguratu daitezke. Baina ezin da beste elementurik konfiguratu (hala nola DNS-zerbitzariak, WINS-zerbitzariak eta IP darabilen telefono bat automatikoki konfiguratzeko SIP atebideak). Konfigurazio horiek DHCPv6-n ezartzen dira, bereziki egoerarik gabeko aukeraren bidez (*stateless configuration*). Egoerak kontuan hartzen ez dituenez, sare-administratzaileak ez du IPv6 sarera konektatzen diren terminalen gaineko kontrolik. Ingurune komunera sar daitezkeen guztiek dute IPv6 sarerako sarbidea.
- Helbideratze automatikoa, egoerak kontuan hartuta (*stateful*). Kasu horretan, IPv4-ren kasuan bezala, IPv6 helbidea DHCPv6-ren bidez konfiguratzen da. Hala, helbide multzo bat konfiguratu daiteke, baita terminal bakoitzari helbide partikularrak esleitu ere. Egoerekiko konfigurazioan DHCPv6 erabiliz, sarbidea estuago kontrola daiteke. Bada parametro bat (bide lehenetsia) DHCPv6-ren bidez oraindik lortu ezin dena, baina hori lortzeko lanean ari dira. Horregatik, DHCPv6 egoerak kontuan hartuta erabili arren, bide lehenetsia lortzeko, bideratze-iragarkien mekanismo bat erabili beharra dago.

Aukeratzen den helbideratze-mekanismoa aukeratzen dela, IPv6 helbideak kudeatzeko aukera ematen duen aplikazioren bat izatea komeni da. Liburu hau idazteko unean[1], hauek ziren aukera batzuk: Haci (aplikazio librea), IP Address Management Module (Men & Mice), Address Commander (Incognito Aplicaciones) eta VitalQIP (Alcatel Lucent).

1 Itzultzailearen oharra. Erreferentzia hori jatorrizko liburuaren argitalpenari dagokio (2009), eta ez itzulpenaren argitalpenari.

3.2. Bideratze-plana

IPv6-ren bideratze-planak lehendik IPv4-rekin egiten denaren antzekoa izan behar du. Oro har, enpresatan, zentzuzkoa izaten da IPv6-n IPv4-ren topologiari eustea. Bi topologia badaude, sarearen bideratze-eragiketa gehiago egin behar da, eta gorabehera gehiago sortzen dira.

IPv6-n, bideratze-aukera hauek daude:

- Bideratze estatikoa.
- Bideratze dinamikoa.

Eta IPv6-ko bideratze dinamikoan, maila hauek daude:

- Distantzia-bektorean oinarritutako protokoloak: RIPNG (RIP Next Generation).
- Bide-bektorean (*path vector*) oinarritutako protokoloak: BGPv4.
- Loturen egoeran oinarritutako protokoloak: ISIS edo OSPFv3.

Aukera horiei guztiei dagokienez, enpresaren ahalmena hartu behar da kontuan, batez ere. IPv4 sarerako OSPFv2 erabiltzen ari bagara, zentzuzkoa da IPv6rako OSPFv3 eta kanpoko bideratzeentzat BGPv4 erabiltzea. IPv4-rako helbideratze estatikoa erabiltzen badugu, berriz, IPv6-rako konfigurazio bera erabil daiteke.

Ahal den neurrian RIPNG erabiltzea ekiditen badugu, konbergentzia-denbora luzeak eta topologia ez osorik ezagutzeak eragindako arazoak saihesten dira. RIPNG erabiliz gero, gainera, trafikoaren ingeniaritzako teknika modernoak ezin dira erabili.

3.3. IPv6-ko segurtasun-plana

Sare batean IPv6 konfiguratzen denean, sare-maila baten bidezko sarbidea gaitzen dugu. Horregatik, IPv4-rako zeuden babes perimetralerako arauek ez dute IPv6-rako balio. Baina segurtasuna ez da suebakia edo beste elementuren bat konfiguratzea soilik. Urtetan landutako prozesu eta prozedurak ere badira (askotan nazioarteko gomendioei, hala nola ISO 27000ri, jarraituz egindakoak), eta denak ala denak berrikusi eta aztertu behar dira. IP siglek Internet protokolo adierazten dute, eta Internet protokoloan IPv4 eta IPv6, biak, sartzen dira. Garrantzitsua da hori kontuan hartzea. Bereizketa hori bataren eta bestearen prozeduretan egin behar da.

Konfigurazio perimetrala egiteko, IPv4-ren arauen parekoak diren IPv6-ren arauak konfiguratu behar dira. Ikus dezagun, adibide batekin, FreeBSD duen ekipo batean IPFW erabiliz web-zerbitzari baten arauak nola konfiguratu:

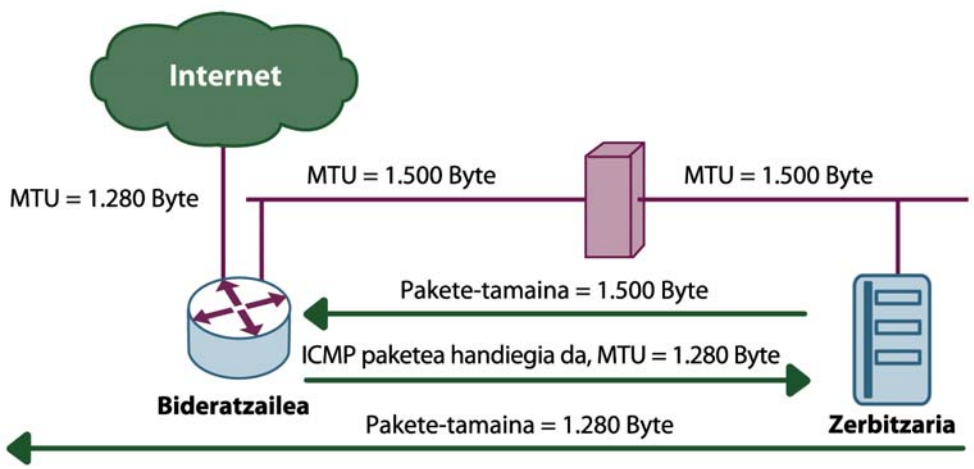
```
ipfw add 1020 permit log tcp from any to "$ip4" dst-port 80 setup
    keep-state in via bge0
ipfw add 2020 permit log tcp from any to "$ip6" dst-port 80 setup
    keep-state in via bge0
```

Adibide horretan, $ip4 aldagaiak web-zerbitzariaren IPv4 helbidea adierazten du, eta $ip6 aldagaiak, berriz, IPv6 helbidea. IPFW-ren kasuan, araua IPv4-ri edo IPv6-ri aplikatu behar zaion hautemateko, arauko helbideen formatuari begiratzen zaio. Erabili beharreko suebakia aztertzean, hori egiaztatu egin behar da, eta IPv6-n egoerak mantentzeko ahalmena ere bai.

IPv4-tik abiatuta IPv6-n suebakia konfiguratzean, arreta berezia behar dute bi puntuk: ICMPv6 eta multicast.

ICMPv6-ri dagokionez, mota berriak hartu behar dira kontuan: 128 mota orain *echo request* da, eta 129 mota, berriz, *echo reply*. Bestalde, hori baino garrantzitsuagoa da kontuan hartzea IPv6-k ez duela bideratzaileetan etendurarik egiten, baizik eta muturretik muturrerakoa soilik dela. Askotariko MTUak (edo transmisio-unitate maximoak) dituen ingurune batean komunikazioa ondo egiteko, bidearen MTUa ezagutzeko prozesua ezartzen da (alegia, PMTUD). Hala, 7.irudian, PMTUD prozesuaren azalpena dago. Han, 2 motako ICMPv6 paketeei zerbitzarirako sarbidea eman behar die suebakiak. RFC4890 dokumentuan, ICMPv6 paketeak iragazteko aholkuak daude.

Intereseko beste kasua multicast iragazteari buruzkoa da, eta, batez ere, loturarekiko lokala den multicast (ff02::/16 helbideak) iragazteari buruzkoa. IPv6-n ez dago difusio-helbiderik (*broadcast*-helbiderik), eta multicast-en erabileraren baitan daude helbideen konfigurazio automatikoa, helbide bikoiztuak hautematea eta hurrengo nodoak aurkitzea. Suebakiak loturarekiko lokala den multicast iragazten badu, IPv6-n ez da ibiltzen.



7. IRUDIA. **ZER MTU DUGUN JAKITEA**

Zer MTU duen jakiteko, zerbitzariak 1.500 B-ko pakete bat bidaltzen du (7. irudia). Pakete hori bideratzaile batek baztertzen du bideko punturen batean, hurrengo loturaren MTUa baino handiagoa delako. Bideratzaileak ICMPv6-ren 2 motako kontrol-pakete bat itzultzen dio zerbitzariari, «Packet too Big», arazoa sortu duen loturaren MTUari buruzko informazioarekin. Zerbitzariak, mezu hori jasotzean, komunikazioaren MTU berrira ego-

kitzen du paketea. Bideko suebakiak zerbitzariari 2 motako ICMPv6 paketeak blokeatzen badizkio, ez dago komunikaziorik.

IPv6 onartzeko egokitu egin behar dira, suebakia ez ezik, segurtasun perimetrala kontuan hartzen dituzten ekipo guztiak, hala nola IDSa eta *log* edo erregistro-egunkariak analizatzeko tresnak.

3.4. Zerbitzu-plana eta IPv6

Enpresen zerbitzuak egokitu egin behar dira, IPv6 onar dezaten. Zerbitzu horiek kanpokoak nahiz barrukoak dira; besteak beste, aplikazio komertzialak, kode irekiko aplikazioak eta bertan sortutako aplikazioak. Arau praktikoa: IP paketeak edo IP helbideak erabiltzen dituen aplikazio edo ekipo guztiak aztertu behar dira, IPv6 onartzen duten ikusteko.

Adibidez, hauek: posta elektronikoa, weba, txat edo berriketa, DNSa, kudeaketa-sistemak (bereziki helbideenak).

IPv6-rekin dabiltzan zerbitzuak atalean, IPv6 onartzeko zenbait zerbitzu nola konfiguratu daitezkeen ikusi dugu.

4. IPv6-rako aldaketa enpresa-sare batean, eta IPv4-ren ahitzea

IPv4 besterik erabiltzen ez duen sare batetik IPv6 ere erabiltzen duen sare baterako aldaketa ez da egun bakar batean egingo; alegia, ez da telebista digitalerako aldaketa edo 1983ko urtarrilaren 1ean Interneten NCPtik TCP/IPra egindako aldaketa bezala egingo. Prozesua pixkanaka egingo da: iturriek eta/edo trafiko-hartzaileek IPv6-rako aldaketa egiten duten neurrian, trafikoa protokolo berrira aldatzen joango da. Horregatik, IPv4 eta IPv6 urte askoan ibiliko dira bitarteko fisiko beretan aldi berean, eta ez dago argi IPv4 guztiz desagertuko denik ere. Enpresa-sareen administratzaileen ustez, hori ez da harritzekoa, IPv4 eta beste protokolo batzuk bitarteko fisiko beretan batera ibiltzearen esperientzia zabala baita (adibidez, IPX, AppleTalk edo DECnet protokoloekin batera).

Trantsizioa pixkanaka egiten ari da, eta bezeroek eta zerbitzariek ez dute batera egin beharrik. Baliteke une jakin batean bezeroak IPv6 onartzea eta zerbitzariak ez, eta alderantziz. Gainera, baliteke bezeroen sistema eragileek tunel automatikoak egiteko mekanismoak ere izatea (adibidez, 6to4 edo Teredo), eta, ondorioz, bezeroen IPv6 konektagarritasuna ez behar bezain ona izatea. Sistema eragile batzuetan (adibidez, Vistan), erabiltzaileek askotan ez dute jakiten funtzio hori gaitua dutenik.

Enpresa batean IPv6 ezartzeko plana egiten denean, bi elementu bereizi hartu behar dira kontuan: azpiegitura eta zerbitzuak. Kasu batean zein bestean, arreta berezia izan behar da bezeroek zerbitzuak okerrera ez egiteko

Azpiegiturari dagokionez (alegia, bideratzaileen, suebakien, datu-baseen eta kudeaketa-aplikazioen konfigurazioari), IPv6-n gehiegizko atzerapena duen konexio bat hautatzeagatik okertu liteke zerbitzua. IPv6 erabiltzen hasi den bezero batek zerbitzu bat IPv6-n ere badagoela ikustean, IPv6-koa hobesten du IPv4-koaren gainetik. IPv6-ko konexioaren atzerapena IPv4-koarena baino askoz ere handiagoa bada, bezeroak horren eragina jasango du. Arazo hori konpontzeko, konexio natiboak edo hurbileko puntuekiko tunelak hobetsi behar dira. Enpresak bere bideratze-politika badu, konexio guztiak IPv6-rekin konfiguratzen saiatu behar du.

Zerbitzuen konfigurazioari dagokionez, une erabakigarria da DNS zerbitzarietako AAAA erregistroen bidez IPv6 helbideak argitaratzen direnekoa. Kanpoko eta barruko bezeroek era batera edo bestera (jatorriz edo tunelen bidez) IPv6 sarbidea duten unetik aurrera, IPv6 sarbidea IPv4 sarbidearen gainetik hobetsiko dute. Horretarako, garrantzitsua da IPv6 sarbiderik ez duten zerbitzuetarako AAAA erregistrorik ez konfiguratzea. Bestalde, jardunbide egokia izaten da hasieran *ipv6.nireenpresa.niredomeinua* erako domeinuekin probak egitea.

Lehenago ikusi dugunez, gerta liteke etorkizun hurbil samarrean Interneten IPv4 helbide publiko gehiago ezin esleitu izatea. IPv4 helbideen eskasia hori kontuan hartuta, bi erronkari egin behar diote aurre enpresek:

- Enpresaren zerbitzuetarako behar beste IPv4 helbide ez izatea.
- IPv6 helbideak besterik ez dituzten bezeroei zerbitzua eman behar izatea.

Lehenengo kasuaren muturrean egongo litzateke IPv4 helbide bat ere ez duen enpresa bat, zeinak bai IPv6 eta bai IPv4 edukia atzitu behar baititu, eta IPv6 eta IPv4 darabilten kanpoko bezeroei zerbitzua eman ere bai. Horretarako, NAT-PT izeneko konponbide bat sortu zuten; RFC4966 dokumentuaren arabera, konponbide hori zaharkitua dago. IETFn, konponbide horren ordezkotzat NAT64/NAT46 aztertzen ari dira, eta deskribatutako egoeran dauden enpresetan ezarriko da. Hornitzaileren batek itzulitako IPv4 helbide publiko edo pribaturen bat izanez gero (alegia, Carrier Grade NAT edo CGN bat izanez gero), IPv4-ko edukia NAT itzulpen arruntaren bidez atzitzen da gehienetan.

Bigarren kasua, berriz, IPv6 soilik darabilten bezeroren bat duten enpresei dagokie; bezero horiek zerbitzu guztiak atzi ditzaketela bermatu behar dute enpresek.

Datozen urteetan iritsiko diren aldaketak nola gertatuko diren eta zer aukera teknologiko gailenduko den ez jakiteak zalantza ugari pizten du, pizten duenez. Baina gertatzen dena gertatzen dela, enpresa-sareetan IPv6 egongo da, eta enpresek beren buruak prestatu behar dituzte oraindik zalantzaz (baina baita aukeraz ere) betea dagoen etorkizun horretara begira.

6. Hezkuntza- eta ikerketa-ingurunea

1. Sarrera

Kapitulu honetan, ikerketa- eta hezkuntza-sareetan IPv6 zabaltzeak zer ezaugarri dituen azalduko dugu. Sare horiek, oro har, unibertsitatez eta ikerketa-zentroz osatuak daude, eta batzuetan, baita ikastetxez eta haiekin erlazionatutako beste erakunde batzuez ere. Sektoreko esperientzia oso garrantzitsua da; IP protokoloaren bertsio berriaren garapenean aitzindari izan denez, hura ezartzen esperientzia handiena sektore honek du.

Kapitulu honetan, IPv6-k ingurune horretarako zer abantaila dituen ikusiko dugu, eta dagoeneko teknologia hau ezarria duten munduko sare nagusiak azalduko ditugu. Bestalde, unibertsitate edo ikerketa-zentro batek IPv6 bere sarean erraz ezartzeko behar den informazioa emango dugu, ikuspegi praktikotik.

2. Zergatik eta zertarako erabiltzen da IPv6 hezkuntzan eta ikerketan?

Hezkuntza- edo zientzia-sektoreak urratu du IPv6 protokoloa ezartzeko bidea, eta, gaur egun, sektore horrek du esperientzia zabalena. Hala, geure buruari galdetu behar diogu zergatik izan den hori horrela. Galdera horri erantzuten saiatuko gara atal honetan.

2.1. Historia pixka bat

Interneten jatorrira jota, ikus dezakegu sarearen oinarriko teknologia ikerketa- eta hezkuntza-inguruneei estu lotua dagoela. Gogora dezagun, adibidez, gaur egungo Interneten oinarria osatzen duten protokoloak —alegia, TCP/IP— AEBko defentsa-alorreko ikerketa-proiektuetan sortu zirela eta proiektu horietan funtsezkoak izan zirela Stanfordeko Unibertsitatea eta Londresko Unibertsitatea.

Ondoren, beste esperientzia batzuek lagundu zuten gaur egun ezagutzen dugun Internet garatzen eta bilakatzen; adibidez, WWW (World Wide Web) posible egin zuten protokoloek eta HTTP[1] protokoloak, zeinak CERN[2]eko ikerketako beharrei erantzuteko

1 http://www.w3.org/Protocols/HTTP/AsImplemented.html
2 http://public.web.cern.ch/public/

sortu baitzituzten. Halaber, lehen nabigatzaile grafikoa, gaur egun hain arrunta dena, 1992. urtean garatu zuen NCSA[3]k (National Center for Supercomputing Applications). Eta horrela aipatuko genituzke gaur egun Interneten erabiltzen diren teknologia, protokolo, software eta aplikazio gehienak.

IPv6-rekin ere antzekoa gertatu da. IETFk esan zuenean IP protokoloaren bertsio berri bat, IPv4-ren mugak gainditzen dituena, ikertu eta haren sorrera sustatu behar zela, unibertsitateetan eta ikerketa-zentroetan oinarritutako taldeak izan ziren berriro prozesuaren buru (besteak beste, MIT, Harvardeko Unibertsitatea eta CERN), Interneten alorreko enpresa nagusiekin batera (ikus, adibidez, RFC1752[4]).

2.2. Aurreko esperientziak

IPv6-ren erabilerari dagokionez, lehen esperientzietako bat 6bone proiektuan sortu zen, eta protokoloaren bertsio berria probatzeko sare «birtual» bat ezartzeko saioa izan zen. Sare hori birtuala dela diogu, Interneteko IPv4 loturetan kapsulatutako tuneletan oinarritzen zirelako hasierako konexio asko; dena den, aurrerago, jatorrizko konexioetarako trantsizioa egin zen. Saiakuntza hori 2006. urtean bukatu zen.

IPv6-ren eskala handiko lehen ezarpenak hezkuntzako edo ikerketako sareetan egin ziren. Hauek izan ziren, besteak beste, sare horiek: AEBko Abilene (Internet 2), Europako Geant, Txinako CERNET2 eta CSTNET2 eta Japongo JGN2.

Europak IPv6 sustatu du zenbait ikerketa-proiekturen bidez, eta aipatzekoak dira, adibidez, 6NET[5], Euro6IX[6] eta GEANT[7] ekimenak.

Ekimen horiekin batera, aipamen berezia merezi du DSD eta Linux sistema eragileetarako egindako IPv6-ren garapenek; KAME eta USAGI proiektuen bidez egin dituzte, hurrenez hurren, eta unibertsitateek proiektuetan parte hartu dute.

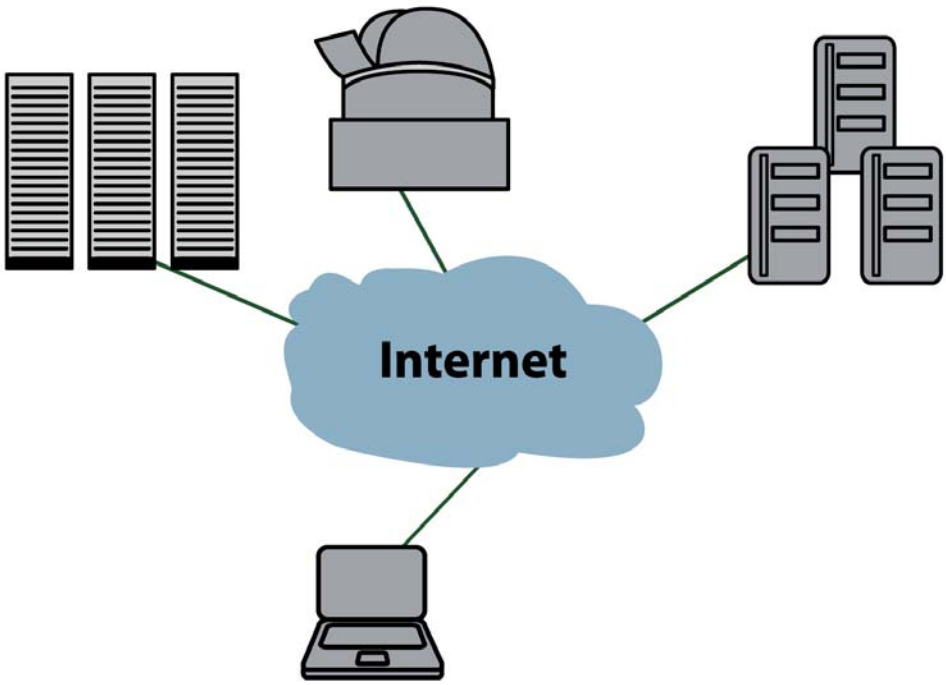
Erreferentzia horiek guztiek erakusten dute lotura estua dagoela hezkuntza- eta zientzia-alorren eta IP protokoloaren bertsio berriaren garapen eta erabileraren artean. Horregatik, sektore horietan zabaldu zen bizkorren protokolo berriaren erabilera, eta sektore horietan ikusi zuten ezaugarri berriek zer aukera ematen zuten. Hurrengo puntuan, horren adibide batzuk ikusiko ditugu.

3 http://www.ncsa.uiuc.edu/
4 http://www.ietf.org/rfc/rfc1752.txt
5 http://www.6net.org/
6 http://www.euro6ix.org/
7 http://www.geant.net

2.3. Gaur egungo sare akademikoen zerbitzuak eta aplikazioak

Gaur egungo sare akademiko/zientifikoek badituzte zerbitzu batzuk beste sare mota batzuetan ezohikoak direnak. Zerbitzu horietako batzuk aipatuko ditugu, eta ikusiko dugu IPv6-k nola laguntzen duen zerbitzu horiez hobeto baliatzen.

- Gaur egun, horrelako sareetan, badira *grid* deritzen sare motak ere; aplikazioen eta sareko zerbitzuen arteko maila batean daude sistema horiek, eta globalki banatutako baliabideak partekatzeko eta baliabide horiek urrunetik atzitzeko aukera izateko dira. Baliabide horiek izan daitezke, adibidez, kalkulu-ahalmena, datuen biltegiratzea, tresna garestien erabilera (adibidez, punta puntako teknologiako mikroskopioak) eta dauden tokira joateko zailak diren tresnen erabilera (adibidez, urruti dauden teleskopioak).



1. IRUDIA. ***GRID* BATEN BIDEZ PARTEKATUTAKO BALIABIDEAK**

Horrelako sistemen bidez, ekipoaren jabe den erakundeaz kanpoko jendeak ere erabil dezake ekipo hori; horregatik deritze *erakunde birtual*. Kapitulu honen asmoa ez da *grid*-sistemei buruzko xehetasunak ematea, baizik eta zerbitzu horiei IPv6 ezartzeak dakarzkien onurak aipatzea. Batetik, IPSec-ek ematen dituen segurtasun-ahalmenek —hala nola autentifikazioa eta muturretik muturrerako datuen zifraketak— beharrezko pribatutasuna eta kontrola ematen dituzte. Eta, bestetik, IP helbide global publikoki atzigarriak izateko aukerari esker, *grid*-zerbitzuak eskala handian zabaldu daitezke, bai baliabideen ikuspegitik, bai horiek erabil ditzaketen gailuen ikuspegitik.

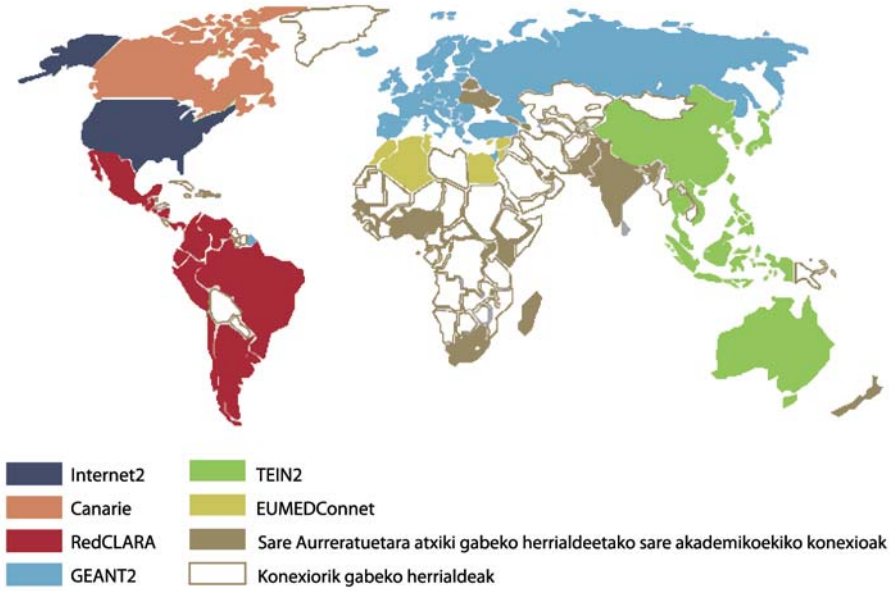
- Horrelako sareetan, ohikoa da multicast teknologia ere. Teknologia horri esker, banda-zabaleraren erabilera hobezina da datuak hartzaile askori igortzen zaizkienean, ez baita hartzaile bakoitzarentzat transmisioaren erreplikarik egin beharrik. Orduan, edukia kalitate hobeko seinale baten bidez igor daiteke, erabili beharreko banda-zabalera ez baita hartzaile kopuruaren arabera biderkatzen. Multicast erabiltzen da bideoaren eta audioaren streaminga egiteko, eskaripeko edukiarentzako, puntu anitzeko bideokonferentzietarako, eta abarretarako. Eta IPv4-n teknologia hori erabilgarri dagoen arren, protokoloaren diseinutik beretik da IPv6-ren parte, eta IPv6-n erabiltzea errazagoa da.
- Bideokonferentziak eguneroko lanaren parte dira irakasleentzat eta ikertzaileentzat, eta, askotan, NATen erabilerak mugatu egiten ditu. IP publiko bat izanez gero, arazorik gabe ezartzen dira muturretik muturrerako komunikazioak.
- Lehenago *grid*en kasurako ere esan dugunez, IPv6 protokoloak, berez duen mugikortasunari esker, baliabideak edozein erakundetatik atzitzeko aukera ematen du. Ezaugarri hori erakargarria da, ohikoa baita ikertzaileak lantalde batetik bestera joatea.
- Azkenik, bai banda-zabalera eta bai egiten diren datuen transferentzia hazi egin dira. Horregatik, banda-zabalera eraginkorrago erabiltzeko, marko erraldoiak erabili behar izaten dira (9.000 B edo gehiagoko *jumbo frame*ak). IPv6-k, «jumbogramen» bidez, emari hori hobetzeko aukera ematen du, sareak teknologia hori erabiltzeko prestatuak dauden neurrian.

3. Munduko sare akademikoak

Unibertsitate edo ikerketa-zentro batean IPv6 zabaltzeaz hitz egin aurretik, dagoeneko badauden hezkuntzako edo ikerketako sareen testuinguruan kokatu behar dugu geure burua, erabilgarri dauden zerbitzuei buruzko ikuspegi orokorra izan dezagun.

Gaur egun, zientzia- eta hezkuntza-alorrak sare fisikoen bidez lotuak daude, eta sare horietako gehienek ezaugarri aurreratuak dituzte, hala nola zerbitzu-kalitatea, multicast eta berezko IPv6.

2. irudian, NRENen munduko mapa ageri da; alegia, munduko sare akademikoen mapa bat. Sare horiek REN izen generikoa dute, ingelesezko sigletan oinarritzen dena (*Research and Education Network*). Ingelesezko sigla horiei, normalean, *N* letra eransten zaie, estaldura nazionala dutela adierazteko. Hala lortzen da NREN izena.



2. IRUDIA. **NRENEN MUNDUKO MAPA**[8]

Urteak dira sare horietako gehienek IPv6 onartzen dutela. Beraz, erabilgarritasun horretaz baliatu gaitezke, munduko zein tokitan gauden, gure erakundean jatorrizko konektagarritasuna lortzeko.

Ondoren, eskualde-sare nagusiak aipatuko ditugu. Sare horietako asko sare nazionalez osatuak daude (alegia, NRENez), eta sare nazionalak dira, azken finean, konektagarritasuna toki jakinetara helarazten dutenak (unibertsitateetara, ikerketa-zentroetara, institutuetara, eskoletara eta abarretara). Aurrerago ikusiko dugunez, sare nazional horietatik lortzen ditugu gure erakundean IPv6 ezartzeko behar ditugun baliabideak.

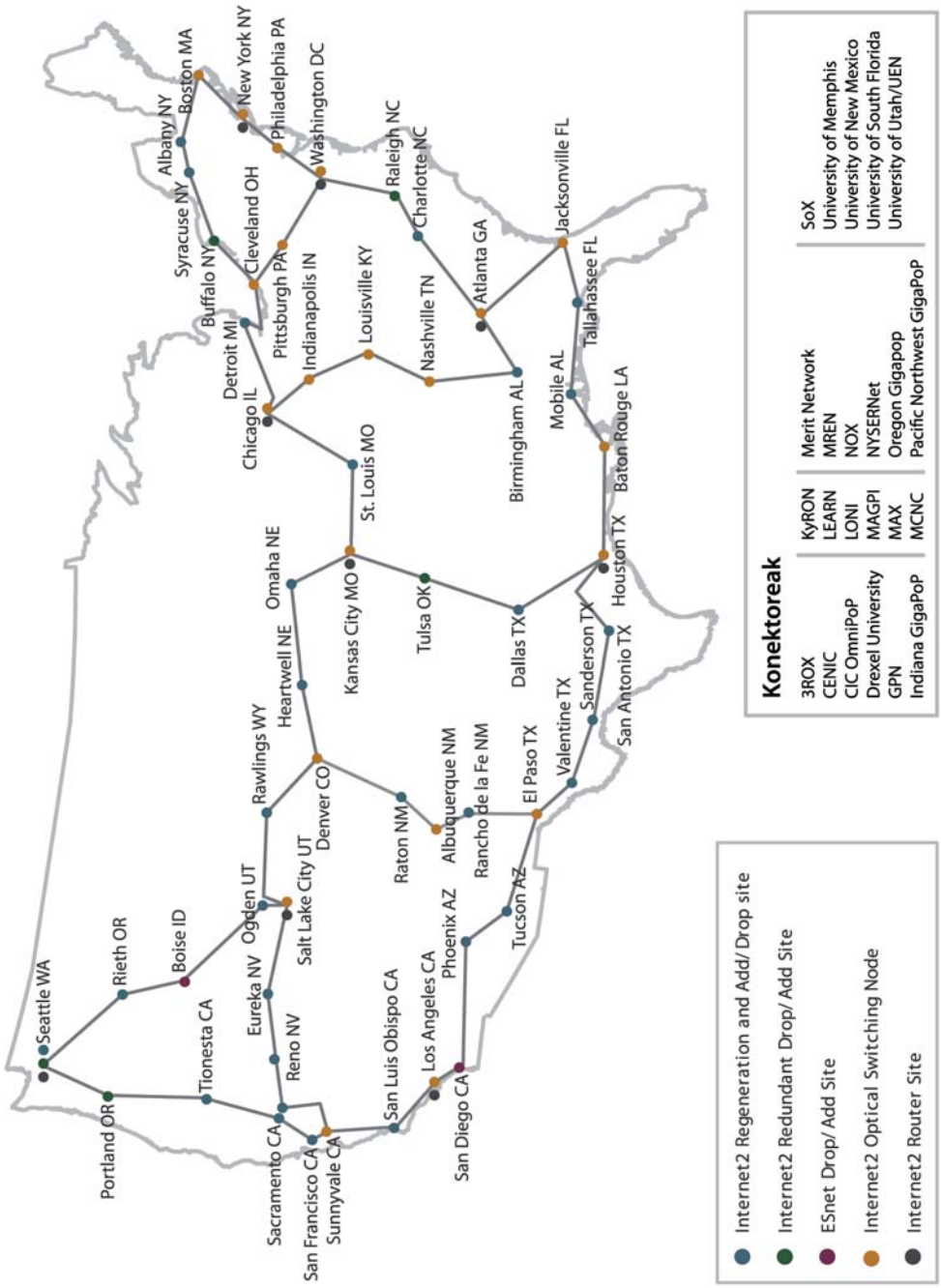
AEBko unibertsitateak Abilene sareari lotuak daude, Internet2 proiektuaren bidez; ikus 3. irudia: Abilene (Internet2) - AEB.

Latinoamerikan, RedCLARA sareak lotzen ditu ikerketako eta hezkuntzako sare nazional guztiak (NRENak); ikus 4. irudia: RedCLARA - Latinoamerika.

Europan, GEANT sarea herrialde guztietara iristen da (bertsio berriak GEANT3 izena du). 3.500 unibertsitate eta ikerketa-zentro baino gehiago lotzen ditu. Ikus 5. irudia: GEANT2 - Europa.

Azkenik, Asia-Pazifikoa izeneko eskualdean, TEIN2 sareak antzeko ezaugarriak ditu; inguru horretako sare nazional nagusiak eta Europa lotzen ditu. Ikus 6. irudia: TEIN2 - Asiako Pazifikoko eskualdea.

8 http://www.redclara.net/index.php?option=com_wrapper&Itemid=293&lang=es

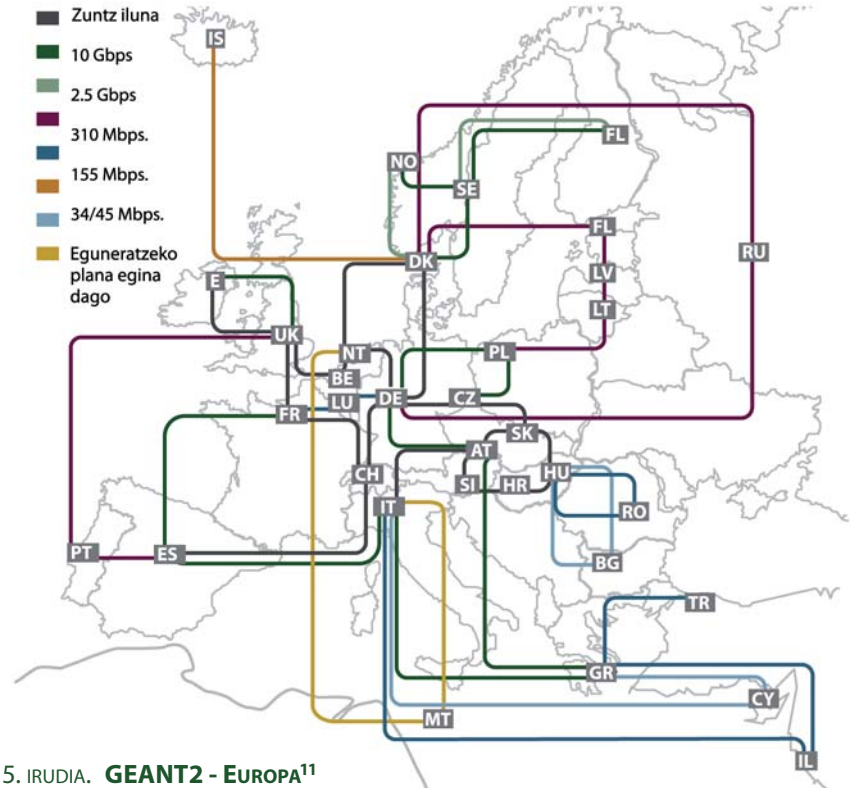


3. IRUDIA. **ABILENE (INTERNET2) - AEB**[9]

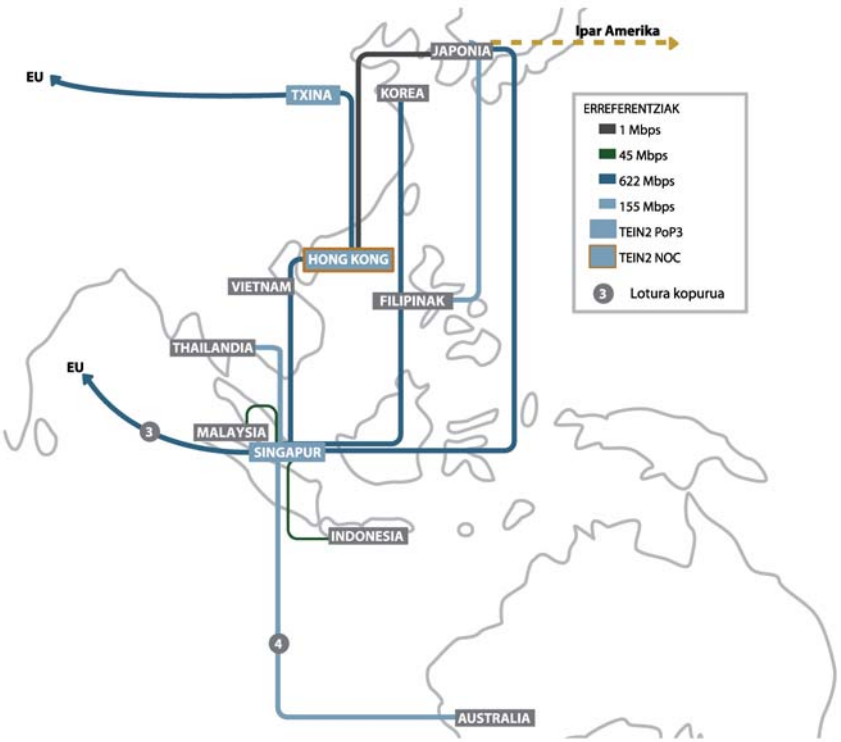
9 http://www.internet2.edu/pubs/200904-Internet2CombinedInfrastructureTopology.pdf

4. IRUDIA. **REDCLARA - LATINOAMERIKA**[10]

10 http://www.redclara.net/index.php?option=com_content&task=view&id=51&Itemid=236



5. IRUDIA. **GEANT2 - EUROPA**[11]



6. IRUDIA. **TEIN2 - ASIAKO ETA PAZIFIKOKO ESKUALDEA**[12]

11 http://www.geant2.net/upload/img/jan08map.jpg
12 http://www.tein2.net/upload/img/TEIN2-web.gif

4. IPv6 unibertsitate edo ikerketa-zentro batean ezartzea

Atal honetan, unibertsitate bateko sarean (edo hezkuntzako nahiz zientziako ezaugarriak dituen erakunde batekoan) IPv6 ezartzeko jarraitu behar diren urratsen berri emango dugu.

Pentsa liteke ez dagoela alderik mota honetako erakunde bateko eta enpresa edo bulego txiki bateko sareen artean. Baina badituzte ezaugarri berezi batzuk, eta merezi du bereiz aztertzea. Dena den, kontuan hartu behar da ikertzaileen eta irakasleen zerbitzura dauden sareez ari garela, ez administraziokoez, azken horiek liburuko beste kapitulu batzuetan azaldutakoak bezalakoxeak baitira.

4.1. Kontuan hartu beharreko ekipoak, aplikazioak eta zerbitzuak

Hemen aztertzen ari garen sareetan, oro har, ekipo hauek izaten dira:

- Bideratzaileak
- Zerbitzariak
- Lanpostuak (PCak, eramangarriak eta beste gailu batzuk)
- Bideokonferentzia-ekipoak
- Kommutadoreak (kabledunak nahiz haririk gabeak)
- Suebakia

Normalean, besteak beste, zerbitzu hauek izaten dituzte:

- DNS
- Posta elektronikoa: sartzen dena, ateratzen dena eta postontziak
- HTTP/HTTPS
- Direktorioak eta autentifikazio-zerbitzuak
- *Grid*ak
- Kontrola

Ezaugarri horien arabera, gehien erabiltzen diren aplikazioak identifika ditzakegu. Kode irekiko aukerei erreparatuko diegu, lantzen ari garen ingurunean horiek baitira ohikoenak.

- Bind
- Sendmail edo Postfix
- Apache
- OpenLDAP
- Radius
- Globus
- Kontrolerako aplikazio libreen zenbait pakete

Aipatutako aplikazio-pakete guztien azken bertsioek onartzen dute IPv6. Beraz, konfigurazio-aukeretan hori kontuan hartu besterik ez dugu egin behar. Horretan hasi aurretik, ordea, erabil daitezkeen helbide-barrutiak aztertuko ditugu.

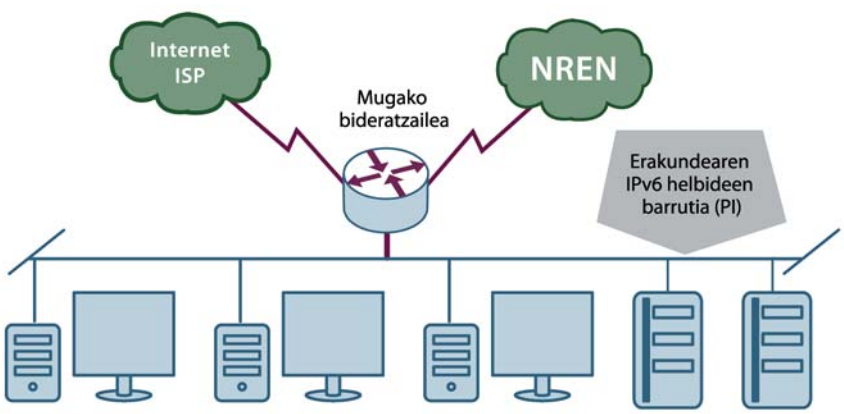
4.2. Nola esleitu IPv6 helbideak unibertsitate batean

Horrelako erakunde baterako IPv6 barruti bat finkatzeko orduan, kontuan izan behar dugu ikerketa-zentro eta unibertsitate gehienak hezkuntzako eta ikerketako sare nazional edo eskualde-sare (NREN) batera konektatuak daudela.

NREN horrek, normalean, badu jatorrizko IPv6 konektagarritasuna, eta helbide-barruti bat eman ahal izango dio gure erakundeari.

Horrelakoetan, /48 barruti bat lortzen da; beraz, 256 /56 azpisare izan ditzakegu, ohiko erabileren arabera erakundean bertan banatzeko.

Bestalde, aipatu beharra dago hezkuntzako edo zientziako erakundeek, NREN batera konektatuak egoteaz gainera, hornitzaile batengandik Internet zerbitzua jasotzen dutela.

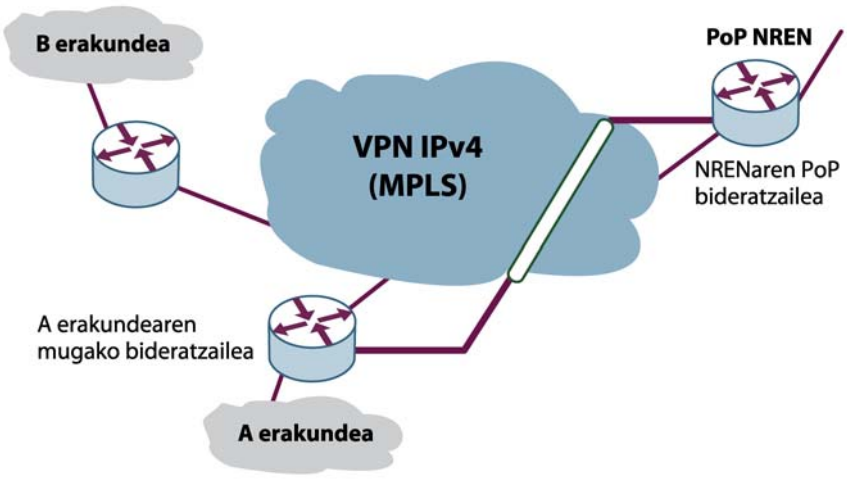


7. IRUDIA. **NREN BATEKO AMAIERAKO ERAKUNDE BATEN KONEKTAGARRITASUNAREN ESKEMA**

Horrelako kasuetan, normalean, bete egiten dira norberaren IPv6 barrutia zuzenean Eskualdeko Internet Erregistroei (RIRei) eskatzeko baldintzak. Gainera, RIR batzuek arau bereziak izaten dituzte unibertsitate, ikerketa-zentro eta antzeko erakundeentzako, askotariko hornitzaile ez izanik ere.

Erakundeari NRENak ematen dion konexioak aipamen berezia merezi du. Gehienetan, puntutik punturako lotura garden baten bidezko konexioa izaten da, eta NRENeko

puntu batera iristen da. Horrelakoetan, IPv6 jatorrizko gisa konfiguratzea ez da zaila izaten. Baina, batzuetan, NRENaren barruko konektagarritasuna hornitzaile baten VPN teknologiaren baten bidez egiten da (normalean, MPLS).



8. IRUDIA. **NREN BATEN BARNEKO KONEKTAGARRITASUNA, VPN BATEN BIDEZKOA**

Zer egin daiteke halakoetan? IPv6 trafikoa IPv4-n kapsulatzeko teknikaren bat erabiltzea izaten da konponbidea. Oso erraza izan daiteke hori. Adibidez, NRENeko puntuaren eta erakundearen irteerako bideratzailearen artean konfiguratutako tunel bat. 6PE, «garraiatzaile-garraiatzailea» edo beste teknikaren bat ere erabil daiteke.

4.3. Ekipoen konfigurazioa

Ondoren, lehentxeago aipatutako tresnen konfigurazioaren deskribapen labur bat egingo dugu; hain zuzen, erakunde akademiko baten sarean IPv6 ezartzeko behar den konfigurazioarena.

4.3.1. Bideratzaileak

Bideratzaileek erakundeari dagozkion IPv6 helbideak konfiguratuak izan behar dituzte, IPv6 gaitua izango duten interfazeetan. Sareko aurrezenbakiak LAN bakoitzean jakinaraztea baimentzea komeni da, ahal denean gailuak automatikoki konfiguratu daitezen.

Erakundeak erabiltzen duen barneko bideratze-protokoloa ere aipatu behar da: IPv4-z gain IPv6 motako informazioa trukatzea kontuan hartu behar denez, barneko bideratze-sistemak IPv6 ere onartu behar du. OSPFv3 edo IS-IS erabiltzea gomendatzen dugu, IP-ren bertsio bakoitzeko topologiekin lan egiteko aukera ematen dutelako. Azken puntu hori garrantzitsua da barneko sarean IPv6 faseka ezartzen denean; horrela-

ko neurririk hartu ezean, arazoak sortuko lirateke, tarteko ekipo batzuk ez dabiltzalako IPv6-rekin.

Konfigurazio-adibidea (Cisco):

```
interface GigabitEthernet0/1
ipv6 address 2001:0db8:1009:101::1/64
ipv6 nd prefix 2001:0db8:1009:101::1/64
ipv6 ospf 1 area 0

ipv6 router ospf 1
router-id 1.1.1.1
area 0 range 2001:db8:1009::/48
```

NRENarekiko konfigurazioan, erakundeak, segur aski, BGP saio bat beharko du, bere aurrezenbakia argitaratzeko eta erakundeaz kanpoko aurrezenbaki guztien berri jasotzeko. Lotura hori kanporantz bideratua dagoen lotura bakarra bada, bide lehenetsi bat erabil daiteke; orduan, NRENak bide estatiko bat izango du gure aurrezenbakira, lotura lehenetsi horren bidez.

Adibidea:

```
router bgp 64500
address-family ipv6 unicast
neighbor 2001:0db8:ffff::2/64 remote-as xxx
network 2001:0db8:1009::/48
```


Lehenago aipatu dugunez, baliteke NRENarekiko konexioa edo unibertsitatearen barruko sarearen zati bat IPv4 bidezkoa soilik izatea. Halakoetan, tunel bat egin behar da eskuz, IPv6 onartzen duten muturren artean.

Adibidea:

```
interface tunnel 1000
ipv6 address 2001:db8:FFFF:FFFF::1/64
tunnel source GigabitEthernet 0/1
tunnel destination 10.1.1.1
tunnel mode ipv6ip
```

4.3.2. Zerbitzariak

Horrelako erakundeetan, normalean, Linux edo Unix sistema eragileak erabiltzen dira zerbitzua emateko. Sistema horiek duela urte askotik onartzen dute IPv6. Oso bertsio egonkorrak dituzte, eta konfiguratzea ez da zaila izaten.

Oro har, ez dugu zerbitzarien konfigurazio automatikoa erabiliko; helbide estatikoak zehaztu nahi izango ditugu, eta hori eskuz egingo dugu. Linux sistemetan, nukleoa-

ren parametro baten bidez desgaitu daiteke konfigurazio automatikoa: **"net.ipv6.conf.*.autoconf=0"**.

Interfazeetako IP helbideen konfigurazioa, berriz, sistema eragilearen araberakoa da. Adibidez, Solarisen, /etc/hostname6.xxx fitxategi bat definitzen da, non xxx sare-interfazearen izena baita. Ubuntun eta Debianen, berriz, /etc/network/interfaces fitxategia erabiltzen da.

Normalean, zerbitzariak DNSn erregistratuak egotea nahi izaten dugu, bai zuzeneko zonei dagokienez, bai alderantzizkoei dagokienez. Hori aurrerago ikusiko dugu, DNS nola konfiguratu azaltzen duen atalean.

4.3.3. Lanpostuak (PCak, eramangarriak eta beste gailu batzuk)

Mahaigaineko PCek eta PC eramangarriek IPv6 onartzen duten sistema eragileak izango dituzte (Linux nahiz Windows). Batzuetan, baliteke lanpostu batzuek Unix sistemekin lan egitea; sistema eragile horretan ere, dagoeneko aipatu dugunez, IPv6 ezartzea erraza da.

Horrelako gailuak automatikoki konfiguratzea komeni da, eta, ahal bada, DHCPv6 zerbitzari batekin, zerbitzari horrek helbide-esleipenen gaineko kontrol handiagoa ematen baitu, eta beste informazioren bat emateko aukera ere bai (adibidez, DNS-zerbitzariak zein diren). Aplikazio hori erabiliz, gainera, erregistroak erakundearen DNSan automatikoki eguneratu ahal izango dira.

Oro har, IP protokoloaren bertsio berriari dagokionez, eguneroko aplikazioek ez dute arazorik ematen. Aplikazio horien artean daude, besteak beste, posta elektronikoaren bezeroak, web-arakatzaileak, lankidetza-sistemak eta abar.

Unibertsitate baten sarera konektatuak egoten dira datuak lortzeko prestatuak dauden eta sareko interfaze bat duten tresnak, hala nola mikroskopioak, analizagailuak, kontrolagailuak eta sentsoreak. Halakoek IPv6 ez onartzeko aukera handiak daude. Sareko inprimagailuen eta eskanerren ezaugarriak ere mugatuak izan litezke, eta IPv4-rekin bateragarria izaten jarraitzeko beharra kontuan hartu beharko da. Hori horrela, erabiltzaileen terminalek pila bikoitzeko edo *dual stack* sistema izatea gomendatzen dugu.

4.3.4. Bideokonferentzia-ekipoak

Mota honetako erakundeek, software-bidezko sistemak ez ezik, bideokonferentziak egiteko ekipo espezializatuak zaten dituzte. Aretokoak nahiz mahaigainekoak izaten dira, eta hardware espezializatuz eta software jabedunez osatuak egoten dira. Merkatuko ekipo ezagunenen artean daude, adibidez, Polycom, Tandberg, Aethra, Sony eta LifeSize etxeetakoak; eta etxe bakoitzak, gainera, modelo-aukera zabala izaten du.

Markaren eta modeloaren araberakoa da IPv6-ren onartze-maila. Beraz, kapitulu honen irismenetik kanpora gelditzen da horien inguruko konfigurazio-aholkuak ematea. Dena den, bideokonferentzia-ekipo berri bat erosteko orduan, kontuan izan IPv6 protokoloa zenbateraino onartzen duen. Batzuetan, IPv6-n SIP protokoloa besterik ezin da erabili, eta H323 bidezko komunikazioak ez dira onartzen. Baliteke, halaber, ekipoa eskuz konfiguratzeko aukera mugatua izatea, eta automatikoki konfiguratzeko mekanismoak soilik onartzea. Puntu horiek berak hartu behar dira kontuan, MCU (Puntu anitzeko kontrol-unitate) motako ekipoekin.

4.3.5. Kommutadoreak (kabledunak nahiz haririk gabeak)

IPv6-ren ikuspegitik, bigarren mailako gailuek ez lukete arazorik sortu behar, ez baitute goragoko mailetako trafikoa interpretatu beharrik. Dena den, kommutadoreei dagokienez, zenbait ezaugarri onartzea komeni da. Adibidez, *MLD snooping* ezaugarria, multicast trafikoa zein atakatara bidali ebazten duena ataketara konektatutako gailuak zer multicast talderen harpidedun diren oinarri hartuta.

Haririk gabeko sarbideei dagokienez, berriz, unibertsitateetan, oro har, modu gardenean erabiltzen dira, eta sarbide besterik ez dira izaten. Horregatik, ez dute arazorik sortzen. Ekipo horiek bideratzaile gisa jokatzen dutenetan soilik hartu behar izaten dira kontuan IPv6 onartzea eta gailuaren konfigurazio-aukerak. Baina, esan bezala, honelako erakundeetan ez dira bideratzaile gisa erabiltzen, administrazio zentralizaturik onartzen ez dutelako.

4.3.6. Suebakiak (firewalls)

Suebakiak sareko azpiegituraren puntu erabakigarria dira. IPv6 onartzen dutela egiaztatu behar da, baita iragazte-arauak IPv4-rekin egiten denaren antzera konfiguratzen uzten dutela ere. Hemen ez ditugu merkatuko marka guztiak aztertuko, asko eta askotarikoak baitira. Kode irekikoak badaudela besterik ez dugu esango, hala nola ip6tables Linuxerako eta ip6fw BSDrako.

Garrantzitsua da kontuan izatea IPv6-n eta IPv4-n arauek berdinak izan behar dutela. Bestela, protokoloaren bertsio batean eta bestean arau desberdinen arabera jokatzen arituko ginateke.

4.4. IPv6 darabilten zerbitzuak ezartzea

Atal hau bukatzeko, honelako erakundeek ezarri behar izaten dituzten zerbitzu batzuk aztertuko ditugu. Horrelako zenbait zerbitzu nola konfiguratzen diren eta kasuan kasu kontuan zer hartu behar den ikusiko dugu ondoren. Bestalde, zerbitzu arruntenen konfigurazioari buruzko informazio gehiago dago zerbitzuei eta zerbitzariei buruzko kapituluan.

4.4.1. DNS

Unibertsitateek eta ikerketa-zentroek beren IPv4 helbide-barrutiak izaten dituzte, eta beren izen-zerbitzariak kudeatzen dituzte (bai zuzeneko domeinuenak bai alderantzizkoenak). IPv6-ren kasua antzekoa da. Ikus dezagun nola konfiguratzen den zerbitzu hau.

DNSri dagokionez, BIND aplikazioa erabiltzen da gehien, eta, dagoeneko esan dugunez, IPv6 onartzen du. Izen-zerbitzarian IPv6 helbideek aldez aurretik konfiguratuak egon behar dute, eta, barneko sarean, izen-zerbitzariak bai IPv4 bidez bai IPv6 bidez atzigarria izan behar du. Hala, DNSk IPv6-n jatorriz erantzun dezake.

IPv4-n A erregistroek definitzen dituzte izen bati lotutako IP helbideak. IPv6-n, berriz, AAAA erregistroak erabiltzen dira, eta funtzionamendua antzekoa da. Oro har, bi erregistro motak definitzen ditugu zona berean.

Adibidea:

```
ns1  IN   A      192.0.2.18
     IN   AAAA   2001:0db8::18
ns2  IN   A      192.0.2.12
     IN   AAAA   2001:0db8::12
```

Bestalde, alderantzizkoak ere definitu behar dira dagokien zonan; IPv6-rako ip6.arpa da zona hori. IPv4-n erabiltzen diren PTR erregistro berak erabiltzen dira. Kontuan izan behar da, normalean, IPv6 helbideak idaztean zero taldeak ez direla jartzen, baina hemen denak osatu behar direla. Gainera, helbideko zifra hamaseitar guztiak sartu behar dira alderantzizko adierazpenean, puntuz bereizita. Horregatik, zailagoa da alderantzizko zonak eskuz editatzea.

Adibidea:

```
$ORIGIN 0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

8.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN PTR ns1.adibidea.org.
2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN PTR ns2.adibidea.org.
```

Hala, IP helbide bat estatikoki esleitua duten zerbitzari eta ekipoei buruzko informazio guztia defini daiteke.

Baina IPv6-ren tresna garrantzitsuenetako bat gailuen konfigurazio automatikoa da. Nola isla dezakegu informazio hori DNSn, aukera horren dinamika galdu gabe? Horretarako BINDen bertsio eguneratuak erabiltzen dira, eguneratze dinamikorako aukera ematen dutelako. Teknika horren bidez, nodo batek edo DHCPv6 zerbitzariak gehitu diezazkiekete erregistroak zuzeneko zonari eta alderantzizkoari. Horrelakoetan, aldaketak baimentzeko, DNS zerbitzariaren eta bezeroaren artean partekatutako gako bat erabiltzen da. Hala, errazagoa da prozesu hori DHCPv6 zerbitzaritik egitea, zerbitzari horrek izango baitu DNSren zonak dinamikoki aldatzeko baimena. Funtzio hori behar bezala

nola konfiguratzen den azaltzea ez dago kapitulu honen asmoetan. Beraz, ez gara xehetasunetan sartuko. Baina informazio egokia aurkitzen da BINDen eskuliburuetan eta DNSri buruzko dokumentuetan.

4.2.2. Posta elektronikoa: sartzen dena, ateratzen dena eta postontziak

IPv6-rekin dabilen SMTP zerbitzu bat (bai sarrerakoa eta bai irteerakoa) ezartzeko, zerbitzariak IPv6 helbideak izatea besterik ez da behar, zerbitzu horretarako erabiltzen den softwarea protokoloaren bertsio berria erabiltzeko prestatua dagoelako.

Postontziei dagokienez, IPv6-rekin dabilen POP3 edo IMAP software bat erabili behar da. Badaude IPv6 onartzen duten kode irekiko bertsioak; adibidez, Washingtongo Unibertsitatekoa[13].

4.4.3. Web-zerbitzariak

Horrelako sareetan, web-zerbitzaria ezinbesteko zerbitzua izaten da, erakundeek webgune nagusiez gainera fakultate, sail eta abarren web-orriak izaten dituztelako. Proiektuen, ikasle taldeen, katedren, eta hainbat zerbitzariren araberako web-orriak egoten dira sare berean.

Zorionez, kode irekiko sistemetan Apache zerbitzaria erabiltzen da gehien, eta IPv6 arazorik gabe kudeatzeko prestatua dago.

Kontuan hartu behar da zerbitzaria konfiguratu behar dela bai IPv4 bai IPv6 bidezko eskaerei erantzuteko. Hori, askotan, IPv6 *socket* bakar bat erabiliz egin izan da, horretarako, mapatutako IPv4 helbideak erabiliz (alegia, ::ffff:a.b.c.d erako helbideak).

Zerbitzu hau behar bezala ibiltzeko, erakundean instalatutako web-zerbitzari bakoitzari dagozkion erregistroak DNSn definitu behar dira. Alegia, AAAA erregistroak eta alderantzizkoak definitu behar dira ip6.arpa hierarkiaren barruan.

4.4.4. Direktorioak eta autentifikazio-zerbitzuak

Erakunde akademikoetan oso ohikoa da direktorio-zerbitzua erabiltzea. Zerbitzu horren bidez, erakundeko pertsonei buruzko informazioa atzitzen da, eta antzeko beste erakunde batzuekin partekatu daiteke. Horrela, pertsona bakoitzari buruzko datuak bilduak daude: bai datu pertsonalak, bai baliabideen atzipenari dagozkionak (lanpostuak, sarea, posta elektronikoaren autentifikazioa eta abar).

13 http://www.washington.edu/imap/

Horrelako direktorioetarako, LDAP erabiltzen da gehien; kode irekiko openLDAP softwarea oso zabaldua dago, eta IPv6 jatorriz onartzen du. Web-zerbitzarietan bezala, pila bikoitzeko sarbidea onartu beharko litzateke, IP protokoloaren bertsioa edozein dela ere.

Direktorioekin erlazionatua dago RADIUS zerbitzua. Protokolo bat da, eta, protokolo horren bidez, baliabideen atzipena autentifikatu eta baimendu daiteke, banandurik, eskaerak dagokion erakundeko zerbitzarira bideratuz. Hala, komunitate akademikoan zenbait zerbitzu ezartzen dira. Adibidez, ikertzaileek edo irakasleek erakunde batetik bestera egiten dituzten joan-etorriak, beste toki batzuetatik jatorrizko erakundean baleude bezalaxe baliabideetara sartzeko aukera mantenduz.

Gure erakundean RADIUS ezartzen duen softwareak IPv6 onartzen duela egiaztatu behar dugu. Erabilgarri dauden kode irekiko softwareetako batek, freeradius-ek, onartzen du. Ekipoak zerbitzari horretara bai IPv4 bai IPv6 erabiliz konekta daitezkeela egiaztatu behar da, gure sarearen azpiegiturako funtsezko zerbitzua baita hori.

4.4.5. *Grid*ak

Lehenago aipatu ditugu IPv6-n *grid* sistemek dituzten onurak. Sistema horiek Globus Toolkit-en oinarritzen dira, eta software horren bertsio berrienek IPv6 onartzen dute. Beraz, software horretan oinarritutako garapenak IPren bertsio berria erabiltzeko prestatuak daude. Sistema zer zerbitzariren gainean exekutatzen den, eta grid zerbitzuak zer aplikazioren gainean definitzen diren, IPv6 onartzeko prestatuak egon behar dute, Globus Toolkit-ek arazorik eman ez diezagun. Eta, normalean, onartzen dute.

4.4.6. Kontrola

Unibertsitateetako sareek, normalean, sareko trafikoari buruzko informazioa ematen duten zenbait sistema jartzen dituzte erabiltzaileen eskura. Sistema horiekin, besteak beste, ezaugarri hauek neurtu daitezke: zer zerbitzu erabili dituzten, trafikoaren jatorriko eta helburuko IPak eta informazio-truke handiena zer sistema autonomoren artean egiten den. Halaber, sare-administratzaileek, bai erakundekoek bai hura osatzen duten ataletakoek (fakultateak, sailak...) sarearen azpiegitura osatzen duten loturen kontrola behar dute.

Hainbat software-pakete erabiltzen da horretarako. IPv6 onartzen dute, besteak beste, hauek: MRTG, Cacti, Nagios, Ntop eta Ethereal.

5. Kontuan hartu beharreko beste puntu batzuk

Amaitzeko, IPv6-ren ezaugarri batzuk nabarmenduko ditugu, zeinak unibertsitateetako sareetarako eta sare horien administratzaileentzat lagungarri izan baitaitezke.

5.1. Erabilgarri dauden helbideak

Unibertsitateetan, ekipo asko izaten dira, eta administrazio desberdinen menpeko azpisare asko ere bai (fakultateak, sailak...). Ikertzaileek eta irakasleek erabiltzen dituzten aplikazio askotarako IP publiko globalki atzigarriak behar dira. IPv6-k eskakizun hori betetzen laguntzen du.

5.2. Konfigurazio automatikoa

Terminal asko eta administrazio deszentralizatua dituzten sareen kasuan (halakoak izaten dira erakunde mota honetakoak), lagungarria izaten da ekipoak automatikoki konfiguratzeko aukera (batez ere DHCPv6-rekin). Hala, terminalekiko IP helbideen esleipenaren gaineko kontrola handiagoa da, bai sare kabledunetan, bai haririk gabekoetan.

5.3. Birzenbakitzea

Aztertzen ari garen sare moten tamaina handia kontuan hartuta, ezinbestekoa da sareak erraz (bideratzaileetan aldaketak programatu hutsarekin) birzenbakitzeko aukera. Internet hornitzaileak kontratatzeko orduan, malgutasun handia ematen du horrek. Izan ere, batetik bestera aldatzeak ez die sare-administratzaileei lan handirik ematen.

5.4. Mugikortasuna

Mugikortasuna oso ohikoa da ikertzaileen eta irakasleen artean. Horregatik, beste sare batzuetatik lantokian bertan baleude bezala baliabideak atzitzeko aukerari esker, errazagoa da erakunde bat baino gehiagotako lagunez osatutako lan-taldeak eratzea.

5.5. Beste kontu praktiko batzuk

Atal hau amaitzeko, zenbait aplikazio azalduko ditugu, tradizional samarrak izan arren ikerketa-inguruneetan asko erabiltzen direnak.

Ohikoa da FTP erabiliz datuen transferentzia egitea, eta urruneko makina batean SSH saio baten bidez prozesuak exekutatzea. Bi aplikazio horiek —datuak eta programa baten exekuzioaren emaitza igorriz— beste toki batzuen konputazio-ahalmena erabiltzeko aukera ematen dute. Bi aplikazioek onartzen dute IPv6; beraz, aldez aurretiko konfigurazziorik gabe erabil daitezke.

Urruneko bistaratzea ere askotan erabiltzen da, bai X leihoen sistemen bidezkoa (X Window Systems), bai interfaze sinpleagoen bidezkoa (adibidez, VNC). Horrelakoetan ere IPv6 erabiltzeak ez du arazorik sortzen: X leihoek onartzen dute, eta VNCren bertsio batzuek ere bai.

Urruneko hezkuntzan, bestalde, ohikoak dira *campus birtual* edo *hezkuntza birtualeko ingurune* deritzen software-paketeak. Moodle aplikazioa da gehien erabiltzen denetako bat, IPv6 onartzen duelako.

Azkenik, askotan garrantzitsua izaten da jakitea ea tokiren batekin muturretik muturrerako IPv6 konektagarritasunik badugun. Informazio hori lotzeko, traceroute6, mtr edo antzeko tresnaren bat erabil dezakegu; gure trafikoak helburura iristeko egiten duen bidearen berri ematen digute. Hala, bide guztia IPv6-rekin badabil, aukera horretaz balia gaitezke. Ostalari edo zerbitzari batek IPv6 paketeei erantzuten dien ere begiratu dezakegu, ping6-rekin.

6. Ondorioak

Kapitulu honetan, erakunde zientifiko edo akademikoetako sareen ezaugarri bereziak aztertu ditugu. Ezaugarri horiek badute isla Interneten oinarriko teknologien historian eta ikerketan, baita aplikazio eta protokolo berrien saiakuntzan ere.

Gaur egungo zientziarako edo hezkuntzarako beharrezkoak diren zerbitzu asko ez dituzte erabiltzen enpresa-sareek edo Internet hornitzaileek, eta, horrexegatik, azterketa berezia merezi dute.

Agerian gelditu da zerbitzu eta aplikazio horietako gehienek IPv6-ren gainean aritzeko balio dutela eta protokoloaren bertsio berriaren erabileran esperientzia zabala dagoela. Hori kontuan hartuta, gure erakundeetan jatorriz IPv6 onartzen duten sareak jartzeko moduan gaude.

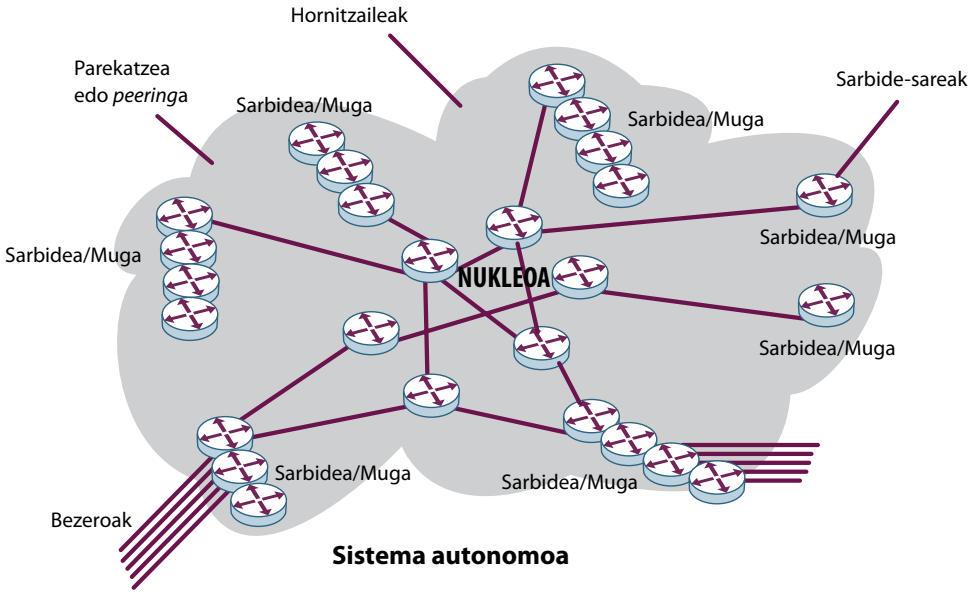
7. Internet zerbitzu-hornitzaileak (ISPak)

1. Kapitulu hau nori zuzendua dagoen

Liburuaren atal hau zuzendua dago, hain zuzen, gaur egun IPv4 zerbitzuak soilik ematen dituen IP sare nagusi baten plangintza egiteko edo halako IP sare nagusi batekin eragiketak egiteko ardura dutenei. Egoera horretan daude hainbat Internet zerbitzu-hornitzaile, zerbitzu mota askotakoak (sarbide dedikatuen hornitzaileak, banda zabalaren hornitzaileak, eskualdeko hornitzaileak, eta abar). Konfigurazioak sinplifikatzeko, adibide batzuk ikusiko ditugu, eta adibide horiek erreferentzia gisa erabiliko ditugu.

Administratzaileak, proiektuari ekitean, zeri aurre egin behar dien azalduko dugu. Helbideratze-plan bat egin behar du, interfazeei helbideak esleitu behar dizkie (IPv6 erabiltzean kontuan hartu beharreko xehetasun batzuk daude), IP sare nagusiarekin lan egiteko erabiltzen diren zerbitzuak kontuan hartu behar ditu, IPv6 pareak (*peers*) ezartzean bideratzaileari dagozkion xehetasun batzuk kontuan hartu behar ditu, eta abar.

Diagrama honetan, zerbitzu-hornitzaile baten topologia tipikoa ageri da. Eremu horretan IPv6 nola ezartzen den ikusiko dugu.



1. IRUDIA. **SARE NAGUSIA (*BACKBONE*). ADIBIDEA**

Hornitzailearen sareak sare nagusian bideratzaile asko baditu, bide-islatzaileen eskema bat erabiltzen da (*route reflector*). Hori beharrezkoa da BGPren ezarpena faseka egin ahal izateko. Deskribatutako konfigurazioak adibide bat besterik ez dira, orain martxan dauden BGP konfigurazioak osatzen laguntzeko.

Irudiko zona nabarmenduko ekipoetan egin behar diren aldaketak deskribatuko ditugu hemen. Kapitulu honetan ez dugu azalduko beste ekipoetan zer aldaketa egin behar den, liburuko beste atal batzuetan azaldu baitugu hori. Ez dugu bezero-ekipoen konfigurazioen xehetasunik emango, ezta LAN sareenak, ostalarienak (bezeroenak zein zerbitzarienak) eta banda zabalaren hornitzaileek erabiltzen dituzten sarbide-sareenak ere.

1.1. Testuan kontuan hartu ditugun teknologiak eta hornitzaileak

Aurkeztutako konfigurazio-adibideetarako, Ciscoren IOS eta Juniperren JunOS hartu ditugu kontuan. Badira kontuan hartu ez ditugun bideratzaile-hornitzaile gehiago ere, baina sare nagusietan gutxiago erabiltzen dira; bestalde, beste ekipo batzuetako komando-lerroaren interfazea (CLI edo *Command Line Interface*) Ciscoren IOSen antzekoa da.

Sare nagusian bi hornitzaileak erabiliz gero ere erabil daitezke konfigurazio hauek adibide gisa. Gutxitan egin behar izaten dira konfigurazio bereziak Ciscoren eta Juniperren arteko bateragarritasunerako.

1.2. Gaitu beharreko zerbitzuen deskribapena

IP sare nagusi batean IPv6 ezartzeko, aukera bat baino gehiago dago. Administratzaileak kasuan-kasuan aukeratu behar du egokiena, hornitzailearen zerbitzuen, sarearen tamainaren eta instalatuak dauden ekipoen ahalmenaren arabera.

Beste ingurune batzuetan gertatzen denaren antzera, pila bikoitza jartzea komeni da. Dena den, sarearen nukleoan, pila bikoitza baino metodo sinpleagoak eta bizkorragoak, tunelak baino eraginkorragoak, ezar ditzakegu. Adibidez, 6PE darabilen MPLS.

Testua ez korapilatzeko, bi kasu horiek soilik aurkeztuko ditugu: pila bikoitzeko ezarpena eta MPLS sare nagusia. Tunelen erabilerari eta haien konfigurazioei erreferentzia egingo diegu, baina ez da komeni konfigurazio hori erabiltzea. 6PE-ren erabilera beste zerbitzu batzuk emateko MPLS ezarria duten hornitzaileei dagokie, baina sarearen nukleoak pila bikoitza onartu ezin duenean ere erabiltzen da.

1.3. Bezeroek IPv6 darabilte, baina hornitzaileak ez du gaitu

Konfigurazio-adibideei eta ezarpen-gomendioei ekin aurretik, kontuan izan behar da balitekeela bezero askok IPv6 erabiltzea hornitzaileak gaitu baino lehen. Aurreko kapituluetan azaldu dugu hornitzaileak IPv6 onartzen ez duenean IPv6 erabiltzeko zer

trantsizio-mekanismo dauden. Abantaila handia lirudike horrek, eta zerbitzu-hornitzaile batek pentsa lezake IPv6-ren ezarpena atzera dezakeela, hain zuzen, bezeroek presiorik egingo ez diotelako. Mekanismo horiek, ordea, ez dituzte behar guztiak asetzen, eta, askotan, arazoak daudenean diagnostikoa egitea zailtzen dute.

Oso lagungarria izaten da bezeroek trantsizio-mekanismo horiek nola erabiltzen dituzten ikustea. Horretarako, bezeroak zer Teredo edo 6to4 errele erabiltzen ari diren aztertu behar da. Litekeena da trantsizio-mekanismo automatikoen bidez erabilitako IPv6 zerbitzuak onak ez izatea. Bestalde, trantsizio-elementuek badute beti eraginkortasun ezaren bat, bai pakete bakoitzari eransten dioten kapsulaketarengatik (*overhead*), bai paketeek bi muturren eta erreleen artean egin behar duten ibilbide luzeagoarengatik.

Sare nagusian IPv6 ezarri ondoren, errele horietakoren bat gaitzea komeni da, jatorriz IPv6-ren bidez konektatzen ez diren bezeroek zerbitzu hobea izan dezaten hornitzailearen sarean bertan instalatutako 6to4 edo Teredo errelea erabiliz.

2. Zerbitzuaren osagaiak

2.1. Internet zerbitzu-hornitzaile baten sarea

Hemen deskribatzen ditugun konfigurazioek azaltzen dute nola ezartzen diren IGP eta BGP, sare nagusian IPv6 gaitzeko. Demagun IGP soilik dela sare nagusiko interfazeen bideratze-informazioa mantentzeko, eta BGPk dauzkala bai taula osoa eta bai hornitzailearen sare/bide guztiak. OSPFn eta ISISen behar diren konfigurazioak besterik ez ditugu ikusiko, horiek baitira gaur egun gehien erabiltzen diren barneko bideratze-protokoloak.

IPv4-rako, joko dugu sare nagusian bideratzea (*routing*) ondo konfiguratua dagoela (bai BGP mailan bai IGP mailan). Hala, IPv6 gaitzeko egin beharrekoa soilik deskribatuko dugu. Alegia, bideratze-protokoloak ezagutzen eta erabiltzen ditugula joko dugu, eta ez ditugu protokolo horien ezarpen klasikoak azalduko, eta ez dugu protokolo horiei buruzko beste xehetasunik emango.

BGPri dagokionez, ikusiko dugu zer konfigurazio behar den ondoko BGPekin guztiz konektaturiko sare bat eratzeko; bide-islatzaileak erabiltzen diren kasu orokorragorako ere baliagarriak dira konfigurazio horiek. Bide-islatzaileak erabiltzea komeni da sare nagusian lau bideratzaile baino gehiago daudenean.

2.1.1. Ekipo nagusiak (nukleoa) eta atzipen-ekipoak (mugako ekipoak)

IP sare nagusiak diseinatzeko jardunbide egokienen arabera, izango ditugu, batetik, bideratzaile nagusiak (normalean nukleoko bideratzaile deritzenak) eta, bestetik, mugako ekipoak edo atzipen-ekipoak (*edge*-bideratzaileak). Dokumentu hau arintzeko, ez ditugu sartu bi kasuetarako IGP mailako eta BGP mailako bideratzeen konfigurazio guztiak,

oso antzekoak baitira. Kasu batzuetan (adibidez, MPLSren kasuan), ordea, bereizketa hori garrantzitsua da, aldaketek atzipen-ekipoei soilik eragiten dietelako.

Sarearen tamainak ere ez du eragin handirik egin beharreko konfigurazioetan. Aurrerago ikusiko dugunez, IPv6 gaitzeko, gehikuntza batzuk besterik ez zaizkie egin behar interfazeetan, BGPn eta, batzuetan, IGPn lehendik dauzkagun konfigurazioei. Asmoa da uneko sare nagusiak dauzkan estandar berak erabiltzea. Baliteke konfigurazio bat baino gehiago erabiltzea, hala nola bide-islatzaileen hierarkia bat, doikuntzak IGPko edo BGPko tenporizadoreetan, eta abar. Ezaugarri horiek guztiak IPv6-rako ere erabilgarri daude.

2.1.2. Gorako bideko hornitzaileak (*upstream providers*)

Norberaren sareko ezarpenei ekin aurretik, hornitzaileekin harremanetan jartzea komeni da. Gaur egun, hornitzaile askok eskaintzen diete jatorrizko IPv6 bezeroei; beste batzuek, tunelen bidez soilik egiten dute, eta beste batzuek oraindik ez dute zerbitzu hori ematen. Zure hornitzaileak IPv6 zerbitzurik ez badu, ez baditu IPv4 eta IPv6 zerbitzuak ataka berean eman nahi, edo ezin badu hori egin, tunel bat erabili beharko duzu. Komeni da, lehenik eta behin, zure hornitzailearen gorako bideko hornitzailearekin harremanetan jartzea, edo dagokion NAPean galdetzea ea herrialdean edo eskualdean badagoen IPv6 tunelen doako zerbitzurik.

Tokiko zerbitzurik ez badago, eta gorako bideko hornitzaileek zerbitzu hori ematen ez badute, zerbitzu publiko bat erabili beharko da. Zure sarearen eta tunelaren beste muturraren arteko IPv4 konexioaren kalitatea ona dela egiaztatu behar da; horretarako, konexioan ezin da pakete asko galdu edo atzerapen handirik izan.

IPv6 tunelen zerbitzu publikoa ematen du, adibidez, OCCAID[1] erakundeak (IPv6 bidezko zirkulazioa eskaintzeko borondatezko baliabideak dituen sare bat da). Zerbitzu hori erabili ahal izateko, frogatu egin behar da nork bere hornitzaileei IPv6 bidezko zirkulazioa eskatu diela eta hornitzaileek ezin dutela zerbitzu hori eman.

2.1.3. Zerbitzariak eta zerbitzuak

Hasieran, zerbitzuek eta zerbitzariek ez dute eguneraketarik behar. Sare nagusian IPv6-rako bideratzea gaitzean, IPv4-rako zeuden funtzio guztiak mantentzen dira, eta zerbitzuek ez dute ondoriorik jasaten. Gauza bat bakarra egiaztatu behar da: IPv6 gaitua duten sistema eragileek ez dute konfigurazio automatikoa erabili behar, ezta horren ondorioz IPv6 erabiltzen hasi ere. Zerbitzuak, zerbitzariak eta suebakiak erabiltzen hasi aurretik, bideratzea ondo konfiguratu behar da.

Zerbitzuek ondoriorik jasaten ez duten arren, zerbitzu publikoetan IPv6 gaitzea komeni da, ezarpena zentzuzkoa izan dadin. Gure DNSek IPv4 bidezko eskaerei soilik eran-

1 http://www.occaid.org/initiatives.php?node=gips

tzuten badiete, ez dugu IPv6 bidezko zirkulazio handirik izango. Zerbitzarietan eta zerbitzuetan behar diren konfigurazioei buruzko xehetasunak haiei buruzko kapituluan daude.

2.1.4. Parekatzeak edo *peering*ak

Gaur egun, IPv6 zirkulazio gehiena doako parekatze eta interkonexioen bidez egin daiteke. Hornitzaileek errazago onartzen dituzte IPv6 bidezko doako zirkulazio-interkonexioak IPv4 bidezkoak baino. Lehendabizi uneko IPv4 parekatzeei galdetu behar zaie ea IPv6 bidezko interkonexiorik onartzen duten, eta, onartzekotan, nola.

Ohikoa izaten da tokiko NAPek IPv6-ren proiekturen bat izatea; proiektu horiek, batzuetan, kideen arteko parekatzea soilik ematen dute, eta, beste batzuetan, zerbitzu gehiago ematen dituzte (adibidez, IPv6 bidezko zirkulazioa). Hurbilen dagoen NAP/IXP-rekin harremanetan jartzea komeni da, norberaren herrian edo herrialdean IPv6-ren ezarpenaren egoera zein den hobeto jakiteko.

3. IPv6 sarean ezartzea

3.1. Plana eta etapa gomendatuak

Sareko beste proiektu batzuetan bezala, ekipoetan aldaketak egin aurretik plan xehe bat lantzea komeni da. Azaldutako ezarpen guztiek eragina dute IP sare nagusian, eta baliteke zerbitzuei ere eragitea.

Sare nagusian IPv6 ezartzeko lehenengo urratsa, oro har, proiektuaren buru izango diren langileak bilatzea izaten da. Martxan dagoen sareko zerbitzuak, ekipoak eta konfigurazioak ondo ezagutu eta ulertu behar dituzte, plana egitean erabaki zuzenak hartu ahal izateko. Langile horiek sareko ekipoen uneko hornitzailearekin harremanetan egotea ere komeni da, hasieratik mugak zein diren jakin dezaten, baita laguntza tekniko egokia jaso dezaten ere.

Aldi berean, eskualdeko erregistroari IPv6 helbideak eska dakizkieke. Indarrean dauden arauei eta prozedurei buruzko xehetasunak aurreraxeago deskribatu ditugu. Helbideratze-plana egiteko, /32 bat jasoko dela jo daiteke; hala, ez da itxaron behar behin betiko blokea jaso arte. Erregistroak zer bloke dugun esandakoan, txantiloiak eguneratu besterik ez da egin behar. Blokeen lehen 8 zifra hamaseitarrak soilik aldatuko dira.

Ondoren, ezarpen-aukerak aztertu behar dira (pila bikoitza, 6PE, tunelak eta abar), eta, sarean konfiguratuak dauden zerbitzuak kontuan hartuta, egokiena zein den erabaki. Kapitulu honetan ikusiko dugu zer aukera dauden, aukerek zer konfigurazio duten, eta guretzat egokiena zein den.

Ezarpen motaren eta uneko bideratze-konfigurazioen arabera, zer ekipo landu behar diren identifikatzen da. Ondoren, zer baliabide ditugun ikusi behar da (ekipo ba-

koitzak zenbat memoria duen erabilgarri, prozesadorearen erabilera zein den, eta abar), ziurtatzeko ekipoek ez diotela behar bezala ibiltzeari utziko konfigurazioen eraginez. Gogoratu IPv4-ren topologiak eta IPv6-renak ez dutela nahitaez berdinak izan beharrik. Loturaren batek edo ekiporen batek ez badu IPv6 onartzen, eta beste bideren bat aukeran badago, IGPri bide erabilgarriak soilik ikusaraz diezazkiokegu. IGP IS-IS bada, aukera hori ezartzea konplexuagoa da.

Ondoren, konfigurazio-plana eraikitzen da: hasteko, bideratzaileetan IPv6 gaitzen da; ondoren, behar bada, IGP konfiguratzen da; eta, azkenik, BGP saioetan IPv6 gaitzen da.

4. Eskualde-erregistroko IPv6 blokeak nola jasotzen diren

Kapitulu hau Internet zerbitzu-hornitzaileei zuzendua dagoela kontuan hartuta, norberaren IPv6 blokeak erabiltzea gomendatzen dugu (alegia, zuzenean RIR edo Eskualdeko Internet Erregistroetatik jasotakoak). Baliteke IPv4 helbideen kasuan blokeak zuzenean jasotzeko aukerarik ez izana. Hala eta guztiz ere, IPv6 helbideen kasurako erregistro-arauak berrikustea komeni da. Adibidez, bere bezeroentzat IPv4 helbide pribatuak (RFC1918) erabiltzen dituen banda zabalaren hornitzaile batek helbideratze pribatu horien ordez IPv6 helbide publikoak erabili nahi baditu (kasu honetan, IPv6 globalak), erregistroari eskaera bat egin diezaioke, eta aldaketa hori egiteko behar dituen IPv6 helbideak eskatu.

Erregistrotik IP helbideak jaso nahi dituzten Internet hornitzaileei aplikatzen zaizkien arau batzuk azalduko ditugu hemen:

Gutxieneko banaketa:

RIRek, IPv6-ren banaketei dagokienez, gutxieneko tamaina bat hartzen dute kontuan, aurrezenbakian oinarritutako iragazkiari laguntzeko. IPv6 helbide-espazio baten banaketa-tamaina minimoa /32 da (behar izanez gero bloke handiagoa eskatzeko aukera dago, jakina).

IPv4-ren azpiegiturari dagokionez:

IPv4 zerbitzuen hornitzaile batek IPv6 espazioa eskatzen badu dauzkan zerbitzuak IPv6-ra aldatzeko, azpiegitura IPv6 bidezkoa soilik izanik onargarria izango litzatekeen eskaera baino handiagoa egin dezake; horretarako, IPv4-ko bezeroen kopurua hartzen da oinarri.

Batzuetan, hornitzaileek ez diete bezeroei IP helbiderik esleitzen, baina badituzte beren blokeak, azken erabiltzaileen arauak erabiliz erregistroak esleitutakoak. IPv4 helbide eramangarriak edukiz gero, IPv6 helbide eramangarriak atzi daitezke. LACNICen indarrean dagoen araudiak hau dio:

> *LACNICek IPv6 helbide eramangarriak esleituko dizkie azken erabiltzaileei, baldin eta aldez aurretik LACNICek esleitutako IPv4 helbide eramangarriak badituzte.*

Esleipenak /32 tamainako blokeak edo txikiagoak izango dira, baina, beti ere, /48 tamainakoak edo handiagoak.

Batzuetan, baliteke aldez aurretik LACNICek esleitutako IPv4 helbide eramangarririk izan gabe IPv6 helbide eramangarriak lortu ahal izatea. Erregistrotik IPv6 helbideak jasotzeko, LACNICen, ezaugarri hauek bete behar dira:

- Esleipena Interneteko domeinu baten barruko bide-sisteman jakinarazten bada, erakunde hartzaileak bloke bakar bat jakinarazi behar du, eta bloke horrek bildu behar du jasotako IPv6 helbideen esleipen osoa.
- Informazio xehea eman behar du, eta eskatutako blokea handik hiru, sei eta hamabi hilabetera nola erabiliko den erakutsi behar du.
- Helbideratze-planak eta azpisare bakoitzaren terminal kopurua jakinarazi behar ditu, gutxienez urtean behin.
- Sarearen topologiaren deskribapen xehatua eman behar du.
- Sarearen bideratze-planen deskribapen zehatza egin behar du, erabiliko dituzten bideratze-protokoloak eta dauzkaten mugak barne.
- Esleipenak /32 tamainako blokeak edo txikiagoak izango dira, baina, beti ere, /48 tamainakoak edo handiagoak.

5. Helbideratze-plana

Helbideratze-plana egiteko aholkuak eman aurretik, gogora ditzagun arau batzuk:

Segmentuek edo blokeek ezin dute inondik inora /64 baino txikiagoak izan. Arau honen salbuespen bakarrak interfazeak izan litezke. Dena den, aurrerago ikusiko dugu puntutik punturako interfazeetan ere /64 erabiltzea komeni dela.

Bezeroei esleipenak egiteko, RFC3177k eta RIRek irizpide hau erabiltzea gomendatzen dute:

- Oro har, harpidedunak oso handiak izan ezean, /48. Alegia, etxeko bezeroek ere /48 jaso beharko lukete.
- Diseinuz azpisare bakar bat soilik behar dela jakinez gero, /64. Banakako konexioetan soilik (adibidez, *dial-up* edo kommutatutako lineen bidezko konexioetan).

Bezeroei /48 blokeak edo handiagoak esleitzea komeni da. Bezeroak ezin du zatitu jasotako blokea /64 tamainako bloketan baino txikiagoetan. Hori horrela, bezeroen eskura 2^{16} (65.535) segmentu edo bloke uzten dira, bere barneko sarean erabil ditzan, eta segmentu horietako bakoitzak 2^{64} gailu eduki ditzake. /48 tamainako blokeak baino handiagoak esleituz gero, ondo dokumentatu behar da hori, erregistroari IPv6 bloke gehiago eskatzean zuritu ahal izateko. Bezero batek /48 baino tamaina handiagoko bloke bat jaso dezake, baldin eta lantoki edo bulego bat baino gehiago baditu; horietako bakoitzak /48 jasotzen du.

Badago IPv6-ko helbideratze-planari buruzko erreferentzia on bat ARIN[2]en wikian.

RFC4291 ere erreferentzia ona da. Dokumentu horretan, bideratzaileetako eta ostalarietako helbide moten deskribapena, adierazpidea eta aholkuak daude.

LAN sarearen (Ethernet) segmentu bakoitzak /64 bat erabiliko du.

Sarearen azpiegiturari dagokionez, PoP bakoitzeko /48 gordetzea komeni da. PoP askotan, blokearen zati handi bat erabili gabe geratuko da. Hala eta guztiz ere, hobe da bloke erabat independentea erabiltzea (alegia, bezeroentzat erabiltzen ez dena), baita libre geratzen diren helbide batzuk uztea ere (aurrerago PoP-erako erabili ahal izateko).

Komeni da, halaber, /64 bat *loopback*ei dedikatua uztea. Horietako bakoitza /128 izanik, /64 bakar batean erabilgarri dauden helbideen kopurua nahikoa izango da.

Puntutik punturako interfaze bakoitzerako /64 erabiltzea komeni da. Hori, itxuraz, IP helbideak alferrik xahutzea da, /127 nahikoa izaten baita (IPv4-n /31 erabiltzea bezalaxe). Baina, RFC3627n azaltzen denez, /127 erabiltzeak eragozpenak eragin ditzake lan egiteko orduan.

5.1. IPv6-en esleipenekin erlazionatutako arauak (bezeroei egindako esleipenenak eta barnekoenak)

Bezeroei esleipenak egiteko, ez dago gehienezko tamainarik (IPv4-ekin ez bezala). Hornitzaile bakoitzak bere esleipen-arauak izan ditzake, helbide-bloke osoa ahalik eta hobekien erabiltzea sustatzeko. Dena den, azken erabiltzaileei egiten zaizkien /48 esleipen guztiak RIRean edo NIRean erregistratu behar dira, hurrena banaketa bat behar denean ebaluazioa behar bezala egin ahal izateko.

RIRei nahiz NIRei ez zaie axola LIRek edo ISPek zer tamainako helbideak esleitzen dituzten. Horregatik, normalean ez dute eskatzen IPv6-ren erabiltzaileen sareei buruzko informazio xeherik, IPv4-rekin eskatzen zuten arren. Noiz edo noiz besterik ez dute eskatzen informazio hori.

5.1.1. Operadorearen azpiegiturari egindako esleipenak

Sareko PoP bakoitzak /48 dedikatu bat izan dezake. Kasu horretan ere, IPv6 helbideen erabilera, itxuraz, ez da oso eraginkorra. Hala eta guztiz ere, erabilera horrek gaur egungo arauak betetzen ditu. LACNICen araudiak hau dio:

2 http://www.getipv6.info/index.php/IPv6_Addressing_Plans.

Erakunde batek (ISP/LIR) /48 bat esleitu dezake PoP bakoitzeko, IPv6 bidezko zerbitzuen operadore baten azpiegitura-zerbitzu gisa. PoP bati egindako esleipen bakoitza esleipen bakar bat da, PoP horren erabiltzaile kopurua gorabehera. Operadorearen beraren eragiketetarako esleipen bereizi bat lor daiteke.

5.2. NAT eta sarearen babesa

Sarean erabilitako IPv4 helbideratze-planak, askotan, helbide pribatuak darabiltzaten segmentuak ditu (RCF1918), azken horietan erabilitako gailuak ezkutatzeko. Horrelakoetan, segmentu horietatik Internet atzitzeko, NAT (Sareko Helbideen Itzulpena) erabiltzen da. IP pribatuen eta NATen erabilera bi ikuspegitatik aztertzea komeni da:

- NATek IP helbide asko gaitzen dituzte
- Segmentu babestuak atzitzeko segurtasun-baliabidea da NAT

Zoritxarrez, NAT erabiltzeak asko konplikatzen ditu aplikazioak, eta, batzuetan, aplikazioak erabiltzea ere eragozten du. Konektagarritasun-arazoen diagnostikoak egitea oso zaila izaten da, eta, normalean, aplikazioen arteko konexio batek sare publiko bat zeharkatu behar badu, software-garatzaileek kontuan hartu behar dute aplikazioek NAT onartzea.

IPv6 erabiltzen denean, ez dago NAT erabili beharrik; berez, ez dago estandarizatua ere. Behar diren gailu guztietarako behar beste IPv6 helbide izango ditugu. Denek ala denek eduki ahal izango dituzte IPv6 helbide esklusiboak.

Segurtasunari edo NAT babes gisa erabiltzeak dituen abantailei dagokienez, RFC4864 irakurtzea komeni da; batez ere, NAT erabili gabe antzeko segurtasun-maila edo hobea lortzeko babes-arauei buruzko zatia (*Local Network Protection*).

Globalki atzigarriak ez diren IPv6 helbide esklusiboak (ULA[3]: Unique Local Addresses) behar izanez gero, tresna[4] bat erabil daiteke.

IPv6 ezartzean plangintza eta aholkularitza egokia falta badira, segurtasun-arazo larriak sor daitezke. Zoritxarrez, 90eko hamarkadaren amaieraz geroztik, pertsona eta hornitzaile askok entzun dute IPv4 helbideak bukatzen ari direla. Hala, arazoa orain arte iritsi ez zaigunez, askok uste dute ez dela inoiz iritsiko. Horregatik, unea iritsitakoan ezarpena etsi-etsian egiteko arriskua dute. IPv6-n badaude segurtasunarekin zerikusia duten ezaugarri egoki batzuk (adibidez, derrigorrezko IPSec, NAT kentzea eta abar); baina aplikazioetan eta suebakietan eragin handia dute (adibidez, ICMP pakete batzuk onartu beharra), eta kontuan hartu behar dira. RFC4942n IPv6 ezartzeak segurtasunean duen eraginaren azterketa bat dago.

3 RFC4193: http://www.ietf.org/rfc/rfc4193.txt
4 http://www.sixxs.net/tools/grh/ula/

5.3. Konfigurazioak

5.3.1. Bideratzaileetan IPv6 gaitzea

Juniper etxeko bideratzaileek IPv6 bideratzea gaitua dakarte. Cisco etxeko IOSetan, berriz, komando orokorrak erabili behar ditugu:

```
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
!
```

Juniper bideratzaile baten interfaze batean IPv6 gaitzeko:

```
interfaces fe-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:DB8:C003:1001::1/64;
    }
  }
}
```

Cisco IOSen interfaze bati IPv6 helbide bat esleitzeko:

```
interface GigabitEthernet1/1
description Interface de Backbone
ipv6 address 2001:DB8:C003:1001::1/64
```


5.3.2. IGP konfiguratzea

Sare nagusi osoan pila bikoitza ezartzen bada, IPv6-rako eta IPv4-rako IGP bera erabiltzea komeni da. Sare nagusian MPLS gaitua badago, ez da beharrezkoa IGP konfiguratzea nukleoak IPv6 onar dezan; izan ere, birbidaltze-informazioa PDLren edo RSVP-TEren esku egongo da.

Gaur egun OSPF erabiltzen ari bazara, edo aurrerago IGP aldatzeko asmoa baduzu, baliteke IPv4-rako eta IPv6-rako IGP-prozesuak desberdinak izatea. Horretarako aukerak RFC4029-n daude, eta hauek dira:

- OSPFv2 IPv4-rako eta IS-IS IPv6-rako
- OSPFv2 IPv4-rako eta OSPFv3 IPv6-rako

IPv4-rako IS-IS eta IPv6-rako OSPFv3 erabiltzeko aukera ere badago, baina bi protokoloak ezagutu behar dira, eta bietan ala bietan esperientzia izan behar da. Ez da zentzuzkoa sareko eragiketak alferrik korapilatzea.

IPv4-rako IGP gisa IS-IS erabiltzen ari direnek, prozesu bera erabiliz gaitu dezakete IPv6.

OSPF erabiltzen ari direnek, berriz, beste prozesu bat beharko dute.

Cisco IOS batean sare nagusiko interfaze baterako OSPF konfiguratzea honen antzekoa da:

```
interface Interfaze-izena
description Sare nagusiaren interfazea
ipv6 address 2001:DB8:C003:1001::1/64
ipv6 ospf network point-to-point
ipv6 ospf 1 area 0
```

Eta prozesua konfiguratzea, berriz, honen antzekoa:

```
ipv6 router ospf 1
auto-cost reference-bandwidth 10000
router-id IP-helbidea
area 0 range 2001:db8:C003::/48
```

5.4. BGP saioak

5.4.1. Kontuan hartu beharreko puntu garrantzitsuak

Hemen jarri ditugun BGPren konfigurazioak adibideak besterik ez dira. IPv6 ezartzeko gutxienez behar diren komandoak edo ohikoenak ezagutzeko balio dute. Komando horiek BGPren konfigurazioari (lehendik dagoenari) gehitzen zaizkio, eta uneko saioei, berez, ez liekete eragin behar. Oso litekeena da BGPren IPv4-rako konfigurazioek dituzten doikuntza batzuk aplikagarriak izatea BGPren IPv6-rako saioetarako (adibidez, tenporizadoreetako aldaketak, aurrezenbaki kopuruen mugak, eta abar).

IPv4-n, batzuetan, aurrezenbakien iragarpena ziurtatzeko, erantsitako bloke handirako null balioko bide estatikoak erabiltzen dira (*Hold Down routes*). Halakoetan, IPv6 blokerako gauza bera egitea komeni izaten da.

Adibidez:
Cisco IOSen:

```
ipv6 route 2001:DB8::0/32 Null0 254
```

Juniperren:

```
routing-options {
  rib inet6.0 {
    static {
      route 2001:DB8::0/32 {
      discard;
      install;
      readvertise;
      }
    }
  }
}
```

Oro har, BGPren beharrak eta funtzionamendua berdinak izaten dira IPv4-rako eta IPv6-rako. Horregatik, ona izaten da martxan dagoen BGP konfiguratzean jarraitutako urrats berei jarraitzea. Hala, errazagoa da diagnostikoak egitea, eragiketa-alorrek errazago barneratuko baitituzte konfigurazio berriak.

BGPren konfigurazioa Cisco IOSen

```
router bgp ASNzenbakia
  address-family ipv6
  redistribute commands

  neighbor IP-RR-helbidea activate
  neighbor IP-RR-helbidea send-community
  neighbor IP-RR-helbidea peer-group talde-izena

exit-address-family
```

Konfigurazioa, bide-islatzailea dagoenean (Juniper):

```
protocols {
  bgp {
    group izena {
      family inet6 {
        labeled-unicast {
          explicit-null;
        }
      }
    }
  }
}
```

Bide-islatzailearen konfigurazioa Cisco IOSen:

```
router bgp ASNzenbakia
  address-family ipv6
  neighbor IP-helbidea activate
  neighbor IP-helbidea route-reflector-client
  neighbor IP-helbidea send-community
  neighbor IP-helbidea peer-group taldea
exit-address-family
```

5.4.2. Iragazkiak

Oso litekeena da BGP saioek iragazkiak izatea, helbideratze pribatuko aurrezenbakien trukaketa (RFC1918) nahiz helbideratze okerrak egitea eragozteko. Hauek dira iragazki horien baliokideak BGPren IPv6-rako saioetarako:

Juniperren:

```
policy-options {
  policy-statement ipv6-helbide-baliogabeak {
    term deny-IPv6 {
      from {
        route-filter 0000::/3 orlonger
        route-filter 4000::/2 orlonger
        route-filter 8000::/1 orlonger
        route-filter 2001:DB8::/32 orlonger
      }
      then {
        reject;
      }
    }
  }
}
```

Cisco IOSen:

```
ipv6 prefix-list ipv6-baliogabeak seq 20 permit ::/3 le 128
ipv6 prefix-list ipv6-baliogabeak seq 30 permit 4000::/2 le 128
ipv6 prefix-list ipv6-baliogabeak seq 40 permit 8000::/1 le 128
ipv6 prefix-list ipv6-baliogabeak seq 50 permit 2001:DB8::/32 le 128
```


5.4.3. MPLS darabilten hornitzaileak

Sare nagusian dagoeneko MPLS konfiguratua duten hornitzaileek 6PE izenez ezagutzen den teknika erabil dezakete; IPv6 mugako edo atzipeneko ekipoetan soilik gaitzeko aukera ematen du teknika horrek (PE: *Provider Edge*). Gaur egun MPLSko VPN zerbitzuarentzat erabiltzen den funtzionamenduaren antzekoa da 6PE-rena. MPLS sare nagusian egongo da BGPv4-k trukatutako aurrezenbakiei buruzko informazioa eta *forwarding* edo birbidaltze-informazioa (LDPk edo RSVP-TE-k ezagutzen duena, paketeak sistema autonomoaren beste muturrera nola helarazi jakiteko). Tarteko ekipoen birbidaltze-informazioa ezaguna izango da. Horregatik, mugako ekipoetan soilik konfiguratu behar da pila bikoitzeko IPv6.

6PE zehatz-mehatz nola dabilen jakiteko, ikus RFC4798. RFC horretan azaltzen da, teknika hori ez ezik, kasu konplexuagoetan teknika hori bera nola erabiltzen den; adibidez, sistema autonomo desberdinen interkonexioan. Horretarako, analogia bat egiten du VPNentzat erabilitako ASNen interkonexioaren teknikarekin.

6PE-k badu abantaila bat: erraz konfiguratzen da. MPLS ezarriz gero, zatirik konplexuena egina dago, eta IPv6 gaitzea VPNak erabiltzea baino errazagoa da. Alde txar bat ere badu: bideratzea LSPen arabera egiten da, eta ez pakete bakoitzak daukan IP helbidearen arabera. LSP bat ezarri ezin denean, eta IPv4 paketeren bat (Internetekoa) halabeharrez sare nagusiko bideratzaile batera (nukleoko bideratzaileak barne) etiketarik gabe iristen

denean, IPv4 bidezko zirkulazioan, bideratzaileak pakete hori behar bezala bideratu dezake. IPv6 bidezko zirkulazioan, ordea, arazo hori duten paketeak baztertu egiten dira.

Kapitulu honetan ez dugu deskribatuko nola erabiltzen den IPv6 MPLS gaineko VPNetan; izan ere, liburu hau Interneteko zerbitzura zuzendua dago. Baina erabili, erabil daiteke. RFC4364-n bai IPv4 eta bai IPv6 hartzen dira kontuan (MPLS gaineko VPNentzat erreferentzia gisa erabili ohi den RFC2547 ordezten du RFC4364-k).

Adibidean jarri dugun konfigurazioan, bide-islatzaileak dauzkan BGP bat darabilen 6PE dago, hori baita MPLS hedatu zuten hornitzaileen egoera arruntena.

6PEren konfigurazioak Cisco IOSerako

```
mpls ipv6 source-interface Loopback0

router bgp ASNzenbakia
  address-family ipv6
  redistribute connected route-map ekintza-konektatuentzat
  redistribute static route-map ekintza-estatikoentzat
  neighbor IP-RR-helbidea activate
  neighbor IP-RR-helbidea send-community
  neighbor IP-RR-helbidea send-label
  neighbor IP-RR-helbidea peer-group talde-izena

exit-address-family
```

6PEren konfigurazioak Juniperren

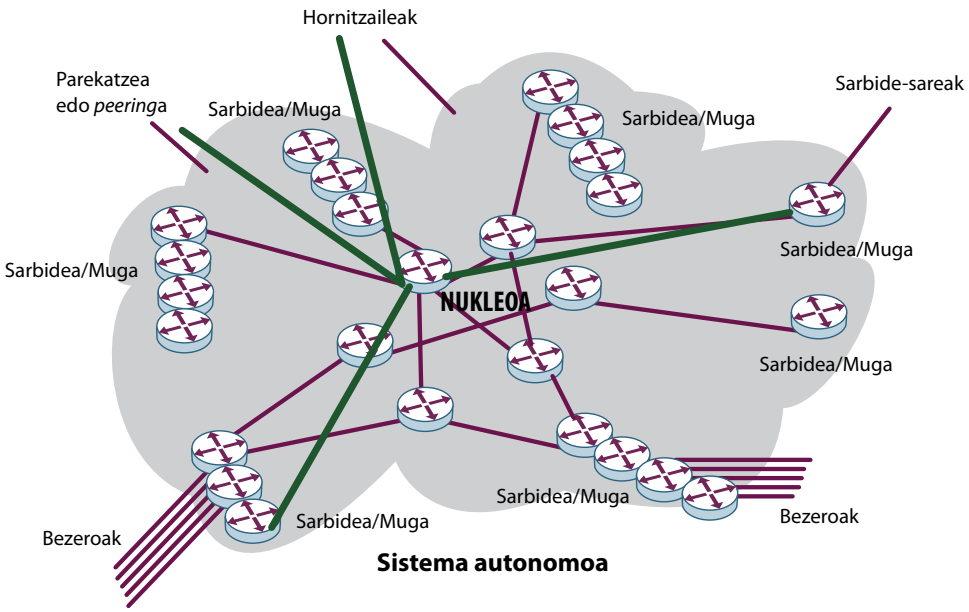
```
protocols {
  bgp {
    group Izena {
      family inet6 {
        labeled-unicast {
          explicit-null;
        }
      }
    }
  }
}
```


5.4.4. Tunelen erabilera

Eraginkortasunaren ikuspegitik, sare nagusian tunelak erabiltzea da aukera txarrena; epe motzerako konponbide bat ematen du, baina ez du balio aurrera egiteko urrats gisa. Hornitzailearen sarearen barruan IPv6 zerbitzuak tunelen bidez ematen badira, diagnostikoak egitea zaila da, IPv6 zerbitzuen erabilgarritasunak ondorioak ditu, eta baliabi-

deak (loturak eta bideratzaileak) ezin dira ondo erabili. Halakoetan, tunelak eskuz konfiguratzen dira. Horiek horrela, aukera hau aldi baterako besterik ez da, eta ezin da sarean behin betiko ezarri.

Sarearen zatiren batean IPv6 ezarri ezin bada, tunel bat konfiguratuta zubi bat eraikitzen da bi IPv6 muturren artean (bi muturren artekoa ezkutatu egiten da), tarteko ekipoak aldatu beharrik gabe. Hala, IPv4 zirkulazio-sarearen topologia eta IPv6 zirkulazio-sarearena desberdinak izango dira. Bigarren irudian ageri da tunelek nola aldatzen duten lehenengo irudiko sarearen topologia. IPv4 bidezko zirkulazioak, mutur batetik bestera joateko, bi bide ditu aukeran. IPv6 bidezko zirkulazioan, ordea, tunelaren konfigurazioaren eraginez, bi muturrak bide bakar bat (tunela) erabiliz lotzen dira, eta sistema horretan zirkulazioak bidea zeharkatu ahal izateko, bi muturretako bideratzaileek erabilgarri egon behar dute.



2. IRUDIA. **TUNELEN ERABILERA. ADIBIDEA**

Tunelak ezartzeko orduan (tunel mota guztiak, ez IPv6 zirkulazioa garraiatzekoak soilik), oso kontuan hartu behar da bai muturren artean onartzen den MTU maximoa eta bai tunelaren interfazeetan konfiguratutakoa. Tunel bakoitza konfiguratu ondoren, tamaina desberdinetako paketeekin zirkulazioa ondo bideratzen dela egiaztatu behar da. RFC4213-ko 3.1 atalean, arazo hau xehe azaltzen dute, baita gomendio batzuk eman ere.

5.4.5. Tunel-aukerak

RFC4213-ko 3. atalean, eskuzko tunelen erabilera bat deskribatzen da. Erabilera horri, tunel automatikoen beste teknika batzuetatik bereizteko, *configured tunneling* (konfigurazioaz baliatuz tunelak egitea) deritzo. RFC horretan bertan, trantsiziorako erabili diren mekanismo automatikoak ere deskribatzen dira, baina ez dira kasu hauetarako erabilga-

rriak. Hornitzaile baten sare nagusian, tunelak erabiltzen dira, hain zuzen, IPv4 mailan soilik ikus daitezkeen bi muturren arteko IPv6 pakete guztiak kapsulatzeko. Paketea IPv4-ren bidez tunelaren muturrera iritsitakoan, muturreko bideratzaileak berreskuratu egiten du kapsulatutako IPv6 edukia, eta IPv6 motako bideratzeari ekiten dio.

Zerbitzu-hornitzaileek oso mekanismo sinplea erabiltzen dute normalean: GRE tunelak (RFC2893). Tunel horiek duela urte askotik erabiltzen dira hainbat protokolo kapsulatzeko, eta ondo frogatua dago badabiltzala. Beste aukera bat L2TPv3 tunelak erabiltzea da (RFC3931).

5.4.6. Bezeroen konexioak tunelak erabiliz

Datozen urteetan, oso ohikoa izango da bezeroek IPv6 bidezko zerbitzuekin probak egin nahi izatea hornitzaileari kontratatutako Internet zerbitzuan pila bikoitza gaitu aurretik. Halaber, gerta liteke bezeroek Internet zerbitzuarentzat konektatua duten bideratzailera ez beste batera IPv6 bidez iritsi behar izatea ere. Horrelakoetan, komeni da IPv6 kapsulatzen duten GRE tunelen muturrak hornitzailearen zerbitzuetan erabilgarri izatea. Hala, bezeroak, hasierako hedapena egiteko, hasieran probatu nahi dituen bideratzaileak soilik erabil ditzake (bat bakarra ere izan liteke).

Tunelen konfigurazioa antzekoa da kasu guztietan. Hona hemen adibide batzuk, erreferentzia gisa:

Cisco IOSerako konfigurazioa

```
interface TunnelAdibideaR1
 no ip address
 ipv6 address 2001:DB8:FFFF::17/64
 tunnel Jatorri-interfazea
 tunnel destination IPv4-Helbidea-Helburua
 tunnel mode ipv6ip
```

Juniperrerako konfigurazioa

```
interfaces {
 Jatorri-interfazea {
  unit UNIT {
   tunnel {
    source IPv4-Helbidea-Jatorria ;
    destination IPv4-Helbidea-Helburua ;
   }
   family inet6 {
    address 2001:DB8::17/64 ;
   }
  }
 }
}
```

6. Ondorioak

Hornitzailearen sare nagusian IPv6 gaitzea ez da lan zaila, eta, segur aski, ekipoetan ez da inbertsiorik egin beharko. Lan hori egin aurretik, ordea, plana egin behar da, eta arreta handiz jokatu behar da sarean aldaketak egiterakoan, bideratze-konfigurazioek eragina baitute nukleoko ekipoetan. Zorionez, garaiz gabiltza hedapena ordena bati jarraituz eta presarik gabe egiteko.

Kapitulu honetan, IPv6 bidezko bideratzea nola gaitzen den besterik ez dugu azaldu. IPv6 bidezko zerbitzuak ematea hori baino lan zailagoa izaten da hornitzaileentzat, liburu honetan jaso ez ditugun alor askori eragiten baitie; alor horiek dira, besteak beste, sarearen zaintza, zerbitzuak hornitzeko sistemak eta kudeaketa-tresnak. Zerbitzariei eta zerbitzuei dagokienez, berriz, badago horiei buruzko kapitulu bat; Internet hornitzaileentzat hori izaten da eman beharreko hurrengo pausoa.

8. Epilogoa

Munduko IPv6-ren hedapenaren ikuspegi orokorra

Aurreko kapituluetan ikusi dugu IPv4 helbideak gaur egun zer egoeratan dauden, IPv6 zergatik behar den, eta Latinoamerikan eta Karibean (liburu hau prestatu dugun tokian) zer urrats egin diren.

Azaldu ditugu, halaber, zenbait sistema eragiletan eta sare-ingurunetan IPv6 hedatzearekin erlazionatutako alderdi teknikoak (etxeko bezeroetatik hasi eta Internet zerbitzu-hornitzaileetara).

Baina zer egoeratan dago IPv6-ren hedapena munduan?

IPv6, oro har, aldaketa bortitzik eragin gabe ari da zabaltzen, batzuetan pauso txikiak emanez, eta beste batzuetan handiak. Hori horrela, hedapenari zer sare motatatik begiratzen zaion, horren araberako informazio zehatzagoa emango dugu.

Hala, sare akademikoei dagokienez, hedapena handia izan da Japonian, Europan eta Ipar Amerikan. Hedapen hori sustatzeko inbertsio publiko handiak egin direlako gertatu da hori, neurri handi batean. Gainera, Europako Batzordeak, sektore pribatuarekin batera, ikerketa eta garapeneko proiektu asko finantzatu ditu; eta proiektu horien bidez industriak eta beste eragile batzuek IPv6 ezagutu, garatu eta estandarizatu egin ahal izan dute, eta hedatzeko beharrezko heldutasunera iritsi dira.

Horrek guztiak ondorio zuzen bat izan du. Herrialde eta eskualde askotan, politika publikoen bidez hau azpimarratu dute: IPv6-ren hedapena ez da garestia, baldin eta plana ondo egiten bada. Alegia, hedapenari aurrea hartu behar zaio (sare bakoitzaren egoera jakinaren araberakoa da plana egiten denetik ezarpena gauzatzen den arte behar den denbora), eta ziurtatu behar da erosten diren ekipoek, aplikazioek eta zerbitzuek IPv6 onartzen dutela; hala, IPv6 gaitu nahi denean, ez dira berriak erosi behar.

Horrelako politika publikoen eraginez, administrazio publikoko sareetan eta haiekin erlazionatutako beste batzuetan (hala nola hezkuntzakoetan, defentsakoetan eta abarretan) IPv6 nahitaez aktibatzeko data jakinak dituzte mundu osoko herrialde eta eskualde batzuetan.

Sare handiei dagokienez, hots, operadore handien sareei dagokienez, eta, batez ere, nazioarteko operadoreei dagokienez (haietako gehienek kontinentearteko sareak dituzte), operadore gehienek pauso handiak eman dituzte IPv6 onartzeko bidean, eta askok IPv6 bidezko oso zerbitzu ona ematen dute.

Baina egoera oso bestelakoa da azken erabiltzaileen muturrean eta Internet zerbitzu-hornitzaile nazionalen nahiz eskualdeko Internet zerbitzu-hornitzaileen sare askotan (badira salbuespenak Japonian, Asiako beste herrialde batzuetan eta Europako eta Ipar Amerikako kasu gutxi batzuetan).

Zein da egoera sistema eragileen, aplikazioen eta zerbitzuen ikuspegitik?

Berez, aurreko kapituluetan argi gelditu denez, ordenagailuen, sakelako telefonoen eta beste gailu askoren sistema eragileak 2001 urtean hasi ziren IPv6 onartzen, eta, gaur egun, ez da erraza IPv6 onartzen ez duten sistemak aurkitzea. Gainera, Internet zerbitzu-hornitzaileek IPv6 bidezko zerbitzurik ematen ez dutenean ere erabil dezakete gailuek IPv6, IPv6-ren diseinuari, IPv6-ren hedapenak IPv4-rekin paraleloan lan egiteko moduan antolatu izanari eta lehenago deskribatutako trantsizio-mekanismoei esker.

Trantsizio-mekanismo automatikoak erabiltzea ez da oso aukera ona. Berez, egokiena da Internet zerbitzu-hornitzaileek azken bezeroen muturrean ere IPv6 ezartzea. Baina, oro har, mundu osoan, urrats hori egiteko dago, eta, horregatik, ahalegin handia egin behar da.

Aplikazioei dagokienez, sistema eragileek oro har IPv6 ondo onartzen dutenez, gero eta ohikoagoa da aplikazioak IPv4-rekin nahiz IPv6-rekin ibiltzea.

Zerbitzuei dagokienez (zerbitzuak dira, adibidez, web-zerbitzariak), IPv6 motel hedatzen ari da, datu-zentroek eta Internet zerbitzu-hornitzaileek ez baitute hedapena egiteko beharrik sumatu (IPv6 ezartzeko arrazoi izango lirateke, adibidez, berehalako pizgarri ekonomikoak). Bada, noski, salbuespenik. Adibidez, Google, zeinak duela bi urte soilik hasita urrats handiak egin baititu. Horrek lehiakideak antzeko erabakiak hartzera bultzatuko ditu, bultzatuko dituenez.

Zirkulazioari dagokionez, azkenik, azken erabiltzaileen muturrean egoera zein den ikusi ondoren espero izatekoa denaz oso bestelakoa da IPv6-ren ezarpenaren egoera. Trantsizio-mekanismoak zeharkatzen dituen IPv6 zirkulazioa nabarmen hazten ari da duela bi urte baino gehiagotik, batetik, erabiltzaile-plataforma ia guztietan IPv6 aktibatua dagoelako (are, ikusi dugunez, sistema eragile askok lehenespenez gaitzen dute), eta, bestetik, trantsizio-mekanismo automatikoei eta aplikazio batzuei (batez ere parekoen edo P2P aplikazioei) esker. Eragin handia izan dute, adibidez, aplikazio hauek: BitTorrent, berehalako mezularitzako aplikazioak, eta sare pribatu birtual automatikoetako aplikazioak.

Banda-zabalera garesti duten eskualdeetan, zirkulazioa automatikoki gehitzea eragingarri ekonomiko handia izango da, Internet zerbitzu-hornitzaileek azken erabiltzaileen muturrean IPv6 lehenbailehen ezar dezaten edo beraien sareetan beretan kokatutako trantsizio-elementuak (adibidez, 6to4 eta Teredo erreleak) erabil daitezen. Hori eginez gero, banda-zabaleran aurreztuko dute, eta bezeroei ematen dieten zerbitzuaren kalitatea nabarmen hobetuko da.

Agortzear daude gailuek Internetera konektatzeko erabiltzen dituzten IPv4 helbideak.

Internetek arrakasta handia izan duenez, zerbitzuak ugaritu eta zerbitzu berriak sortu direnez, eta teknologia etengabe garatu denez, IP protokoloaren bertsio berri bat landu behar izan da (IPv6), behar beste IP helbide izateko (protokolo berrian 340 sextilioi helbide daude).

Protokolo berri hori ezartzeko eta behin betiko geureganatzeko prozesua, ordea, motela da, baina irmoa. Nazioarteko erakunde batzuk (adibidez, Internet Society, LACNIC eta Europako Batzordearen diru-laguntza jasotzen duen 6DEPLOY proiektua) protokolo berria sustatzeko lanean ari dira dagozkien eskualdeetan. Horretarako, mintegiak, hitzaldiak, ikastaroak, tailerrak eta abar antolatzen dituzte.

IPv6 nonahi baliatzeko gidaliburu hau ISOCen Argentina atalaren proiektu bat da, eta erabiltzaileei IPv6 hainbat ingurunetan ezartzeko behar dituzten tresnak emateko asmoz egin dugu, hizkuntza argi eta erraz bat erabiliz eta termino teknikoak baztertuz.

Mónica Abalo Laforgia doktorea
Lehendakaria
Internet Societyren Argentina atala - ISOC-Ar

Laguntzaileak