Arttu Kuulas

Internet-yhteyden kahdentaminen

Metropolia Ammattikorkeakoulu
Tietotekniikka
Tietoverkot
Opinnäytetyö
25.5.2012

Tekijä(t) Otsikko Sivumäärä Aika	Arttu Kuulas Internet-yhteyden kahdentaminen 74 sivua + 1 liite 25.5.2012
Tutkinto	Insinööri AMK
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Marko Uusitalo Tietoliikennepäällikkö Olli Oravainen

Insinöörityössä rakennettiin kahdennettu Internet-yhteys tietoverkon reunalle ulkomaailmaan meneviä yhteyksiä varten. Kahdennuksen ohella tutustuttiin Internetin reitityksestä vastaavaan BGP-protokollaan sekä Internetin rakenteeseen.

Työn alkupuolella käsitellään Internetin rakennetta, sen hallinnollisia järjestelmiä sekä eri järjestelmien välisiä yhteyksiä. Tämän jälkeen työssä käsitellään BGP-protokollaa ja sen ominaisuuksia. BGP-protokolla mahdollistaa reititystietojen jakamisen eri järjestelmien välillä. Työssä tutustuttiin myös BGP-reitityspolitiikoihin yrityksen kannalta.

Verkon reunalle tehtiin reitittimistä sekä muista verkon aktiivilaitteista verkon osa-alue, joka vastaa Internet-reitityksestä.

Yritykset käyttävät Internet-yhteyttä yhä enemmän palveluiden tarjoamiseen asiakkaille ja kumppaneille. Internet-yhteyden kahdentaminen varmistaa yrityksen palveluiden toiminnan jatkumisen, jos toinen yhteyksistä katkeaa. Kahdentaminen nostaa palveluiden saatavuutta ja tavoitettavuutta.

Avainsanat	Internet, BGP, Border Gateway Protocol, Kahdentaminen

Author(s) Title Number of Pages Date	Arttu Kuulas Redundant Internet Connections 77 pages + 1 appendices 25 April 2012
Degree	Degree Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Communications and Data Networks
Instructor(s)	Olli Oravainen, IT-manager Marko Uusitalo, Principal Lecturer

Redundant Internet connection was built in this project. This project also focused on Internet routing with BGP and the structure of the Internet.

First, the structure of the Internet and its autonomous systems was covered along with interconnections between the systems. After that, introduction to BGP and its routing functions along with BGP policies used by companies was given.

Companies offer Internet based services for their partners and customers. Redundant Internet connection allows backup route to take the precedence if the main connection goes down. Redundancy increases availability and accessibility of the services.

Keywords	Internet, BGP, Border Gateway Protocol, Redundancy

Sisällys

Lyhenteet

AfriNIC	African Network Information Centre. Afrikan valtioiden käyttämä alueellinen RIR-rekisteri.
APNIC	Asian Pacific Network Information Centre. Aasian ja Tyynenmeren alueellinen RIR-rekisteri.
AS	Autonomous System. Autonominen järjestelmä, joka on saman tahon hallinnan alla oleva järjestelmä Internetissä.
ASN	Autonomous System Number. Autonomisen järjestelmän numero, jonka perusteella järjestelmät voidaan tunnistaa.
ARIN	American Registry for Internet Numbers. Pohjois-amerikan RIR-rekisteri.
BGP	Border Gateway Protocol. Ulkoinen reititysprotokolla, jonka tehtävänä on vastata Internetin reitityksestä.
CIDR	Classless Inter Domain Routing. IP-osoitteiden jakaminen luokatonta verkkomaskia käyttäen.
eBGP	external BGP. BGP-protokolla, joka toimii eri autonomisten järjestelmien reunareitittimien välillä.
FICIX	Finnish Communication and Internet Exchange. Suomalainen yhdysliikennepiste, jossa operaattorit voivat vaihtaa reititystietoja.
IANA	Internet Assigned Numbers Authority. Organisaatio, joka hallinnoi ja jakaa Internetin resursseja maailmanlaajuisesti.
iBGP	internal BGP. BGP-protokolla, joka toimii autonomisen järjestelmän sisällä.

IGP Interior Gateway Protocol. Sisäinen reititysprotokolla, joka ei yleensä osallistu ulkoiseen reititykseen.

IP Internet Protocol. Protokolla, joka huolehtii pakettien välittämisestä Internetin yli kohteeseen.

IRR Internet Routing Registry. Internetissä sijaitsevia rekistereitä, joihin on tallennettu eri järjestelmien reitityspolitiikat RPSL-kielellä.

LACNIC Latin American and Caribbean Network Information Centre. Etelä-Amerikan ja Karibian alueen RIR-rekisteri.

LIR Local Internet Registry. Paikallinen Internet-rekisteri, joka hallinnoi sille määritettyjen resurssien jakoa.

MD5 Mesasge-Digest algorithm 5. Kryptografinen menetelmä, jota voidaan käyttää esimerkiksi tarkastamaan onko viestin sisältö muuttunut siirron aikana.

MED MULTI EXIT DISC. BGP:n käyttämä attribuutti, jolla voidaan ilmaista naapurijärjestelmälle halukkuus tietyn reitin käytöstä.

NAT Network Address Translation. Tekniikka, jonka avulla tietoliikennelaite voi muokata IP-paketissa olevia kohde- sekä lähdeosoitteita ja kohde- sekä lähdeportteja.

OSI-malli Open Systems Interconnection Reference Model. Käsitteellinen malli, joka kuvaa tiedonsiirrossa käytettävät protokollat.

OSPF Open Shortest Path First. Linkkitietoihin perustuva sisäinen reititysprotokolla.

PA Provider Aggregatable assignment. IP-osoitelohko, joka on saatu operaattorilta.

PI	Provider Independent assignment. IP-osoitelohko, joka on saatu RI-rekisteriltä suoraan.
RIB	Routing Information Base. Reitittimen reititystaulu.
RIP	Routing Information Protocol. Reititysprotokolla, joka käyttää metriikkanaan hyppyjen määrää.
RIPE	Réseaux IP Européens. Euroopassa toimiva järjestö, joka on yksi Internetin kehitykseen osallistuvista järjestöistä.
RIPE NCC	Réseaux IP Européens Network Coordination Centre. Euroopan, Lähi-idän ja Keski-Aasian RIR-rekisteri.
RIR	Regional Internet Registry. Organisaatio, joka vastaa tietyn maantieteellisen alueen Internet-resurssien allokoinnista ja hallinnasta.
RPSL	Routing Policy Specification Language. Reititystietojen merkkauskieli, jonka avulla operaattorit voivat kuvata oman reitityspolitiikkansa.
SPOF	Single Point Of Failure. Piste, joka vikaantuessaan voi aiheuttaa muun järjestelmän toimimattomuuden.
TCP	Transmission Control Protocol. Tiedonsiirtoprotokolla, joka sisältää menetelmät luotettavaan viestien vaihtoon päätepisteiden välillä.
VPN	Virtual Private Network. Tekniikka, jonka avulla voidaan luoda turvallinen tiedonsiirtoväylä Internetin tai muun verkon yli.

1 Johdanto

Insinöörityön tavoitteena on luoda kahdennettu ja virhetilanteista nopeasti palautuva yhteys Internetiin kahden eri palveluntarjoajan kautta. Työn on tilannut Helsingin Energian konsernin liiketoiminto ICT-Palvelut.

Työssä luodaan verkon reunalle modulaarinen verkkoratkaisu, joka noudattaa nykyaikaista verkkoarkkitehtuuria sekä parhaita käytäntöjä. Yhden toimittajan varassa oleva Internet-yhteys on riskitekijä, jos yrityksellä on bisneskriittisiä sovelluksia, joiden tulee toimia Internetin yli. Kahdennus parantaa sovellusten tavoitettavuutta ja luo arvoa yritykselle paremman saatavuuden kautta.

Kahden palveluntarjoajan kautta yrityksen verkon mainostaminen mahdollistaa Internetin käytön jatkumisen, vaikka toisen palveluntarjoajan yhteydet ulkomaailmaan katkeaisivat. Ratkaisu vaatii yritykseltä oman IP-osoiteavaruuden sekä hallinnollisen järjestelmän numeron, jotka voidaan anoa alueelliselta osoiteorganisaatiolta.

Työssä käsitellään kahdentamiseen liittyen Internetin rakennetta ja siihen liittyvää ulkoista reititysprotokollaa, joka mahdollistaa verkkojen tavoitettavuuteen liittyvien tietojen jakamisen eri Internetin hallinnollisten alueiden välillä.

2 Käsitteitä

2.1 IP-Osoite

IPv4-osoite on 32-bittinen luku, jota käytetään OSI-mallin verkkokerroksella verkon laitteiden tunnistamiseen. IP-osoitetta käytetään, kun halutaan ottaa yhteys verkon toiseen laitteeseen. IP-osoite toimii yhteyden lähde- sekä kohdeosoitteena. IP-osoite jaetaan loogisesti kahteen eri osaan, jotka ovat verkolle varattu osa sekä päätelaitteille varattu osa. Osoitteen ensimmäiset bitit on varattu verkko-osoitteille ja jälkimmäiset päätelaitteille. Verkkomaski koostuu bittijonosta, joka kertoo, mitkä IP-osoitteen bitit ovat verkko- ja päätelaiteosoitteita. IP-osoitteen ja verkkomaskin perusteella verkon laitteet pystyvät päättelemään, mihin verkkoon ja mihin porttiin yhteys tulee ohjata. [1, s. 35-40.]

IP-osoitteesta on myös 128-bittinen versio, IPv6, mutta tässä työssä käsitellään vain IPv4-osoitteita.

2.2 Reitittäminen

Reititys tapahtuu reitittimissä, jotka toimivat OSI-mallin verkkokerroksella. Reitittimen tehtävä on välittää liikenne oikeaan paikkaan IP-paketin otsakkeiden perusteella. Reitittäminen tapahtuu reititystaulun avulla, joka rakentuu staattisista tai reititysprotokollilta opituista reiteistä kohdeverkkoihin. IP-paketin kohdeosoite toimii hakuavaimena taulukkoa vasten. Taulukosta saadaan tieto siitä, mistä portista paketti ohjataan kohti tavoiteltua verkkoa ja mikä on seuraavan hypyn osoite. Kohdeosoitetta verrataan sen mukana tulevaan verkkomaskiin, jonka avulla reititystaulusta pyritään löytämään lähimmäksi vastaava kohdeverkko. Reitittimet mahdollistavat tavoitettavuuden eri verkkojen välillä. [2, luku 2.1.]

2.3 Reititysprotokollat

Reititysprotokollien tehtävänä on vaihtaa verkon saatavuustietoja muiden verkon reitittimien kesken. Saatavuustietojen perusteella valitaan reitit kohdeverkkoon ja asennetaan paras reitti IP-reititystauluun, (IP-RIB). Reititysprotokollat ovat dynaamisia eli ne reagoivat verkon muutoksiin ja päivittävät tiedot muutoksesta myös muille reitittimille,

joiden kanssa ne keskustelevat. Reitit samaan kohdeverkkoon luokitellaan ja ne järjestetään arvon/hinnan mukaan, joista tyypillisesti vain paras reitti asennetaan reititystauluun. Reitin arvo määräytyy eri ominaisuuksista, jotka vaihtelevat reititysprotokollittain. Reititysprotokollat mahdollistavat laajemmat reitittävät verkkoalueet, joiden reitityksen suunnittelu olisi erittäin vaikeaa staattisia reittejä käyttämällä. [3, luku 4.]

3 Internetin rakenne

Internet on laaja kommunikaatioverkko, joka yhdistää pienempiä alueita toisiinsa luoden tietoliikenneväylän jokaiselle verkkoon liitetylle koneelle. Internet ei ole kenenkään omaisuutta eikä sen kehitystä aja vain yksi yritys, vaan sen laajuuden takia on syntynyt useita organisaatioita, jotka vastaavat Internetin kehityksestä. Internet on kaikille avoin, ja se on syntynyt useiden organisaatioiden yhteistyöstä. Internet on heterogeeninen järjestelmä, eli se sisältää useita eri tekniikoihin pohjautuvia järjestelmiä, jotka yhdistetään kaiken perustana olevan TCP/IP-protokollaperheen avulla. Nykyään useat tahot tekevät yhteistyötä optimoidakseen Internetin tehokkuutta kommunikaatioväylänä.[4, luku 1 ja 2.]

3.1 Autonomiset järjestelmät

Internet koostuu autonomisista järjestelmistä (Autonomous System, AS), jotka ovat jonkin organisaation ylläpitämiä. Yleensä nämä organisaatiot ovat teleoperaattoreita, palveluntarjoajia tai suuria yrityksiä. Hallinnollisen alueen ylläpitäjän vastuulla ovat alueella käytettävät IP-osoitteet, laitteet, reititysprotokollat ja se, mitä reititystietoja jaetaan eteenpäin muille järjestelmille. Jokainen Internetiin yhdistetty kone sijaitsee jollakin hallinnollisella alueella ja sille on määritelty alueelle kuuluva julkinen IP-osoite. Autonominen järjestelmä on siis tietty verkkokonaisuus, joka on jonkin organisaation hallinnassa. [5, luku 1, 3; 6, s.1.]

Autonomisen järjestelmän sisällä reititystietoa jaetaan erilaisilla sisäisillä reititysprotokollilla (Interior Gateway Protocol, IGP), kuten RIP, EIGRP ja OSPF. Alueen omistajalla on valta määrittää alueensa sisäinen reititys ja se, kuinka alueelle määritetty IP-

avaruus jaetaan. Alueen sisäisessä reitityksessä voidaan myös käyttää privaatteja IP-osoitteita, joita ei reititetä toisille alueille. [5, luku 3.]

Autonomisten alueiden välillä reititystietoja jaetaan BGP-protokollan ylitse, jolloin protokollasta käytetään yleisesti nimitystä eBGP (External-BGP). BGP voi toimia myös AS:n sisällä reitittimien välillä jakaen eBGP:ltä saatua reititystietoa. Tällaisessa tapauksessa protokollasta käytetään nimeä iBGP (Internal-BGP). Ulospäin reititystietoina jaetaan ainakin alueeseen kuuluvat IP-avaruudet, jotta muille alueille välittyy tieto, mistä alueen IP-osoitteet löytyvät ja mitä reittiä pitkin sinne pääsee. Jos ulos jaetaan myös muiden alueiden verkko-osoitteita, niin on mahdollista, että näitä osoitteita jakavaa aluetta voidaan käyttää siirtoverkkona muiden alueiden liikenteelle.

Jokainen autonominen alue päättää itse, mitä osoitteita halutaan ottaa vastaan ja mitä osoitteita jaetaan ulos, eli reititys on muista alueista riippumatonta. Jokaisella autonomisella alueella on oma reitityspolitiikka ja naapurialueiden välillä voi suodattaa reittejä pois tai olla hyväksymättä naapurin tarjoamia reittejä, jonka seurauksena on vaikea ennustaa pakettien kulkemaa reittiä ulkoverkossa. [7, ss2-3.]

3.1.1 Autonomisen järjestelmän numero

Jokaisella autonomisella järjestelmällä on uniikki autonomisen järjestelmän numero (Autonomous System Number, ASN), jonka avulla ne voidaan tunnistaa. 16-Bittinen AS-numero mahdollistaa 65536 uniikkia järjestelmätunnusta, joista 1 - 64511 ovat käytettävissä. Arvot 64512 – 65534 ovat varattuina sisäisiksi AS-numeroiksi, jotka ovat yksityistä käyttöä varten ja joita ei käytetä Internetin reitityksessä. [7, luku 10.] Lisäksi erikoiskäyttöön varattuina ovat AS-numerot 23456 ja 65535. Internetin kasvun takia 16-bittiset AS-numerot ovat hupenemassa ja rinnalle ollaan ottamassa 32-bittinen AS-numero, joka laajentaa käytettävien järjestelmätunnuksien määrän noin 4,3 miljardiin. [8, luku 1, 2 ja 13.]

32-Bittiset AS-numerot merkataan käyttäen seuraavaa formaattia: <ylemmät 16 bittiä>.<alemmat 16 bittiä>, joka tarkoittaa sitä, että ensimmäinen AS-numero on 0.0 ja viimeinen 65535.65535. Arvot 0.0 – 0.65355 on jätetty 16-bittisiä AS-numeroita varten yhteensopivuuden takaamiseksi. Uuden formaatin ja 32-bittisen AS-numeroiden käyt-

töönotto vaatii kuitenkin muutoksia muihin verkon osiin, kuten BGP-protokollaan ja siksi se ei ole vielä saavuttanut suurta suosiota. [9, kappale 32-Bit AS Numbers.]

BGP-reititys perustuu AS-numeroihin, joita käytetään BGP-reitityksessä polun muodostamiseen eri AS:ien verkkojen välillä. ASN on globaalisti uniikki ja, se voidaan määrätä vain yhdelle organisaatiolle käyttöön kerralla, mutta yksi organisaatio voi omistaa useamman ASN:n. AS-numeroiden jakamista kontrolloi viisi eri organisaatiota ARIN (Pohjois-Amerikka), RIPE NCC (Eurooppa), APNIC (Aasia), LACNIC (Etelä-Amerikka), AfriNIC (Afrikka), joita kutsutaan myös alueellisiksi Internet–rekistereiksi (RIR). [8, luku 3.]

3.2 Internetin hallinnollinen hierarkia

3.2.1 RIPE NCC & RIPE

Alueellisten Internet-rekistereiden tehtävänä on edistää Internetin kehitystä jakamalla avoimesti tietoa, kontrolloimalla Internetiin liittyvien resurssien, kuten IP-osoitteiden ja AS-numeroiden, jakoa sekä ylläpitämällä tietokantoja hallinnoitavan alueen resursseista. RIPE NCC hallinnoi Euroopan, Lähi-idän sekä Keski-Aasian maiden Internet-resurssien käyttöä, ja se on yksi viidestä alueellisesta Internet-rekisteristä. Tällä hetkellä alueeseen kuuluu 78 valtiota sekä 7 150 jäsentä. RIPE NCC on toiminut vuodesta 1992 lähtien, ja se on perustettu Hollannissa RIPE-yhteisön aloitteesta luoda erillinen hallinnollinen elin toiminnalle, joka tukee RIPE-yhteisöä päätöksenteossa. RIPE NCC ja RIPE ovat erillisiä, mutta tiivistä yhteistyötä tekeviä järjestöjä. RIPE on ollut olemassa vuodesta 1989 asti. [10.]

RIPE NCC:n toimintaa ohjaa RIPE:n kokouksissa, jotka järjestetään kaksi kertaa vuodessa sekä työryhmissä käydyt keskustelut ja niiden pohjalta luodut politiikat. Näihin osallistuminen on kaikille vapaata ja kuka tahansa voi aloittaa uuden politiikan luomisen, mutta sen on käytävä politiikan luontiin liittyvä prosessi läpi (RIPE Policy Development Process, PDP). Prosessi sisältää neljä vaihetta, jotka jokainen uusi ehdotus käy läpi alkaen aina ehdotuksen luomisesta, keskusteluvaiheesta, arvioinnista sekä yhteenvedosta. Prosessin tavoitteena taata avoin keskustelu, dokumentointi, joka on kaikkien saatavilla, sekä päätöksen hyväksyminen, kun on saavutettu yksimielisyys asiasta. Tä-

män jälkeen uusi politiikka ja siihen liittyvä dokumentointi on lisättävä RIPE-dokumenttikantaan, joka löytyy Internetistä ja on kaikkien käytettävissä. [11.]

3.2.2 RIPE-tietokanta

RIPE hallinnoi WHOIS-tietokantaa, johon on tallennettu tieto hallinnoiman alueen IP-osoitteista, AS-numeroista, reitityspolitiikoista sekä rDNS-tiedoista. Tietokanta koostuu useista objekteista, jotka sisältävät selkokielisenä tekstinä listan ominaisuus-arvo –pareista. Tietokannasta voidaan tehdä hakuja esimerkiksi Internetissä olevilla hakukoneilla tai WHOIS-hakuohjelmilla. Tietokannan tarkoituksena on jakaa tietoa alueista, niihin kuuluvista IP-osoitteista sekä niitä hallitsevista tahoista. Tietokannasta löytyvät reititystiedot ovat tallennettuna RPSL-kielelle, jonka syntaksien mukaan eri alueiden ylläpitäjät voivat tallentaa reitityspolitiikkansa muiden nähtäväksi.

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
% Information related to 'AS51150'

aut-num:        AS51150
as-name:        GABENYNET
descr:          SC GABENY PROMOTION SRL
org:            ORG-GPS3-RIPE
import:         from AS30890 accept ANY
import:         from AS49687 accept ANY
export:         to AS30890 announce AS51150
export:         to AS49687 announce AS51150
admin-c:        DG2380-RIPE
tech-c:         DG2380-RIPE
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         GABENY-MNT
mnt-routes:     GABENY-MNT
source:         RIPE # Filtered
```

Esimerkki 1. Näkymä WHOIS-tietokannan sisältämästä tiedosta, joka on RPSL-kielen syntaksien mukaista.

Esimerkin 1 vasemmassa laidassa on merkittynä objektin ominaisuudet ja oikealle puolelle niiden arvot. Esimerkin aut-num- sekä import- että export-kentät viittaavat autonomisen systeemin 51150 ulkoiseen reitityspolitiikkaan. Reitityspolitiikka kertoo, mitä verkkoja vastaanotetaan muilta ja mitä verkkoja mainostetaan muille AS-alueille. Lisäksi muissa kentissä on kerrottuna mm. organisaation nimi sekä tunnus ja objektin hallitsija.

Internetin reititysrekistereitä, IRR (Internet Routing Registry), on viisi kappaletta: CA*Net, ANS, CW, RADB sekä RIPE, ja ne pitävät tietokannassaan tallennettuna tiedon eri autonomisten alueiden reitityspolitiikoista. Nämä rekisterit päivittävät päivittäin tietokantojen sisällön toisilleen varmistaakseen tietojen säilymisen, vaikka yksi rekistereistä olisi saavuttamattomissa. Tietojen päivittäminen yhteen rekisteriin on riittävää ja IR-rekisterit muodostavatkin yhdessä yhden ison tietokannan, jonka avulla on mahdollista tarkastella maailmanlaajuisesti reitityspolitiikoita.

RPSL mahdollistaa reitittimen konfiguraatiotiedoston luomisen suoraan IR-rekisterin tietokannasta löytyvien RPSL-kielen mukaan kuvattujen tietojen perusteella, jonka seurauksena tietoliikennelaitteiden ulkoisen reitityspolitiikan luominen helpottuu. Tällä pyritään ehkäisemään virheellisten reititystietojen jakamista, joka saattaa tapahtua helposti, jos reitittimen konfiguraatio tehdään käsin. Tietokannasta voi myös tarkistaa muiden autonomisten alueiden reitityspolitiikat ja ottaa ne huomioon omia reitityspolitiikoita suunniteltaessa. [12, luku 1;13, luku 1; 3, s.66-74.]

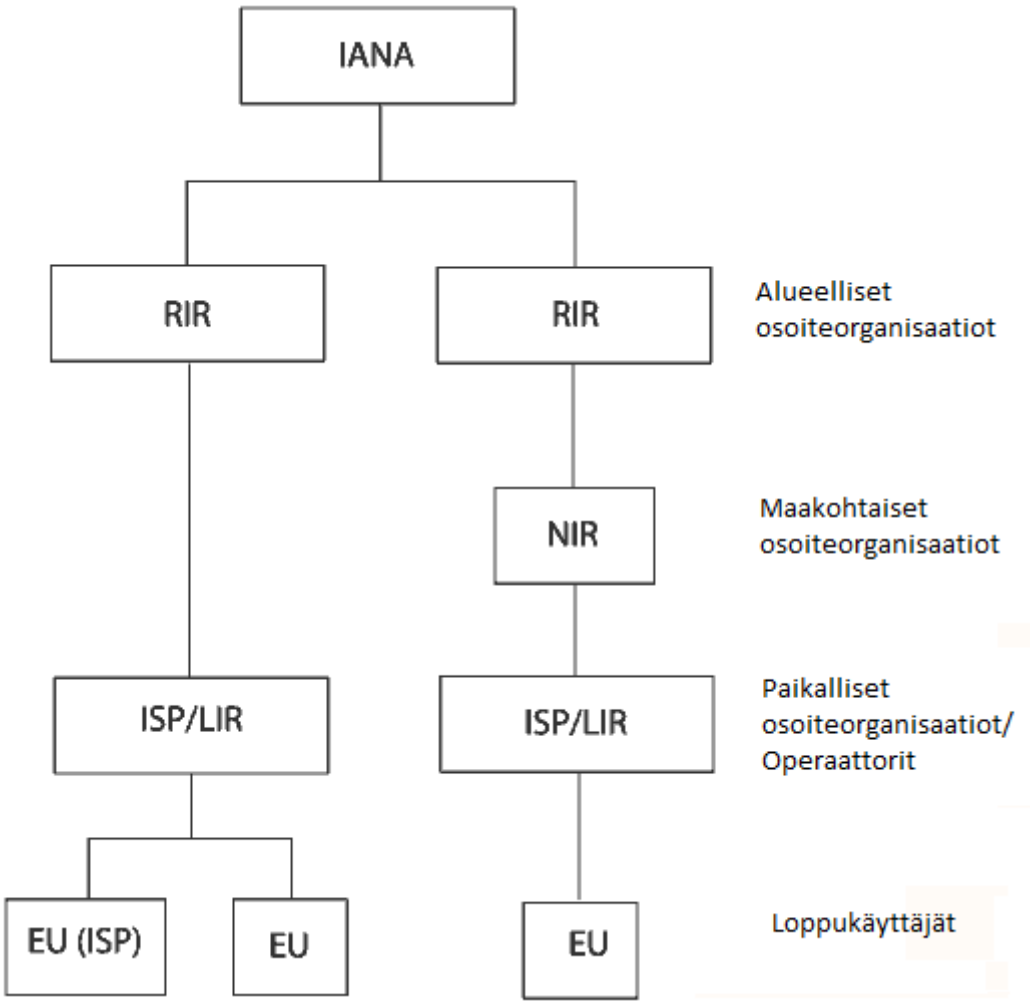
3.2.3 IANA

Maailmanlaajuisesti resurssien varausta hallinnoi IANA (Internet Assigned Numbers Authority), joka jakaa alueellisille Internet-rekistereille verkko-osoitelohkoja ja autonomisen järjestelmän numeroita. IANA myös hallinnoi juurinimipalvelimia ja lukuisia muita Internetin infrastruktuurille tärkeitä komponentteja. Kaikki alueelliset Internet-rekisterit toimivat IANA:n alaisuudessa. [8, luku 3; 13, luku 1 ja 2.]

IANA jakaa verkko-osoitelohkot A-luokan osoitteina, joka tarkoittaa 32-bittisessä IPv4-osoitteessa sitä, että 8 ensimmäistä bittiä on varattuna verkko-osoitteelle ja loput 24 bittiä on päätelaitteita varten, joka tarkoittaa yhteensä 16 777 216 (2^{24}) käytettävää osoitetta per lohko. [14.]

IPv4-osoitteet ovat loppumassa ja sen seurauksena ollaan siirtymässä 128-bittisten IPv6-osoitteiden käyttöön, joita IANA jakaa minimissään /12-maskin lohkoissa, joka tarkoittaa 12 bitin varaamista verkko-osoitteelle ja 116 bitin varaamista päätelaitteita varten eli 2^{116} käytettävää osoitetta per lohko. Allokaatio pyritään tekemää niin, että se

täyttää osoitetarpeen vähintäänkin seuraaviksi 18 kuukaudeksi. Uusia lohkoja jaetaan, kun vanhat lohkot ovat ehtymässä. [15.]



Kuva 1. Internetin hierarkiaa.

3.3 IP-osoitteiden hierarkia

Internetin rekistereiden hierarkian pohjalla ovat lokaalit Internet-rekisterit (Local Internet Registries, LIR), jotka saavat resurssinsa alueellisilta rekistereiltä. Lisäksi on olemassa välimuotoja, kuten maakohtaiset rekisterit (National Internet Registries, NIR), jotka huolehtivat resurssien jakamisesta valtion sisällä. Maakohtaisia rekistereitä on pääosin vain APNIC- sekä LATNIC-alueilla. [16.]

Lokaaliksi Internet-rekisteriksi luokitellaan organisaatiot, jotka ovat solmineet jäsensopimuksen alueellisen Internet-rekisterin kanssa. Yleensä tällaiset organisaatiot ovat

operaattoreita tai palveluntarjoajia. LIR pystyy jakamaan eteenpäin RI-rekisteriltä saatua osoitelohkoa sekä anomaan uusia osoitelohkoja ja AS-numeroita käyttöönsä tarpeen mukaan. Käytännössä tämä tarkoittaa resurssien vastuun siirtämistä niin, että jokainen LIR noudattaa itse omaa politiikkaa osoitteiden jakamisessa. [17, luku 3.2.1.]

LI-rekisterit saavat käyttöönsä suuria osoitelohkoja, jotta Internetin reititystaulu olisi helpommin hallittavissa ja skaalautuvampi. RIPE NCC ei esimerkiksi hyväksy jäseniksi yrityksiä tai organisaatioita, jotka haluaisivat vain pienen osoitelohkon käyttöönsä. Tämä aiheuttaisi reitityksen skaalautumisessa ongelmia, sillä useita pienempiä osoitelohkoja voi olla vaikea tai mahdoton ryhmittää ja jakaa ryhmitettyä reititystietoa eteenpäin. [18, luku 4.]

Loppukäyttäjä, joka on yleensä yritys, voi anoa osoitteita ja AS-numeroita joko suoraan RI-rekisteriltä tai solmimalla sopimuksen LIR:n kanssa, jonka osoiteavaruudesta yritykselle lohkotaan oma osuus käyttäen luokatonta verkkomaskia (CIDR). Tyypillisesti yritykset vuokraavat operaattorin omistuksessa olevasta IP-avaruudesta lohkon, jolloin yrityksen ei itse tarvitse ostaa tai ylläpitää omaa verkkolohkoaan, eikä myöskään huolehtia verkko-osoitteen toivotettavuustietojen jakamisesta muualle Internetiin. Huomattavasti yleisempi tapa, ja myös reitityksen kannalta parempi vaihtoehto, on tehdä sopimus LIR:n kanssa. LIR voi myös tehdä tarvittavat rekisterimuutokset IRR:n kantaan sekä ylläpitää rekisterimerkintöjä, joka vähentää yrityksen oman IT-hallinnon taakkaa. [19, luku 9; 18, luku 4.]

Suoraan RI-rekisteriltä saatu osoiteavaruus, toimittajariippumaton osoite (Provider Independent, PI-osoite), kulkee aina loppukäyttäjän mukana, mutta vaatii sen, että loppukäyttäjä ja palveluntarjoaja sopivat alueen reitittämisestä muualle Internetiin. PI-osoitteet hankaloittavat reittien yhdistämistä, sillä ne eivät tule palveluntarjoajan omasta osoiteavaruudesta, vaan näitä verkkoja joudutaan mainostamaan erikseen palveluntarjoajan omien verkkojen lisäksi. LI-rekisteriltä saatu osoiteavaruus (Provider Aggregatable, PA-osoite) on helppo summata muiden loppukäyttäjien verkkojen kanssa, jotka on myös saatu samalta LIR:ltä ja sen mainostamisessa voidaan käyttää CIDR-merkintää hyödyksi, eli verkot voidaan summata ennen mainostamista, jolloin ne rasittavat vähemmän Internetin reititystaulua.[20, luku 2] Huonona puolena PA-osoitteelle voidaan mainita se, että jos yritys päättää vaihtaa palveluntarjoajaa on yrityksen myös

vaihdettava omat julkiset IP-osoitteet, sillä PA-osoitteet eivät ole yrityksen omistuksessa. PA-osoite voidaan nimittää aina uuden asiakkaan käyttöön. [21, luku2.1; 19, luku 9.]

Internetin reititystaulua pyritään pitämään pienenä ja helposti hallittavana reittien summaamisella ja siksi RIR:t pyrkivät välttämään verkkojen sirpaloitumista jakamalla osoiteavaruuksia järkevästi, jotta ne voidaan summata.

Esimerkki palveluntarjoajan verkosta, jonka osoiteavaruudet eivät ole yhtenevät, eli se on sirpaloitunut.

Palveluntarjoajan verkot 192.168.0.0/24, 192.168.1.0/24 ja 192.168.60.0/24. Kaksi ensimmäistä verkkoa voidaan mainostaa summattuna verkkona 192.168.0.0/23 ja sen lisäksi joudutaan mainostamaan vielä verkko 192.168.60.0/24 erikseen. Seurauksena se, että naapurille mainostetaan kahta eri verkko-osoitetta, mikä vastaavasti lisää reititystaulujen raskautta. Jos edellisen esimerkkitapauksen verkot olisivatkin 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 ja 192.168.3.0/24, niin naapuri AS:lle voitaisiin mainostaa pelkästään 192.168.0.0/22-verkkoa. Tämä osoittaa, kuinka tärkeää on IP-osoitteiden allokoinnin kontrollointi ja luokattomien maskien käyttö reititystietoja jakaessa.

Lisäksi on otettava huomioon, että pienempien ja sirpaloituneiden IP-lohkojen käyttäminen ei onnistu aina, sillä jotkin operaattorit ei välttämättä suostu reitittämään pienempiä lohkoja. Eikä ole taetta, että ylemmän tason operaattorit reitittävät hierarkiassa alempana olevien operaattoreiden asiakkaiden PI-osoitteita. PA-osoitteet noudattavat hierarkiaa ja niiden reititys voidaan taata. [22, luku 1 ja 2; 18, luku 4.]

3.4 Autonomisten järjestelmien välinen liikenne

3.4.1 Transit-liikenne

Transit-sopimuksilla tarkoitetaan palvelujen tuottamista alemman tason operaattoreille. Palvelulla tarkoitetaan tässä tapauksessa pääsyä reititystauluun ja omien reittien mainostamista alaspäin reitityshierarkiassa, jonka kautta alemman tason operaattorille

avautuu pääsy jokaiseen ylemmän tason tuntemaan verkkoon. Transit-palvelua myyvä operaattori mainostaa Transit-sopimusten kautta opittuja verkkoja muualle Internetiin, jotta taataan mainostettavalle verkolle globaali tavoitettavuus. Transit-verkko toimii muille verkoille siirtoverkkona.

3.4.2 Peering-liikenne

Peering-sopimuksilla tarkoitetaan reittitietojen vaihtamista kahden eri operaattorin välillä. Peering-sopimuksissa mainostetaan vain omia verkkoja eikä Transit- tai muiden peering-sopimusten kautta opittuja verkkoja. Peering-sopimuksia tehdään saman tason operaattoreiden kesken, joiden avulla päästään käsiksi suurempaan määrään reittejä, joihin muuten pääsisi vain Transit-yhteyden kautta. Peering-sopimuksien avulla voidaan vähentää maksullista Transit-liikenteen määrää. Peering-sopimukset ovat käytännössä ilmaisia jos, osapuolet vaihtavat keskimäärin arviolta saman verran dataa yhteyden ylitse. [23, luku 3] Peering-suhteiden kautta saadut suorat reitit voivat myös vähentää verkkoviivettä verkkojen välillä ja opittujen verkkojen avulla voidaan myös mahdollisesti jakaa liikennettä useampien verkkojen kesken. [24.]

Peeringiä on kahta eri tyyppiä: yksityistä sekä julkista. Yksityinen peering on kahdenkeskistä reititystietojen vaihtamista, joka järjestetään suorina yhteyksinä eri operaattoreiden välille. Kahdenkeskisessä reititystietojen vaihdossa muut osapuolet eivät vie liikenteeltä kaistaa, mutta huonona puolena on kallis hinta, jos halutaan solmia vastaavia sopimuksia useamman osapuolen välille. Yksityisissä Peering-sopimuksissa molemmat osapuolet vastaavat kuluista ja yhteyden ylläpidosta. [17, luku 3.3.2.]

Julkinen peering mahdollistaa sopimusten solmimisen useamman operaattorin välillä yhden linkin kautta. Se tapahtuu yhdysliikennepisteen (Internet Exchange, IX) kautta. IX toimii paikkana, johon useat eri operaattorit ovat yhteydessä saman median, kuten Ethernetin kautta. Yhdysliikennepisteen hyvänä puolena on usean operaattorin reititystietojen saatavuuden parantuminen, kun taas huonona puolena on jaettu resurssien käyttö muiden osapuolten kesken. Asiakkaat liittyvät yleensä kahteen yhdysliikennepisteen kytkimistä, jotta toinen voi toimia varalla toisen mennessä epäkuntoon. Yhdysliikennepisteet ovat operaattoreiden tai useiden organisaatioiden ylläpitämiä solmupisteitä, joiden tarkoitus on edistää Internetin reititystietojen tehokkaampaa vaihtamista.

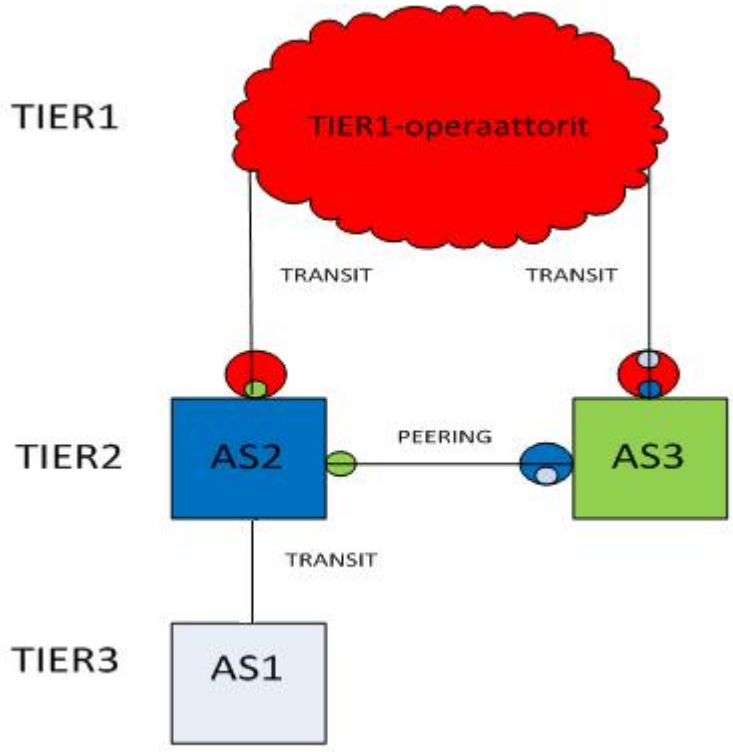
Suomessa palvelua tarjoaa FICIX, jonka kolme yhdysliikennepisteen kytkintä sijaitsee Espoossa, Helsingissä ja Oulussa. [24.]

3.5 Reititystietojen jakaminen Internetissä

Internetin reititys on järjestäytynyt hierarkisesti, ja se on jaoteltu karkeasti kolmeen eri tasoon. Ylimpänä toimivat Tier1-operaattorit pääsevät käsiksi globaaliin reititystauluun, jonka kautta ne tietävät reitit kaikkialle Internetiin. Tier1-operaattorit ovat yhteydessä muihin Tier1-operaattoreihin Peering-sopimusten kautta. Tier1-operaattorit myyvät pääsyä omaan reititystauluunsa Tier2-operaattoreille. Tier2-operaattorit voivat solmivat keskenään Peering-sopimuksia ja tarjoavat Tier3-operaattoreille pääsyä reititystauluihinsa. Alimman tason operaattorit omistavat vain tyypillisesti omat verkkonsa, joita he mainostavat BGP:llä ylemmän tason järjestelmille. Alimman tason operaattori pääsee käsiksi muun Internetin reititystauluun toisen tason verkkojen kautta, joilta tämä palvelu ostetaan. [17, luku 3.2.2; 2, luku 1.1.1.]

Internet-liikenteen hierarkia muodostuu eri tason operaattoreiden Transit-sopimusten kautta. Liikenne kulkee ylöspäin Transit-linkkien kautta, kunnes pääsee Tier1-operaattoreiden verkkoihin tai kunnes löytää vaihtoehtoisen reitin Peering-suhteiden kautta. Liikenteen on aina kuljettava yhden Peering-suhteen kautta, jonka jälkeen verkossa palataan alaspäin Transit-linkkejä pitkin.

Internet toimii ns. bottom-up-mallin mukaisesti. Ylemmällä tasolla oleva operaattori tietää suuremman määrän reittejä, sillä reittitiedot aggregoituvat ylöspäin (Transit) mentäessä, joka tarkoittaa reititystietojen keräämistä aina alemmilta tasoilta. Runkoverkko muodostuukin pääosin ylimmän tason operaattoreista, sillä niiden kautta on mahdollista päästä suureen osaan Internetin verkoista. Tämän takia lähtevä liikenne kanavoituu joissakin pisteissä, mutta palaa taas vähemmän käytettyjä reittejä pitkin kohteeseen.



Kuva 2. Peering- ja Transit-suhteet.

Kuvassa 2 näkyy eri järjestelmien väliset suhteet sekä myös karkea jako eri verkon tasoihin. AS2 mainostaa aliverkkoaan, AS1, naapurilleen AS3:lle Peering-suhteen kautta. Reittimainostuksia kuvataan ympyröillä ja värit kertovat, mistä verkkoja viesti sisältää. AS3 saa reitin Tier1-operaattorin siirtoverkon kautta AS1:n verkkoihin, sillä ylimmän tason operaattoreilla on tieto jokaisesta Internetin reitistä, myös AS1:stä. AS2 ja AS3 mainostavat keskenään vain omistamiaan verkkoja, jonka seurauksena kummatkin oppivat toistensa verkot ja pääsevät liikennöimään niihin kulkematta ylemmän tason operaattorin kautta.

4 BGP

BGP on autonomisten järjestelmien välillä toimiva ulkoinen reititysprotokolla, jonka uusin versio on BGP-4. BGP:n laajennus, MBGP (Multiprotocol BGP), on tuonut tuen IPv6-osoitteille sekä mahdollisuuden monilähetykseen (Multicast) käyttäen IPv4- tai IPv6-protokollaa. Laajennus on mahdollistanut BGP:n käytön MPLS (Multi Protocol Label Switching) VPN (Virtual Private Network) -tunneleissa, joissa BGP:tä käytetään välittämään VPN-tunnelikohtaisia reititystauluja verkon ylitse kohdereititimille. BGPv4 tukee myös CIDR-merkintää, joka mahdollistaa verkkojen summaamisen.

BGP on polkuvektoriprotokolla, eikä se ylläpidä tietoa verkon tarkasta topologiasta. BGP käyttää parhaan polun määrittämiseen läpi kulkemiensa AS-numeroiden listaa, AS-polkua (AS-path). AS-polku koostuu jokaisesta autonomisen järjestelmän numerosta, jonka läpi reititysviesti on kulkenut. BGP näkee AS:n yhtenä kokonaisuutena, sisälsi se sitten tuhansia tai vain muutamia reitittimiä. BGP hahmottaa suuria kokonaisuuksia, siksi se kykeneekin toimimaan Internetin reitity. [25, luku 1 ja 3; 26, luku 1.]

BGP:n käyttämä Adminisrative Distance (AD) riippuu siitä, onko reitti opittu eBGP- vai iBGP-naapurilta. Eri reititysprotokollien kesken ei voida arvioida reitin preferenssiä käyttäen reititysprotokollien omia metriikoita. Cisco käyttää AD-arvoa reititysprotokollien reittien priorisoinnissa. Alhaisin AD-arvo ratkaisee reititystauluun asennettavan reitin, jos samaan verkkoon on usean eri protokollan kautta opittu reitti. BGP käyttää eBGP-reiteille AD-arvoa 20, iBGP-reiteille 200 ja reitittimen lokaaleille reiteille 20. Reititysprotokollan AD-arvoa voi muuttaa, mutta se ei ole suositeltavaa. [27, s.752.]

BGP käyttää TCP-porttia 179 muodostaessaan tiedonsiirtoväylän kahden BGP-puhujan välille. TCP on yhteydellinen protokolla, eli se varmistaa pakettien perille pääsyn. TCP tarkistaa myös pakettivirheet ja pyytää lähettämään uudelleen virheelliset paketit. TCP:n käyttö mahdollistaa sen, että BGP-protokollan ei tarvitse itse huolehtia viestin lähettämiseen ja vastaanottamiseen liittyvistä asioista, vaan se saa ne palveluna TCP:ltä. BGP-yhteys muodostetaan aina kahden osapuolen välille kolmitiekättelynä. Siinä osapuolet vaihtavat ACK- ja SYN-paketteja muodostaakseen yhteyden välilleen. Osapuolten lähetykset ovat yksilähetyksiä (Unicast). [25, luku 3; 3, s.93.]

Marker	Length	Type	Message contents
16 bytes	2 bytes	1 byte	0 - 4077 bytes

Kuva 3. BGP-viestin otsakekenttä

BGP-yhteydessä esiintyy viittä erityyppistä viestiä, jotka ovat Open, Keepalive, Update, Notification ja ROUTE-REFRESH. Niitä käytetään välittämään tietoa yhteyden eri vaiheista. Jokainen viesti koostuu viestin otsakekentästä, jonka Type-kentän arvo kertoo, mistä viestistä on kyse:

1 - OPEN
2 - UPDATE
3 - NOTIFICATION
4 - KEEPALIVE
5 - ROUTER-REFRESH

Marker-kentän kaikki bitit ovat aina 1, ja Length-kenttä kertoo koko viestin yhteispituuden.

OPEN

TCP-yhteyden avaamisen jälkeen naapurit lähettävät Open-viestit, joiden avulla BGP-naapurit voivat neuvotella yhteyden parametreista. Open-viestin jälkeen naapurit vaihtavat reititystaulujensa tiedot.

Version	My AS	Hold time	Identifier	Par len	Optional parameters
1 byte	2 bytes	2 bytes	4 bytes	1 byte	0 - 255 bytes

Kuva 4. OPEN-viesti.

Versiokenttä (Version) kertoo viestin lähettäjän käyttämän BGP:n versionumeron, mahdollisia arvoja ovat 2,3 tai 4. Version neuvottelu aloitetaan uusimmasta vanhimpaan niin, että versionumeroa tiputetaan aina yhdellä, jos vastaanottaja hylkää alkuperäisen ehdotuksen.

AS-numerokenttä (My Autonomous System) kertoo nimensä mukaisesti lähettäjän AS-numeron. Kenttää käytetään mm. määrittämään, onko kyseessä iBGP- vai eBGP-sessio.

Odotusaikakenttä (Hold time) kertoo, kuinka kauan reititin odottaa Keepalive- tai Update-viestiä. Odotusajan mennessä umpeen reititin poistaa naapurin session ja naapurilta saadut reitit. Odotusaika voi olla 0, jolloin Keepalive-viestejä ei tavitse lähettää. BGP-naapurit vertaavat Open-viestin odotusaikakentän arvoja ja valitsevat käyttöönsä lyhyimmän ajastimen arvon.

BGP-Identiteettikenttä (BGP Identifier) toimii viestin lähettäjän tunnisteena.

Optional Parameters -kenttää käytetään mainostamaan BGP:n tukemia laajennuksia, kuten autentikointia ja useamman protokollan tukea. Optional Parameters Length -kenttä kertoo laajennuksien käyttämän pituuden Open-viestissä.

KEEPALIVE

Keepalive-viestejä lähetetään naapureiden kesken BGP-yhteyden ylläpitoon. Niiden pääasiallisena tehtävänä on pitää yllä tietoa siitä, onko naapuri vielä saavutettavissa. Keepalive-viestien vastaanotto käynnistää Holdtime-laskurin. Keepalive-viestillä myös hyväksytään naapurin Open-viestissä tulleet ehdotukset. Keepalive-viesti koostuu vain viestin otsakekentästä. [25, luku 4; 3, s.93.]

UPDATE

Update-viestit sisältävät tietoa reiteistä, niiden poisviennistä tai molemmista samanaikaisesti.

UR length	Withdrawn routes	PA length	Path attributes	NLRI
2 bytes	Variable	2 bytes	Variable	Variable

Kuva 5. BGP Update-viesti.

Withdrawn Routes Length -kenttä kertoo Withdrawn Routes -kentän koko pituuden. Jos arvo on 0, niin yhtään reittiä ei vedetä pois, joka tarkoittaa, että Withdrawn Routes -kenttää ei käytetä viestissä.

Withdrawn Routes -kenttä sisältää listan poisvedettävistä prefikseistä. Jokainen listan prefiksi koostuu Length-kentästä, joka kertoo bitteinä prefiksin pituuden ja Prefix-kentästä, joka sisältää itse prefiksin.

Path Attributes -kentässä on reittiin liittyviä ominaisuuksia, joita BGP voi käyttää esimerkiksi parhaan polun etsimiseen. Total Path Attribute Lenght -kenttä kertoo Path Attributes -kentän koko pituuden.

NLRI-kenttä sisältää listan mainostettavista prefikseistä. NLRI-kentässä voi olla useampia mainostettavia verkkoja, mutta Update-viesti kuvaa vain yhden BGP-reitin, sillä Path Attribute -kentän arvot kuvaavat vain yhden reitin ominaisuuksia. Viesti voi siis sisältää useampia verkkoja, jos ne käyttävät samaa BGP-reittiä, jonka polun ominaisuudet ovat samat.

NOTIFICATION

Notification-viestejä käytetään, kun BGP havaitsee virheitä yhteydessä tai sen parametreissa. Yhteys suljetaan heti Notification-viestin lähettämisen jälkeen. Notification-viesti koostuu Error code-, Error subcode- ja Data -kentistä.

Error code -kenttä kertoo virheen luokan karkeasti ja sillä on kuusi eri mahdollista arvoa. Error subcode -kenttä kuvailee tarkemmin virheen tyypin ja antaa lisätietoa ongelmasta. Data-kenttä sisältää virheeseen liittyvää informaatiota. [25, luku 4.]

ROUTE-REFRESH

BGP-naapurilta voidaan pyytää Route-refresh-viestillä reitityspäivitysten uudelleenlähetystä esimerkiksi tilanteessa, jossa BGP-politiikka on muuttunut ja naapurilta tarvitaan kaikki reitit uudelleentarkastelua varten. Naapurit neuvottelevat Route-refresh-

ominaisuuden käytöstä BGP-yhteyttä muodostaessa. Kummankin naapurin tulee tukea ominaisuutta, jotta sitä voidaan käyttää. [28.]

Polun attribuutit jaetaan neljään kategoriaan.

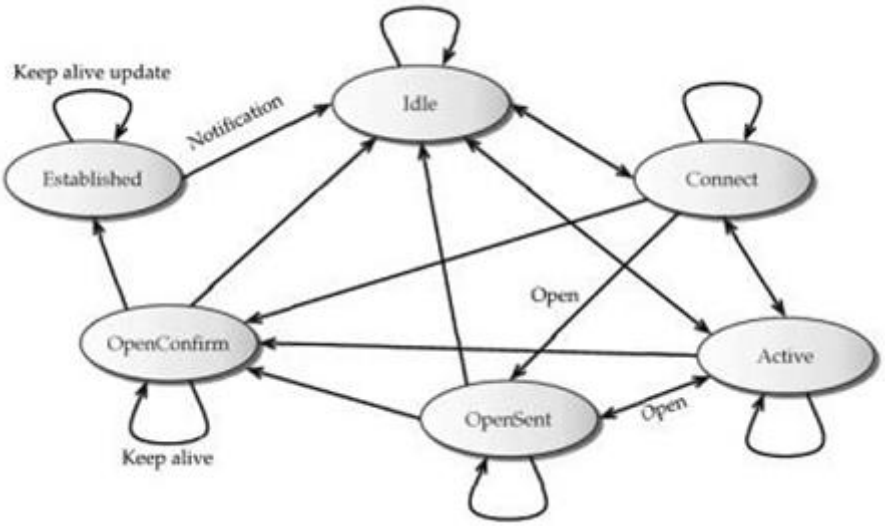
1. Well-known mandatory.
2. Well-known discretionary.
3. Optional transitive.
4. Optional non-transitive.

Jokaisen BGP-implementaation tulee tunnistaa tunnetut polun attribuutit (Well-known). Tunnetut attribuutit voivat olla pakollisia (mandatory), joka tarkoittaa niiden pakollista läsnäoloa UPDATE-viestissä tai valinnaisia (discretionary). Valinnaisten attribuuttien ei tarvitse olla UPDATE-viestissä mukana, mutta ne voivat olla.

UPDATE-viestissä voi olla tunnettujen lisäksi myös vaihtoehtoisia (Optional) attribuutteja, jotka eivät välttämättä esiinny eri valmistajien BGP-implementaatioissa. Kaikkia vaihtoehtoisia attribuutteja ei siis tunnisteta eri implementaatioiden välillä. Transitive-attribuutit tulee lähettää eteenpäin BGP-naapureille, vaikka BGP ei sitä tunnistaisikaan. Tuntematon non-transitive-attribuutit tiputetaan lähettämättä sitä eteenpäin. Mikä tahansa BGP-laite reitin matkalla voi lisätä polkuun uusia transitive-attribuutteja, mutta niiden päivittäminen ei ole pakollista. [25, luku 5.]

4.1 BGP-yhteyden muodostaminen

BGP-naapurit aloittavat yhteyden muodostamisen vaihtamalla Open-viestejä. Yhteyden muodostus käy tietyt tilat ennen kuin yhteys on lopullisesti muodostettu. Tilat kertovat, kuinka toimia ja mikä on seuraava operatiivinen tila, kun naapurin kanssa on vaihdettu viestejä.



Kuva 6. Yhteyden muodostamisen tilat BGP-protokollalla. [29, s.267]

Jokainen yhteys alkaa Idle-tilasta, jolloin BGP-noodi ei ole vielä valmis hyväksymään BGP-yhteyttä. Automaattiset tai manuaaliset tapahtumat käynnistävät session resurssien alustamisen, johon liittyy session aloittaminen vastapuolen kanssa ja sisään tulevien BGP-yhteyksien kuunteleminen. Tämän jälkeen yhteys on valmis siirtymään Connect-tilaan. Idle-tilaan voidaan palata jokaisesta muusta tilasta suoraan, esim. virheellisen tiedon takia.

Connect-tilassa BGP odottaa yhteyden muodostamista. Onnistuneen yhteyden muodostuessa BGP lähettää naapurilleen Open-viestin ja muuttaa tilakseen OpenSent. Jos TCP-yhteyden avauspyyntö on virheellinen, niin tila pysyy ennallaan. Jos avauspyyntö on hyväksytty eikä yhteys muuten muodostu, niin silloin BGP-yhteys menee Active-tilaan. Lisäksi on mahdollista keskeyttää yhteys manuaalisesti tai yhteys voi keskeytyä virheiden takia, jolloin BGP-yhteys palautuu Idle-tilaan. Connect- tilasta on myös mahdollista siirtyä suoraan OpenConfirm-tilaan, jos noodi vastaanottaa Open-viestin. Open-viestiin vastataan lähettämällä naapurille Keepalive–viesti, ja Open-viesti jos naapurille ei olla sitä vielä lähetetty.

Active-tilassa BGP odottaa TCP-yhteyden muodostumista. Active-tila koittaa aktiivisesti muodostaa yhteyttä uudelleen BGP-naapuriin. Active-tilaan ajaudutaan, jos BGP-yhteyden avaamisessa ilmenee ongelmia.

OpenSent-tilassa naapurille lähetetään Open-viesti, jonka jälkeen OpenConfirm-tilassa naapurilta odotetaan saavan Keepalive-viesti ja naapurille myös lähetetään Keepalive-viesti, joka vahvistaa yhteyden avatuksi ja jonka jälkeen yhteys etenee seuraavaan tilaan. Connect-, Active- ja OpenSent–tiloista on mahdollista siirtyä suoraan OpenConfirm-tilaan, kun noodi vastaanottaa Open-viestin.

Established-tilassa yhteys on saatu muodostettua, jonka jälkeen naapurit vaihtavat reititystaulut niiltä osin, joita naapurille mainostetaan. Tämän jälkeen reititystauluja päivitetään vain muutoksien yhteydessä käyttämällä Update-viestejä. Keepalive-viestit pitävät yhteyttä yllä ja jos niitä ei saada Holdtime-laskurin määrittelemänä aikana, niin yhteys nollataan. [29, s.266-272.]

4.2 BGP-Attribuutit

Jokaiseen BGP-reititystaulusta löytyvään verkkoprefiksiin liittyy myös joukko ominaisuuksia, joita voidaan käyttää reittien suodattamisessa reitityspolitiikan sanelemien sääntöjen mukaan. BGP:n reititys perustuu ISP-tasolla politiikoihin, joidenka mukaan tietyt reitit hyväksytään tai hylätään. Seuraavassa on listaus BGP-protokollan tukemista ominaisuuksissa Ciscon implementaatiossa. [30 s.16.]

4.2.1 AS-Path

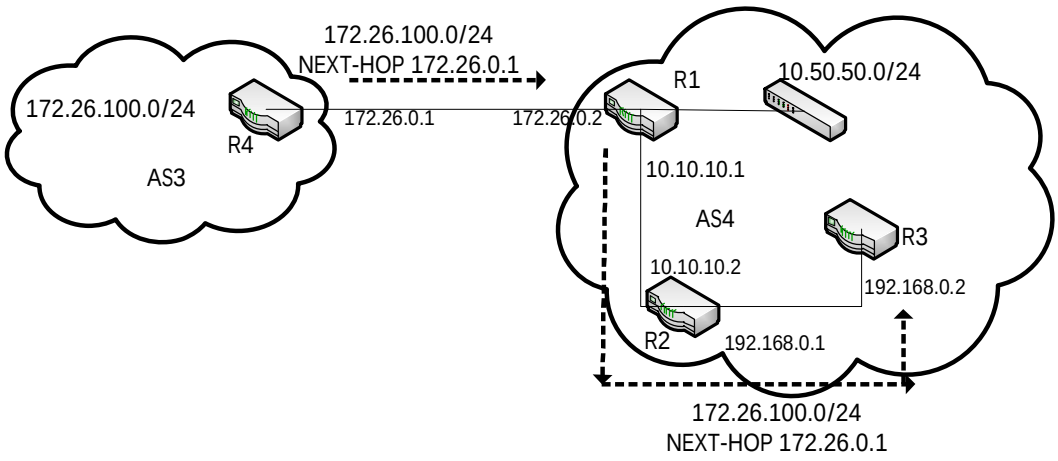
AS_PATH on BGP-reittien mukana kulkeva lista kaikista autonomisista järjestelmistä, joiden läpi reitti on kulkenut, eli AS-polku. Listan ensimmäisenä arvona on lähimmän naapurin AS-numero. Viimeisenä arvona on reitin omistavan järjestelmän AS-numero, eli järjestelmän, joka on syöttänyt reitin BGP-järjestelmään. BGP:n käyttämä mekanismi reitityssilmukoiden havaitsemiseen perustuu AS-polkuun. Reitityssilmukka havaitaan, jos reititin näkee oman AS-numeronsa listassa, jolloin reitti pudotetaan. Tämän lisäksi AS-polku mahdollistaa reittien suodattamisen listassa esiintyvien AS-numeroiden perusteella. AS-polku on myös yksi parhaimman reitin valintaperusteista ja se myös yleensä ratkaisee parhaimman reitin, jos muut reitille annetut arvot ovat muokkaamattomia. Lisäksi on myös mahdollista, että jokin AS lisää oman AS-numeronsa useamman kerran listaan, jonka tarkoituksena on pyrkiä vaikuttamaan reitityspäätöksiin muissa järjestelmissä tekemällä reitistä vähemmän haluttavamman. [29, s.251-252.]

4.2.2 Origin

Origin kertoo verkkoprefiksin alkuperän eli kuinka se on tullut BGP-reititystauluun. Mahdollisia arvoja ovat 0, joka tarkoittaa BGP-prosessin itse injektoimaa verkkoa reititystauluun esimerkiksi network-komennolla, jolloin verkon alkuperä on IGP. Muista reititysprosesseista BGP-prosessiin jaetut reitit saavat merkinnäksi INCOMPLETE, jonka arvo on 3. Kolmas mahdollinen reitin alkuperä on EGP, joka saa arvon 2. BGP suosii alkuperän arvon mukaan reittejä pienimmästä suurimpaan. [29, s.251-252.]

4.2.3 Next-Hop

Next-Hop kertoo reitin seuraavan hypyn reitittimen IP-osoitteen, jonka kautta on pääsy Update-viestissä mainostettuun kohdeverkkoon. BGP käsittelee seuraavan hypyn osoitetta hieman eri tavalla riippuen, mistä reittimainostus lähetetään ja onko verkko AS:n sisäinen vai ulkoinen. [29, s251-252.]



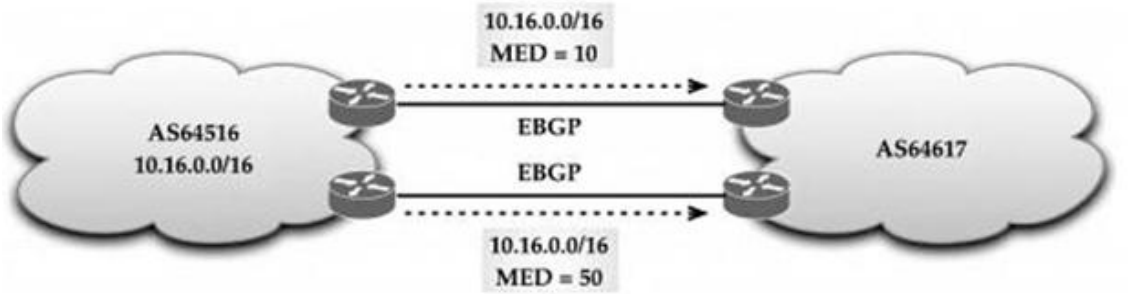
Kuva 7. Seuraavan hypyn käyttö BGP:ssä.

Kuvassa 7 on esimerkki siitä, kuinka Next-Hop toimii. R4 mainostaa UPDATE-viestillä verkkoa 172.26.100.0/24 eBGP-yhteyden yli naapurilleen R1:lle, joka lähettää viestin eteenpäin iBGP-yhteyden yli aina R3:lle saakka. Next-Hop-arvo säilyy myös AS:n sisällä kun viesti lähetetään iBGP-naapureille. Arvona toimii naapuri-AS:n reittiä mainostaneen reitittimen IP-osoite, eli tässä tapauksessa R4:n IP-osoite.

Toinen skenaario BGP:n tavasta käsitellä seuraavan hypyn osoitetta on, jos R1 mainostaisi connected-verkkoa 10.50.50.0/24 R3:lle iBGP-yhteyden yli. Update-viestissä oleva seuraavan hypyn IP-osoite olisi 10.10.10.1, eikä 192.168.0.1, kun se saapuu R3:lle. Seuraavan hypyn osoitetta voidaan ajatella pointterina kohdeverkkoon ja pointterin osoitteeseen reitin voi kertoa esimerkiksi sisäinen reititysprotokolla.

4.2.4 MED

Multi_Exit_Disc–attribuuttia (MED) käytetään välittämään tieto naapuri-AS:lle siitä, mitä linkkiä suositellaan käytettävän järjestelmien väliseen liikenteeseen. MED-attribuutin käytön hyödyt tulevat kun naapurijärjestelmien välillä on useampi liityntäpiste ja halutaan suosia tiettyä linkkiä muiden ylitse valitulle liikenteelle. MED-arvo lähetetään iBGP-naapureille, mutta ei toisen AS:n BGP-reunareitittimelle. Prioriteetiltaan suurempi reitti on se, jolla on pienempi MED-arvo. [30, s.16-21.]



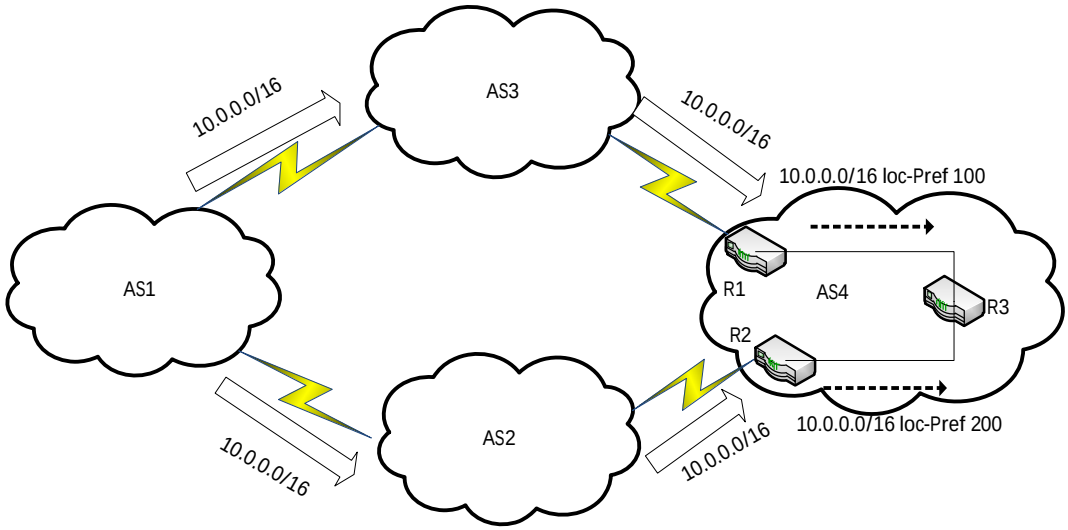
Kuva 8. MED-attribuutti. [29, s.253]

Kuvassa 8 on AS64516 lähettää AS64617:lle tiedon verkosta 10.16.0.0/16 kahta eri linkkiä pitkin eri MED-arvoilla. AS64617 suosii 10.16.0.0/16-verkkoon mentäessä kuvassa ylempänä olevaa linkkiä, jota mainostettiin MED-arvolla 10. Normaalisti MED-arvo on vain verrattavissa reitille, joka tulee saman naapuri-AS:n kautta, mutta Ciscon implementaatiossa on myös mahdollista ottaa huomioon eri AS:ien kautta tulleet MED-arvot parasta reittiä valittaessa. Se tapahtuu komennolla `bgp always-compare-med`.

4.2.5 Local-Pref

LOCAL-PREF-attribuuttilla voidaan priorisoida uloslähteviä reittejä AS:n sisällä iBGP-reitittimien välillä. Sitä ei mainosteta muille AS:lle, vaan se on puhtaasti AS:n sisäisen reititysvalintaan liittyvä ominaisuus. Se voidaan määrittää esimerkiksi kun reittejä ote-

taan vastaan naapurilta ja sen avulla voidaan tehdä karkean tason kuormanjakoa useamman linkin kautta. Prioriteetilta suurempi reitti on se, jolla on suurempi Local-Pref-arvo. [30, s.16-21.]



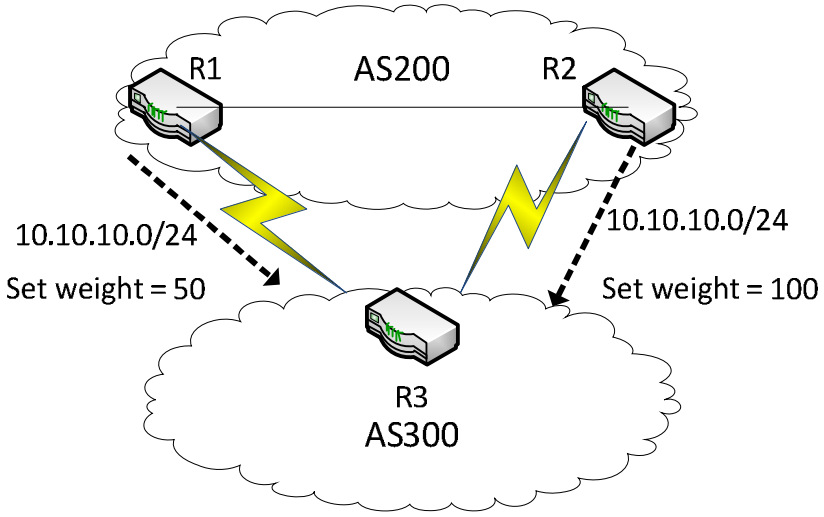
Kuva 9. Local-Pref-arvo.

Kuvassa 9 AS1 mainostaa reittiä 10.0.0.0/16 kahta eri polkua pitkin. AS4:n sisällä reititin R2 muokkaa verkkoon 10.0.0.0/16 liittyvää Lolcal-Pref-ominaisuutta ja muuttaa sen arvoksi 200. R1 ottaa saman reitin vastaan ja lähettää sen muille AS4:n BGP-reitittimille arvolla 100, joka on oletusarvo. AS4:n sisällä reitittimet vertaavat reittiin liittyvää Local-Pref-arvoa ja valitsevat verkkoon 10.0.0.0/16 mentäessä R2:n kautta kulkevan reitin.

4.2.6 Weight

Ciscon implementaatiossa on käytössä myös Weight-ominaisuus, jota paikallinen reititin käyttää valitessaan parasta reittiä. Weight-ominaisuutta käytetään, kun reitittimellä on useampi reitti samaan kohdeverkkoon. Weight-arvoa ei välitetä muille BGP-reitittimille. Prioriteetilta korkein reitti on se, jolla on korkein Weight-arvo.

Kuvassa 10 reititin R3 saa reititysmainokset kahdelta eri AS200:n reitittimeltä koskien verkkoa 10.10.10.0/24 ja asettaa Weight-arvoksi 50 reitittimeltä R1 tulleelle polulle ja vastaavasti reitittimen R2 polun Weight-arvoksi 100. AS300:n reititin R3 suosii tässä tapauksessa reitittimen R2 kautta kulkevaa reittiä. [30, s.16-21.]



Kuva 10. Weight-ominaisuus.

4.2.7 Community

Community on 32-bittinen arvo, eikä se vaikuta suoraan reittien valintaan, vaan sitä voidaan käyttää esimerkiksi reittien merkkaamiseen ja sen pohjalta reitityspäätöksien tekemiseen erilaisten filttereiden kautta. Community-arvo voi olla privaatti tai tunnettu. Ciscon implementaatiossa on käytössä neljä tunnettua community-arvoa.

NO_EXPORT kertoo, että näitä prefiksejä ei tule mainostaa eBGP:n kautta muille järjestelmille, mutta järjestelmän sisällä muille konfederaation alaisille järjestelmille mainostaminen on sallittua.

LOCAL_AS määrittelee, että reittejä ei mainosteta AS:n ulkopuolelle ja vain konfederaation sisällä olevat BGP-naapurit voivat ottaa näitä reittejä vastaan.

NO_ADVERTISE kieltää reitin mainostamista sisäisille tai ulkoisille BGP-naapureille. Reittiä ei mainosteta kenellekään.

INTERNET ei aseta mitään rajoituksia reitille, vaan sitä voidaan mainostaa aivan kenelle tahansa.

Privaattien community-arvojen käyttö on huomattavasti yleisempää. Community-arvot merkintään <ASN:ARVO>, jossa kohtaan ASN tulee AS-numero ja kohtaan ARVO tulee community-arvoa käyttävälle AS:lle jokin merkityksellinen arvo, jota voidaan käyttää esimerkiksi reittien suodattamiseen tiettyihin community-arvoihin perustuen. Tämä käyttäjäystävällisempi merkkaustapa saadaan käyttöön Ciscon laitteissa komennolla ip bgp-community new-format. [30, s.16-21.]

4.2.8 Cluster_list

CLUSTER_LIST-arvoa käytetään reitityssilmukoiden ehkäisyyn reittiheijastimia (Route Reflector, RR) käyttävässä ympäristössä. Tähän arvoon on tallennettuna jokaisen reitittimen CLUSTER_ID, jonka läpi prefiksi on kulkenut. Jos reititin näkee oman CLUTER_ID:nsä, niin reitti on tehnyt silmukan ja se pudotetaan. [30, s.16-21.]

4.3 BGP:n reititystaulut

Reititystietoja säilytetään kolmessa eri BGP:n käyttämässä reititystaulussa (Routing Information Base, RIB), jotka ovat myös tärkeässä osassa valittaessa parhaita reittejä.

Adj-RIBs-In-reititystaulu sisältää tiedon reiteistä, joita naapuri on mainostanut paikalliselle reitittimelle. Jokaista BGP-naapuria varten on oma Adj-RIBs-In-reititystaulu, joka sisältää prosessoimatonta tietoa jokaisesta naapurin mainostamasta reitistä. Adj-RIBs-Out-reititystaulu sisältää reitit, joita paikallinen reititin mainostaa naapureilleen. Tässä reititystaulussa on vain tiedot niistä reiteistä, joita paikallinen reititin on päättänyt mainostaa naapureilleen UPDATE-viestejä käyttäen.

Loc-RIB-reititystalu on BGP-prosessin käyttämä pääreititystaulu, BGP-reititystaulu, ja se sisältää kaikki reitit, joita paikallinen reititin voi käyttää datan reitittämiseen. Reitit on valittu sinne Adj-RIBs-In-reititystaulusta ajamalla sen sisältämät reitit paikallisen reitittimen reitityspolitiikan määrittelemien suodattimien läpi. Se ei ole sama asia kuin reitittimen käyttämä reititystaulu. [31, luku 3.1, 3.2 ja 9.]

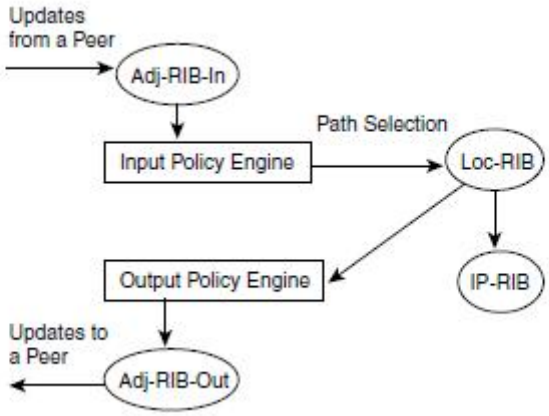
```
Router# show ip bgp

BGP table version is 5, local router ID is 10.0.33.34
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network    Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0    0.0.0.0                  0         32768 ?
*  2.0.0.0    10.0.33.35              10             0 35 ?
*>            0.0.0.0                  0         32768 ?
*  10.0.0.0   10.0.33.35              10             0 35 ?
*>            0.0.0.0                  0         32768 ?
*> 192.168.0.0/16 10.0.33.35          10             0 35 ?
```

Edellä on esimerkki Ciscon reitittimen BGP-reititystaulun tulosteesta. *Network* kertoo, mistä prefiksistä on kyse ja *Next Hop* ilmaisee seuraavan hypyn IP-osoitteen. Jos seuraavan hypyn osoite on 0.0.0.0, niin tämä tarkoittaa sitä, että reititin tietää kyseiseen verkkoon reitin myös jotain muutakin kautta kuin BGP:n avulla. Yleensä tämä tarkoittaa suoraan reitittimeen liitettyä verkkoa, Connected-reittiä. *Path* kertoo AS-polun ja sisältää listan lopussa tiedon reitin alkuperästä, joka on joko IGP, EGP tai Incomplete. [32.]

4.4 Reittien valinta

BGP tarkastaa UPDATE-viestissä olevat uudet reitit ja ajaa ne suodattimien läpi. Reitti tiputetaan, jos se ei läpäise filttereitä. Reitit sijoitetaan ensin Adj-RIB-In-reititystauluun, jossa reitit käyvät prosessin läpi, jonka tarkoituksena on löytää paras reitti useamman vaihtoehdon väliltä. Paras reitti asennetaan BGP-reititystauluun, vanha reitti poistetaan ja siitä ilmoitetaan myös naapureille, joille on aikaisemmin mainostettu kyseistä verkkoa. BGP-reititystaulu päivittää reititystiedot reitittimen IP-reititystauluun.

Jokainen BGP-reititystaulun reitti käy reitityspolitiikoiden määrittelemien filttereiden läpi, jonka seurauksena valitut reitit tallennetaan Adj-RIB-Out-reititystauluun, josta niitä mainostetaan BGP-naapurille. Reititin jakaa tiedon uudesta reitistä jokaiselle iBGP-naapurille, paitsi jos naapurilta on jo saatu aikaisemmin tieto samasta verkosta.



Kuva 11. Reititystietojen käsittely. [30, s.8]

Adj-RIB-In-taulussa voi olla useampia reittejä samaan kohdeverkkoon. Paras reitti valitaan vertailemalla reittien kesken niille määritettyjä attribuutteja. Reitin tulee kuitenkin täyttää tietyt määritelmät ennen kuin sitä voidaan pitää ehdokkaana:

- Next_Hop-attribuutin määrittelemä IP-osoite on oltava saavutettavissa tai muuten reitti tiputetaan valintaprosessista.
- Polku ei ole synkronoitu ja synkronointi on käytössä.
- Sen tulee läpäistä reitittimen Input-politiikka.
- Reitti ei saa olla vaimennettu.

Ciscon implementaatiossa usean polun vertailu alkaa niin, että uusin polku asetetaan parhaaksi poluksi ja sitä verrataan seuraavaksi uusimpaan polkuun. Edellisestä vertailusta selvinnyttä parempaa polkua käytetään vertailussa kolmanteen polkuun ja tätä jatketaan niin kauan, kunnes viimeinenkin poluista on käynyt vertailun läpi. Cisco on määrittänyt seuraavat vertailukriteerit reitin valintaan. Listaa käydään ylhäältä alas, kunnes löydetään eroavaisuus reittien sisältämissä attribuuteissa.

1. Suositaan polkua, jolla on suurin Weight-arvo.
2. Suositaan polkua, jolla on suurin Local-Pref-arvo.
3. Suositaan polkua, joka on lokaalisti injektoitu BGP-reititystauluun, esim. network-komentoa käyttämällä.
4. Suositaan lyhyintä AS-polkua.
5. Reitin alkuperä (Origin), IGP>EGP>INCOMPLETE.
6. Suositaan polkua, jonka MED-arvo on alhaisin.

7. Suositaan ulkoista reittiä (eBGP) ennen sisäistä reittiä (iBGP).
8. Suositaan alhaisinta IGP:n määrittämää metriikkaa BGP:n käyttämään Next-Hop-osoitteeseen.
9. Asennetaan samanarvoiset reitit jos Multipath on käytössä.
10. Suositaan vanhinta eBGP-reittiä.
11. Suositaan alimman reititintunnisteen (Router ID) omaavan reitittimen reittiä
12. Suositaan lyhintä klusterilistan pituutta.
13. Suositaan reittejä, jotka tulevat alimmasta BGP-puhujan IP-osoitteesta.

BGP-reititin on konvergoitunut, kun se täyttää seuraavat ehdot:

- Kaikki mahdolliset reitit on hyväksytty.
- Kaikki mahdolliset reitit on asennettu reititystauluun.
- Jokaisen BGP-puhujan BGP-reititystaulun versionumeron tulee olla sama.
- BGP:n ulos- ja sisääntulojonot ovat tyhjiä.

[30, s.62, s.25-26; 33.]

4.5 Konvergenssin nopeuttaminen

BGP:n konvergenssia on mahdollista nopeuttaa optimoinnilla. Seuraavassa on esitetty muutamia keinoja konvergenssin nopeuttamiseen.

4.5.1 TCP-protokollan optimoiminen

BGP käyttää TCP:tä tietoliikennekanavan muodostamiseen ja sitä optimoimalla voidaan myös nopeuttaa BGP:n toimintaa. Suurimmat TCP:n toimintaan vaikuttavista parametreista ovat suurimman sallitun segmentin koko (Maximum Segment Size, MSS) ja TCP-ikkunan koko. MSS kontrolloi pakettien kokoa ja ikkuna sitä, kuinka nopeasti paketteja voidaan lähettää.

Ikkuna toimii yhteyden puskurina, sillä se määrittelee kuinka paljon kuittaamattomia paketteja voi olla jonossa. Ikkunan koko kertoo, kuinka paljon dataa voidaan vastaanottaa ennen kuin lähetetylle datalle pitää saada kuittaus (ACK). Kuittauksia käytetään varmistamaan datan perillemeno.

Reititin pitää paketteja jonossa, kunnes prosessorilta vapautuu aikaa niiden käsittelemiseen. Suuret määrät ACK-paketteja useilta eri BGP-naapureilta voivat aiheuttaa ruuhkaa jonossa ja täyttää sen, jolloin uudet paketit tiputetaan. BGP-viestit voivat olla kookkaita ja sen takia yksi BGP-viesti voi vaatia useiden pakettien lähettämistä, varsinkin kun suurimman sallitun segmentin koko on pieni. Suurimman sallitun segmentin kokoa nostamalla voidaan vähentää lähetettävien pakettien määrää suhteessa BGP-viestin kokoon, joka vastaavasti vähentää ACK-pakettien määrää jonoissa. Tämä myös nostaa datan ja pakettien otsakkeiden hyötysuhdetta. [30, s.63-69.]

4.5.2 Peer Groups

BGP-naapurit voidaan liittää ryhmiin ja määrittää BGP-konfiguraatiot ryhmälle, joka vastaavasti vähentää konfiguraation määrää, koska jokaista yksittäistä naapuria varten ei tarvitse luoda erillisiä BGP-konfiguraatioita. Samaan ryhmään voi liittää BGP-naapureita, joilla kaikilla on yhteinen reitityspolitiikka. Ryhmän jäseniä varten riittää, kun reititin luo yhden UPDATE-viestin ja lähettää sen jokaiselle ryhmän jäsenelle. Ilman ryhmää reititin joutuisi luomaan jokaista naapuria varten erikseen UPDATE-viestin.

Ilman ryhmää BGP käy jokaisen BGP-reititystaulun rivin läpi jokaista naapuria kohden. Jos BGP-reititystaulussa on 5000 prefiksiä ja naapureita 100, joutuu reititin käymään yhteensä 50 000 riviä läpi. Ryhmän kanssa BGP käy jokaisen reititystaulun rivin läpi jokaista ryhmää kohden. Jos kaikki 100 naapuria kuuluvat samaan ryhmään, joutuu reititin käymään vain 5000 riviä läpi. Ryhmien käyttö vähentää reitittimen prosessorin ja muistin kuormaa. [30, s.74-76.]

4.5.3 Update Packing & BGP Read-Only Mode

Ciscon IOS-versio 12.0(19)S toi parannuksen siihen, kuinka BGP käsittelee NLRI-informaatiota Update-viesteissä. Kaikki verkkoprefiksit (NLRI), joilla on samat polun attribuutit ja niiden kombinaatiot, voidaan pakata yhteen Update-viestiin. Tämä vähentää huomattavasti luotavien Update-viestin määrää.

Normaalisti BGP aloittaa parhaan polun valinnan heti, kun BGP-naapuri avaa yhteyden ja lähettää reittitiedot. Tämä tapahtuu jo ennen kuin kaikki mahdollinen tieto on saatu naapurilta. Seurauksena on se, että naapurilta saatuja reittejä saatetaan mainostaa muille naapureille, vaikka kaikkea reititystietoa ei vielä ole saatu ja paras reitti voi vielä muuttua. Tästä seuraa lukuisia ylimääräisiä päivitysviestejä naapureiden kesken, ja se myös syö päivitysten pakkaamisen tehoa, sillä ne eivät vielä sisällä täydellistä tietoa kaikista reiteistä.

Ratkaisuna ongelmaan on pitää BGP-reititin lukumoodissa, jossa se voi vain ottaa vastaan reittipäivityksiä naapureilta, mutta ei itse lähettää niitä. BGP-reititin palaa takaisin kirjoitusmoodiin, kun se on ottanut vastaan kaikki BGP-naapurin reititystiedot, jonka jälkeen se voi muodostaa täydellisen Update-viestin, joka sisältää kaiken tiedon pakatussa muodossa. Komento `bgp update-delay` *RO_Limit* määrittelee, kuinka kauan reititin pysyy lukutilassa. Reititin poistuu lukutilasta myös silloin kun se saa naapurilta Keepalive-viestin, joka lähetetään kun naapuri on saanut lähetettyä kaikki reititystietonsa. [30, s.81-82.]

4.5.4 BGP Fast External Fallover

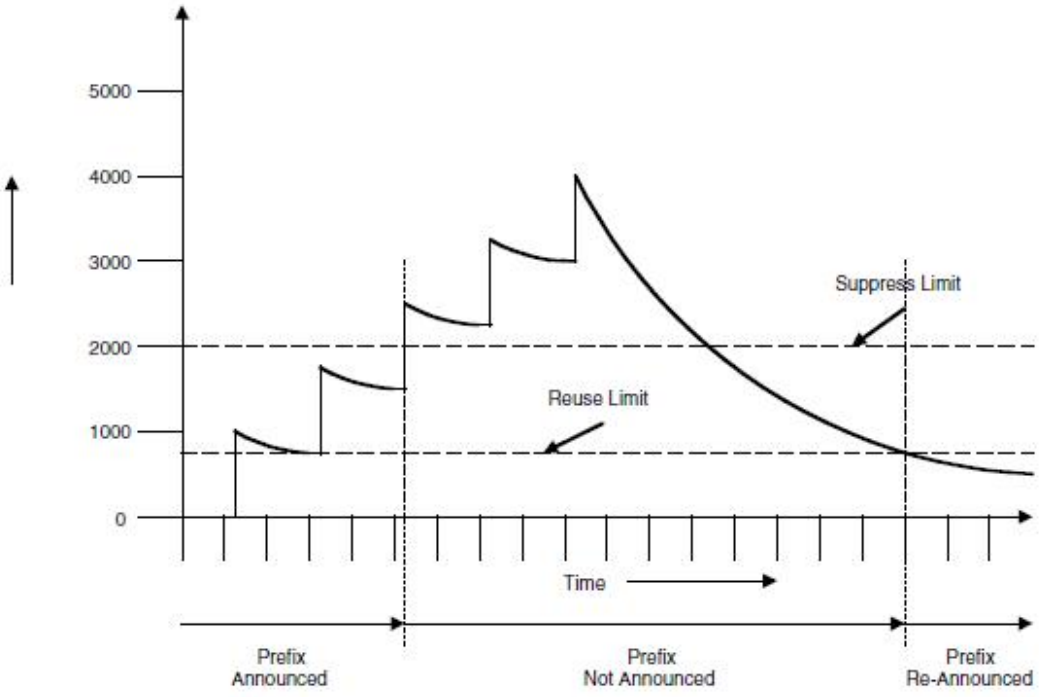
Normaalissa tilanteessa BGP purkaa yhteyden naapuriinsa, kun ei ole saanut Keepalive-viestiä Holdtimen määrittämänä aikana, joka on normaalisti 180sekuntia. Fast External Fallover -ominaisuus purkaa yhteyden heti, kun naapuriin on menetetty yhteys. Ominaisuus on oletusarvoisesti reitittimissä päällä, ja se määritetään globaalisti komennolla `bgp fast-external-fallover` tai porttikohtaisesti `ip bgp fast-external-fallover [permit | deny]`.

Ominaisuudesta voi olla haittaa, jos jokin linkki nousee ja sammuu koko ajan, josta aiheutuu vain se, että yhteys puretaan ja alustetaan koko ajan uudestaan. Tämä myös nopeuttaa reitin vaimennusta. Yhteyden purkamista voi myös nopeuttaa muuttamalla Holdtime-ajastinta pienemmäksi, jolloin yhteys puretaan, kun ajastimen asettama aika on kulunut loppuun. [30, s.83-84.]

4.5.5 Route Flap Dampening

Reitittimelle muodostuu ylimääräistä kuormaa reiteistä, jotka puretaan ja alustetaan hetken päästä uudestaan. Epästabiileista reiteistä seuraa turhaa reititystaulun tietojen päivittämistä ja se kuormittaa reitittimen prosessoria. Ciscon reitittimissä reittejä on mahdollista vaimentaa siksi aikaa, kunnes ne stabiloituvat.

Alas meneville reiteille annetaan rangaistus (penalty), joka on määritettävissä oleva kiinteä arvo, jonka reitti saa joka kerta, kun se menee alas. Oletusarvoisesti se on Ciscon kytkimissä 1000. Reitti vaimennetaan kun rangaistuksen arvo on ylittänyt määritetyn raja-arvon (suppres limit), vaimennusraja, joka on Ciscon kytkimissä oletusarvoisesti 2000. Reitin rangaistuksen määrä laskee ajan kuluessa, ja se voidaan palauttaa käyttöön kun se on alittanut asetetun raja-arvon, uudelleenkäytön rajan (reuse limit). Reittivaimennusta voi käyttää vain eBGP-reitteihin.



Kuva 12. Reitin vaimennus. [30, s.92]

Kuvassa 12 on havainnollistettu, kuinka reitin vaimennus toimii. Reitti on vaimennettu kolmannen epävakauden jälkeen, jolloin se ylitti vaimennusrajan. Reitti on jatkanut rangaistuksen keräämistä vielä vaimennuksenkin jälkeen kunnes lopulta stabilisoitunut.

Ajan kuluessa rangaistuksen määrä on tippunut ja alittanut udelleenkäytön rajan, jonka jälkeen se on voitu ottaa taas käyttöön.
Komennon syntaksi:

Router(config)#router bgp 100
Router(config-router)#bgp dampening *half-life reuse-limit suppress-limit maximum-suppress-time*

Half-life kertoo, missä ajassa yhden rangaistuksen asettama määrä pyyhitään pois. Oletuksena se on 15minuuttia. *Maximum-suppress-time* kertoo, kuinka kauan reitti voi olla maksimissaan vaimennettuna. Vaimennuksen pituus ei kasva tämän rajan yli, vaikka reitille määrättäisiin lisää rangaistuksia. Prefiksille määritetyn maksimirangaistuksen määrän voi laskea kaavalla:

$$\text{max-penalty} = \text{reuse-limit} * 2\left(\frac{\text{max-suppress-time}}{\text{half-life}}\right)$$

Parametreja määritellessä on otettava huomioon maksimirangaistuksen raja, sen on oltava suurempi kuin vaimennusrajan, jotta vaimennus astuu voimaan.

Router(config-router)#bgp dampening 30 750 3000 60

Kyseisistä parametreista seuraisi se, että maksimirangaistukseksi ja vaimennusrajaksi saadaan arvo 3000. Näillä parametreilla vaimennusrajan arvo ei ikinä ylittyisi, ja reitti saisi jatkaa toimintaansa epävakaana. [30, s.91-94.]

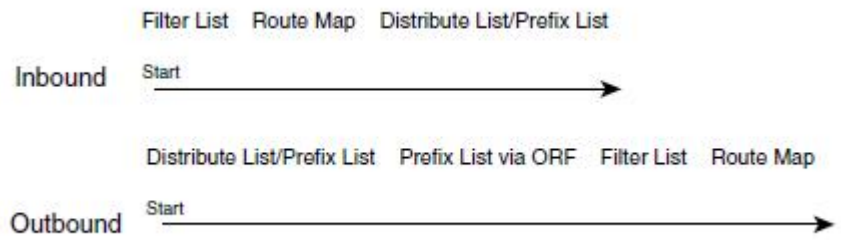
4.5.6 BGP Soft Reconfiguration

BGP joutuu alustamaan naapureiden välisen istunnon joka kerta, kun BGP-reitityspolitiikka päivitetään. Alustamisen takia reittejä joudutaan vetämään pois reititystaulusta ja hetken päästä taas lisäämään sinne. Se aiheuttaa reittien epävakautta, joka pahimmassa tapauksessa voi johtaa jonkin reitin vaimentamiseen. BGP tarjoaa tuen pehmeälle yhteyden alustamiselle, jonka avulla voidaan välttää reititystaulun tietojen edestakaista päivittämistä. Käytännössä tämä tarkoittaa sitä, että BGP-reititin tallentaa jokaisen naapurilta saaman reitin, vaikka BGP-politiikka kieltäisikin reitin vastaanottamisen. Tämä syö reitittimen muistia, mutta mahdollistaa reittien säilyttämisen

kun yhteyttä alustetaan. Politiikan kieltämät reitit tallennetaan myös, mutta BGP ei käytä näitä parhaan reitin valinnan prosessissa eli niitä ei myöskään mainosteta naapureille. Ominaisuuden saa käyttöön komennolla neighbor *address or peer group* soft-reconfiguration-inbound. [30, s.94.]

4.6 Suodatuslistat

BGP käyttää reitityspolitiikan toteuttamiseen erilaisia suodattimia, joiden avulla voidaan valita mainostettavat ja vastaanotettavat reitit. Suodatuslistoja luetaan ylhäältä alas ja sitä jatketaan niin kauan, kunnes verrattavalle säännölle löytyy listasta vastaavuus tai kunnes lista loppuu. Suodatinlistat käsitellään kuvan 13 esittämässä järjestyksessä. Reittipäivityksen tulee läpäistä kaikki suodatinlistat, jotta .



Kuva 13. Suodatinlistojen prosessointijärjestykset. [30, s.123]

4.6.1 Säännölliset lausekkeet

Säännölliset lausekkeet koostuvat säännöistä, joiden avulla haettavasta tiedosta voidaan haarukoida tietoa tarkemmin. Säännöllisiä lausekkeita voidaan käyttää esimerkiksi etsimään tiettyä AS-numeroa AS-polusta. Säännöt koostuvat merkeistä ja niiden asettamista rajoitteista etsittävälle tiedolle. BGP-politiikan käyttämät suodattimet voivat käyttää säännöllisiä lausekkeita spesifisen tiedon löytämiseen. [30, s.109-110.]

Säännöllisen lauseen käyttämät merkit:

.	Mikä tahansa merkki
^	Merkkijonon ensimmäinen merkki
$	Merkkijonon viimeinen merkki
_	Vastaa , tai { tai } tai välilyöntiä
|	Looginen TAI
\	Muuttaa säännöllisen lauseen kontrollimerkin normaaliksi merkiksi
*	Edeltävä merkki voi toistua useamman kerran tai ei kertaakaan
+	Edeltävä merkki voi toistua useamman kerran
?	Edeltävä merkki kerran tai ei kertaakaan
[ ]	Yksi merkki listan rajaamista arvoista

4.6.2 Pääsylistat

Pääsylistoja käytetään suodattamaan liikennettä. Useat eri suodatinlistat voivat käyttää pääsylistoja halutun liikenteen määrittämiseen. Pääsylistat ovat joko standardeja tai laajennettuja. Standardi pääsylista suodattaa liikennettä vain lähdeosoitteen ja maskin perusteella. Laajennettu lista ottaa lähdeosoitteen lisäksi huomioon myös kohdeosoitteen sekä OSI-mallin kuljetuskerroksen portit. Pääsylistat voidaan merkitä numeroilla tai nimellä. Standardi pääsylista käyttää numeroita 1-99 ja 1300-1999, kun laajennettu pääsylista käyttää numeroita 101-199 ja 2000-2699. Standardin pääsylistan syntaksi:

Router(config)# access-list access-list-number| access-list-name {permit|deny} {host|source source-wildcard|any}

Laajennetun pääsylistan syntaksi:
Router(config)# access-list access-list-number| access-list-name {deny|permit} protocol source source-wildcard [operator [port]] destination destination-wildcard [operator [port]]

Esimerkki laajennetusta pääsylistasta 150, joka kieltää telnet yhteyden verkosta 172.26.0.0/16 kaikkialle, mutta sallii kaiken muun: [34, luku 2.]

```
Router(config)#access-list 150 deny tcp  172.26.0.0 255.255.0.0 any eq telnet
Router(config)#access-list 150 permit ip 172.26.0.0 255.255.0.0 any
```

4.6.3 AS-Path-lista

AS-Path-listaa käytetään reititystietojen suodattamiseen AS-Path-attribuutin sisältämien arvojen perusteella. Säännöllisellä lausekkeella pyritään etsimään vastaavuus AS-polun sisältämistä AS-numeroista, jonka jälkeen lista joko sallii tai kieltää reitin. AS-Path-listaa voidaan käyttää neighbor-komennon yhteydessä suodattamaan naapurilta saatavia reittejä. AS-Path-listan avulla voidaan esimerkiksi suodattaa jonkin tietyn AS:n lähettämät reitit kokonaan pois. Komennon syntaksi ja esimerkki:

Router(config)#ip as-path access-list *access-list-number* {permit | deny} *as-regular-expression*

```
Router(config)#ip as-path access-list 10 deny _500$
```

Komento kieltää kaikki reitit, joiden AS-Path-attribuutin viimeisenä arvona on 500, eli sääntö kieltää kaikki reitit, jotka ovat alkuperäisin AS500:sta. [30, s.117-118.]

4.6.4 Community-lista

Community-listoja käytetään reittien suodattamiseen niiden sisältämän Community-attribuutin arvojen perusteella. Community-listoja on kahta eri tyyppiä, nimellisiä ja numeroituja. Listat voivat olla tyypiltään standardeja tai laajennettuja, joista laajennetut käyttävät säännöllisiä lausekkeita. Komennon syntaksi erityyppisille Community-listoille on:

Router(config)#ip community-list *list-number* {permit | deny} *community-number*
Router(config)#ip community-list *list-number* {permit | deny} *regular-expression*

Router(config)#ip community-list standard *list-name* {permit | deny} *community-number*
Router(config)#ip community-list expanded *list-name* {permit | deny} *regular-expression*

Komento ip bgp-community new-format muuttaa oletuksena olevan 16-bittisen community-arvon muotoon AA:NN, jossa AA on AS-numero ja NN on mikä tahansa 16-bittinen arvo.

Listan rivillä voi olla useita eri Community-arvoja välilyönnillä erotettuna. Haku täsmää vain, jos kaikki rivin Community-arvot osuvat haettavaan tietoon, eli samalla rivillä olevien Community-arvojen välillä on Looginen JA. Lista voi sisältää useampia rivejä ja hakutuloksen löytämiseen riittää yhden rivin osuma, eli rivien välillä on looginen TAI.

Router(config)#ip community-list 10 permit 500:20 500:30
Router(config)#ip community-list 20 permit 500:20
Router(config)#ip community-list 20 permit 500:30

Community-lista 10 vaatii, että Community-attribuutti sisältää sekä arvon 500:20 että 500:30. Community-list 20 on määritelty niin, että hakutuloksen osumiseen riittää, kun vain 500:20 tai 500:30 löytyy reitin ominaisuuksista. [30, s.118-120.]

4.6.5 Distribute-lista

Distribute-listaa voidaan käyttää suodattamaan reittejä reitityspäivityksistä. Se käyttää pääsylistoja suodattamiseen. Distribute-listoja käytetään, kun reititystietoja mainostetaan reitittimien välillä tai kun reittejä jaetaan reititysprosessista toiseen. Distribute-listalle määritetään verkot, joita ei haluta tai halutaan mainostaa ja suodatettavien päivitysten suunta. Komennon syntaksi: [35, s.139—140.]

Router(config)#distribute-list access-list-number in/out [interface-name | routing-process]

Esimerkki distribute-listasta, joka hylkää BGP-naapurin mainostaman 172.26.0.0/16-verkon, mutta sallii kaiken muun:

```
Router(config)#access-list 1 deny 170.26.0.0 0.0.255.255
Router(config)#access-list 1 permit any
Router(config-router)#neighbor 10.10.10.1 distribute-list 1 in
```

4.6.6 Prefiksilista

Reittejä on mahdollista suodattaa käyttämällä prefiksilistoja, jotka sopivat BGP-liikenteen suodattamiseen hyvin niiden rakenteen ansiosta. Suodattamiseen käytetään IP-prefiksiä ja prefiksin pituutta. Komennon syntaksi:

```
Router(config)#ip prefix-list {list-name | list-number} [seq number] {deny network/length | permit network/length} [ge ge-length] [le le-length]
```

Listalle voidaan antaa nimi ja listaan syötettävälle riville sen järjestysnumero. Järjestysnumeroa kasvatetaan viidellä viimeisenä listassa olevan rivin järjestysnumeroon nähden, jos sitä ei erikseen määritetä. Kuten kaikki muutkin listat, prefiksilistaa käydään ylhäältä alaspäin niin, että järjestysnumerolta pienimmät ovat listan ylimpänä. Listaa käydään niin pitkään läpi, kunnes verrattavalle prefiksille löydetään listasta sääntö, jonka se täyttää. Prefiksin pituuden määrittäminen on joustavaa lisämääreitä le (less-than-equal-to) ja qe (greater-than-equal-to) käyttämällä.

```
Router(config)#ip prefix-list testi 10 permit 10.0.0.0/24 ge 26
Router(config)#ip prefix-list testi 15 deny 0.0.0.0/0
```

Prefiksilista testi sallii verkon 10.0.0.0 prefiksit, joiden pituus on väliltä 26-32. Tämän lisäksi lista kieltää oletusreitin. [30, s.114-117.]

4.6.7 Route Map

Route map on monipuolinen työkalu reititystietojen muokkaamiseen ja politiikoiden toteuttamiseen. Sitä voidaan käyttää niin reititystietojen jakamisessa eri reititysprosessien välillä kuin BGP-politiikoiden toimeenpanijana. Route map etenee pienimmästä

järjestysnumerosta suurimpaan, kunnes ehdot täyttävä sääntö löytyy, jolloin loput route mapista jätetään käymättä läpi. Järjestysnumerot kertovat, mistä route mapin instanssista on kyse.

Route map koostuu useasta eri instanssista, joiden sisällä käytetään match- ja set-komentoja. Instanssin jokaisen match-säännön asettamat ehdot on käytävä toteen, jotta set-säännön määrittämät muutokset voidaan asettaa voimaan. Match-säännöt käyttävät erilaisia suodatinlistoja ja reittien parametrien arvoja osuman etsimiseen. Set-komento muokkaa match-säännön ehdot täyttäneen reitin ominaisuuksia.

Match-komennolla voi olla useita parametreja, jolloin riittää, kun yksi niistä käy toteen, eli parametrien välillä on looginen TAI. Jos instanssissa on useampi samantyyppinen match-komento, niin riittää kun yksi ehdoista käy toteen, eli samantyyppisten match-komentojen välillä on looginen TAI. Erityyppisten match-komentojen on kaikkien käytävä toteen, eli niiden välillä on looginen JA.

```
(config)# ip as-path access-list 50 permit ^600$
(config)# route-map ESIMERKKI permit 10
(config-route-map)# match as-path 50
(config-route-map)# set community 200:20
```

Route map ESIMERKKI asettaa Community-arvoksi 200:20 kaikille AS-path-listan 50 ehdot täyttäville reiteille.

Route map:n yhteydessä voi myös käyttää Policy-listoja, jotka ovat route map:in osakokonaisuuksia ja käyttävät vain match-lausekkeita. Niiden käyttö vähentää konfiguroinnin tarvetta jos useampi route map sisältää samoja match-lausekkeita. Route mapit voivat viitata Policy-listaan komennolla match policy-list *list-name* ja Policy-lista määritellään komennolla ip policy-list *list-name* {permit | deny}. [30, s.120-122.]

4.7 Internal BGP

BGP käyttää reitityssilmukoiden estämiseen AS-polkua. BGP hylkää reitin, jos sen AS-polusta löytyy sama AS-numero. Samaa mekanismia ei voida käyttää autonomisen jär-

jestelmän sisällä iBGP-yhteyksissä, sillä iBGP:ssä reitittimet eivät lisää AS-numeroa AS-listaan, jolloin silmukoitumista ei voida tarkistaa. Tämän takia iBGP-naapurit eivät mainosta toiselta iBGP-naapurilta saatuja reitityspäivityksiä eteenpäin, jotta ei syntyisi reitityssilmukoita. Autonomisen järjestelmän sisällä iBGP-naapureiden tulee muodostaa full mesh -topologia, jotta reititystiedot voidaan jakaa jokaisen naapurin kesken. Full mesh -topologialla tarkoitetaan sitä, että jokainen iBGP-naapuri muodostaa yhteyden jokaiseen iBGP-naapuriin. Suurissa verkoissa iBGP ei skaalaudu hyvin, ja siksi monet operaattorit käyttävätkin esimerkiksi reittiheijastimia iBGP-tiedon jakamiseen. Reittiheijastimien ideana on se, että BGP-naapurit solmivat yhteyden yhden tai useamman reittiheijastimena toimivan reitittimen kanssa. Reittiheijastin toimii reititystietojen keskitettynä jakopisteenä BGP-naapureiden kesken.

Sisäinen reititysprotokolla ylläpitää tiedon autonomisen järjestelmän sisäisestä verkkotopologiasta ja sen kautta saadaan myös tieto, kuinka tavoittaa jokainen AS:n IP-osoite. Sisäisten reititysprotokollien ansioista iBGP-yhteyksien välissä voi olla useitakin hyppyjä. Next-hop-osoite pysyy muokkaamattomana, kun tietoa välitetään kahden iBGP-naapurin välillä. IGP kertoo iBGP-naapureille, kuinka saavuttaa reitin mukana mainostettu Next-hop-osoite. Sisäiset reititysprotokollat reagoivat nopeammin myös virhetilanteisiin ja konvergoituvat nopeammin.

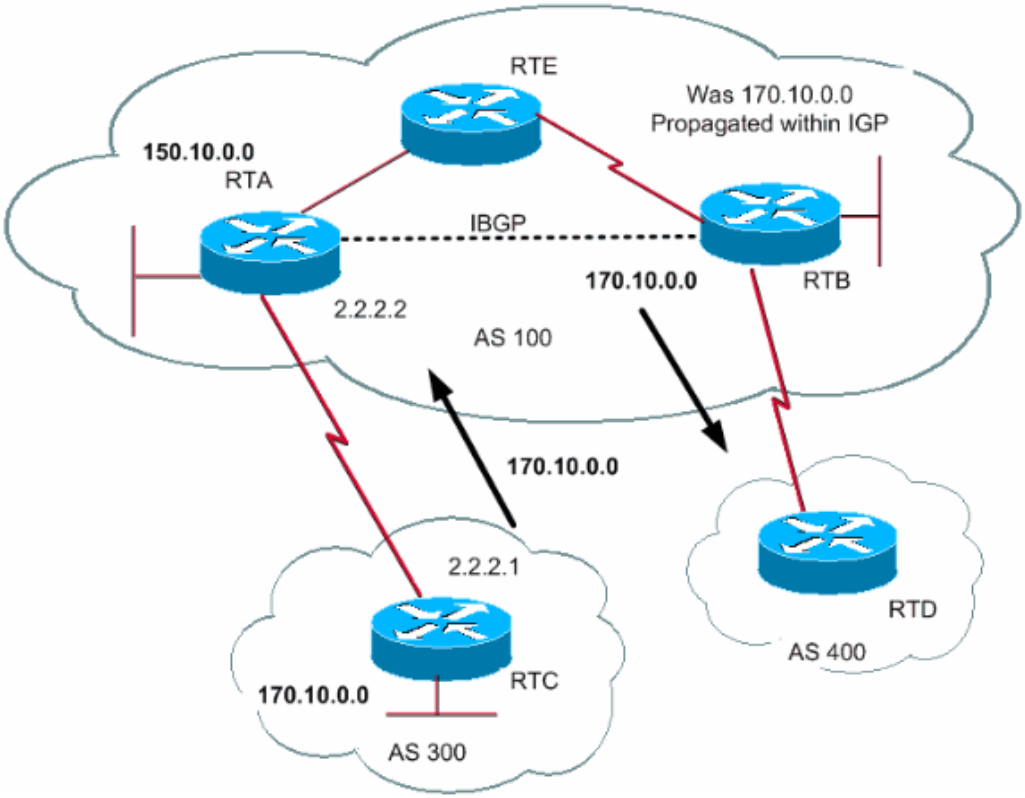
Sisäisen BGP:n reittejä ei jaeta sisäisten reititysprotokollien käyttöön, koska se voi johtaa reitityssilmukoiden syntymiseen. BGP mainostaa iBGP-naapureille vain parasta reittiä verkosta ulos. [30, s.21-24.]

4.8 Synkronointi

BGP määrittelee, että jos autonominen järjestelmä aikoo välittää liikennettä muille järjestelmille, tulee sen muille järjestelmille mainostettavien reittien löytyä myös sisäisen reititysprotokollan kautta. Reittien mukana kulkevat attribuutit eivät säily, jos reitit jaetaan BGP→IGP→BGP, koska sisäiset reititysprotokollat eivät pysty säilyttämään polun attribuuttien ominaisuuksia reitityspäivityksissään.

Synkronoinnilla pyritään takaamaan se, että järjestelmän sisäisillä reitittimillä olisi tieto siitä, mistä kohdeverkko löytyy ja kuinka sinne pääsee. Vaihtoehdot ovat BGP-tietojen

jakaminen IGP:lle, Full mesh-iBGP ja synkronoinnin pois ottaminen. Synkronointia ei tarvita, jos järjestelmä ei välitä liikennettä eri järjestelmien välillä. Synkronoinnin saa pois päältä BGP-prosessin komennolla no synchronization.



Kuva 14. Synkronointi. [36]

Kuvassa 14 reititin RTB ei mainosta verkkoa 170.10.0.0/16 reitittimelle RTD ennen kuin se näkee saman reitin myös sisäisen reititysprotokollan kautta. RTA ja RTB ovat iGBP-naapureita, mutta RTE ei osallistu iBGP-prosessiin. Liikenne 170.10.0.0/16-verkkoon joutuu kulkemaan reitittimen RTE kautta, mutta RTE ei tiedä, kuinka päästä sinne. RTE voisi saada tiedon kohdeverkosta, jos se osallistuisi iBGP-prosessiin tai jos RTA jakaisi reititystiedon BGP-prosessista sisäisen reititysprotokollan käyttöön. Ilman synkronointia RTB mainostaisi verkkoa 170.10.0.0/16 ja RTD:n pyrkimykset päästä sinne pysähtyisivät reitittimeen RTE, koska se ei tunne reittiä kohdeverkkoon. [36.]

4.9 Reittien syöttäminen BGP:lle

Reittien injektoiminen BGP-prosessiin tapahtuu pääasiallisesti kahdella eri komennolla, jotka ovat redistribute ja network.

Network-komennolla injektoitavasta prefiksistä on oltava reitti IP-reititystaulussa tai muuten injektointia ei voida suorittaa BGP-reititystauluun. IP-reititystaulusta on löydyttävä täsmälleen sama verkko ja verkon maski, jos network-komennon kanssa käytetään verkkomaskia. Network-komentoa voi käyttää myös ilman maskia, jolloin automaattinen verkkojen summaaminen muuttaa injektoitavat reitit luokallisiksi verkko-osoitteiksi. Automaattisen summaamisen yhteydessä riittää, kun IP-reititystaulusta löytyy yksi tai useampi luokallisen verkon spesifinen osoite. Reitit saavat Origin-attribuutikseen arvon IGP, kun reitit syötetään BGP-prosessiin network-komennolla.

```
Router(config)#interface fastethernet 0/1
Router(config-int)#ip address 10.10.10.1 255.255.255.0
Router(config-router)#network 10.10.10.0 mask 255.255.255.0
Router(config-router)#no auto-summary
```

Reititystaulusta löytyy verkko 10.10.10.0/24, koska reitittimen fe0/1-portti on suoraan yhteydessä mainittuun verkkoon. Verkko lisätään BGP-tauluun tarkkaa maskia käyttäen.

Redistribute-komennolla voidaan jakaa reittejä BGP-prosessiin eri lähteistä kuten vaikkapa kaikki reitittimen staattiset reitit tai toisesta reititysprotokollasta. Redistribute-komentoa kannattaa käyttää harkiten ja pitää huolta, että BGP-prosessiin ei tule sinne kuulumattomia reittejä. Yleensä reittien jakamisen yhteydessä käytetään erilaisia suodatinlistoja valikoimaan halutut reitit. BGP-prosessiin jaetut reitit saavat Origin-attribuutikseen Incomplete. [30, s.31.]

4.10 BGP-yhteyden konfigurointi

4.10.1 Naapurin määrittäminen

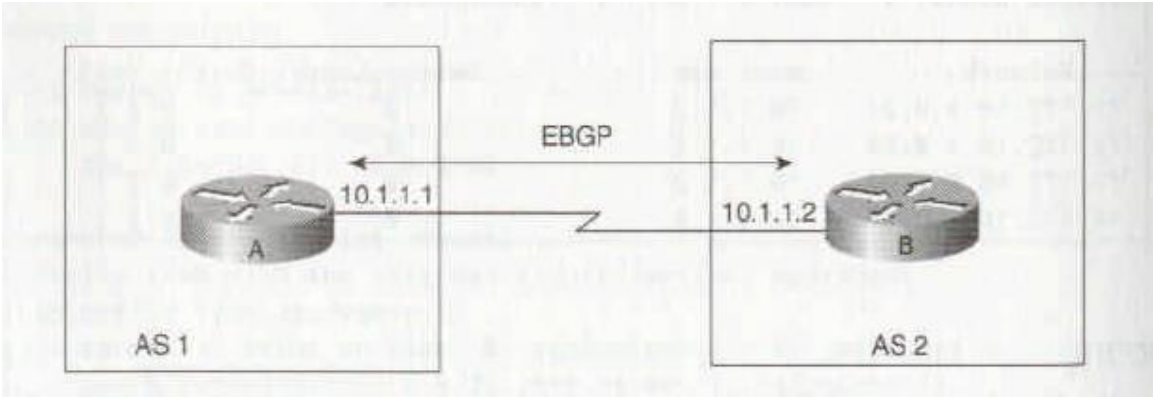
BGP-muodostaa yhteyden jokaiseen naapuriin erikseen. BGP erottaa AS-numeroita vertailemassa, onko kyseessä iBGP- vai eBGP-sessio. BGP-yhteyden konfiguraatio aloitetaan naapurisuhteen määrittämisellä BGP-prosessissa. BGP-reitiysprosessi määritellään komennolla.

Router(config)# router bgp as-number

AS-number kertoo, minkä autonomisen järjestelmän alaisuudessa reititin toimii. Naapuri määritetään komennolla.

Router(config-router)#neighbor {ip-address|peer-group-name} remote-as number

Sisäinen että ulkoinen BGP-yhteys konfiguroidaan samaa komentoa käyttäen. Ainoana erona on komennossa käytettävän AS-numero, joka on eBGP-yhteydessä eri kuin komentoa suorittavan reitittimen AS-numero. Naapurisuhde voidaan solmia käyttämällä naapurireititimen tietoliikenneportin IP-osoitetta tai jos BGP-ryhmää, jos naapuri on määritetty ryhmän jäseneksi.



Kuva 15. BGP-yhteys. [37, s199]

Kuvan 15 reitittimen A ja B solmivat naapurisuhteen. Reittimen A konfiguraatio:

Router(config)# router bgp 1
Router(config-router)#neighbor 10.1.1.2 remote-as 2

Normaalisti eBGP-naapureiden on oltava suoraan tavoitettavissa, jotta BGP pystyy muodostamaan yhteyden naapurin IP-osoitteeseen. Naapureiden ei kuitenkaan tarvitse olla suoraan tavoitettavissa, jos naapurimääritys on tehty käyttäen ebgp multihop-komentoa. [37, s.198-201.]

4.10.2 MD5-autentikointi

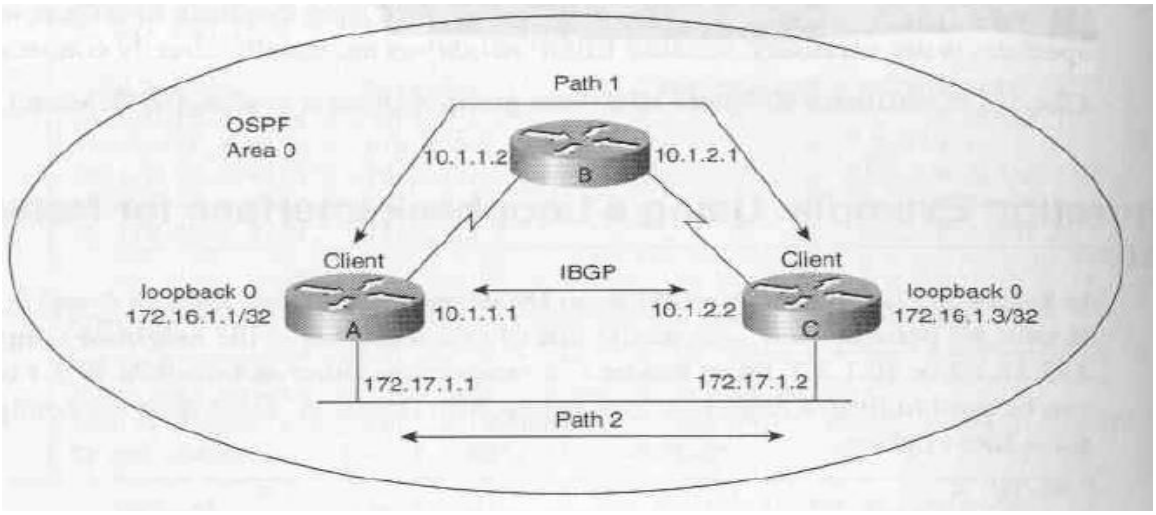
BGP-naapurit voivat autentikoida itsensä käyttämällä MD5-autentikointia BGP-yhteydessä. Autentikointi suojaa vihamielisiltä yhteyksiltä, jotka voisivat esimerkiksi syöttää BGP-prosessiin väärää reititystietoa. Kummallakin BGP-naapurilla pitää olla sama yhteyden salasana määritettynä tai yhteys ei muodostu. Salasanan määrittäminen johtaa uuden BGP-yhteyden luomiseen, jonka jälkeen reititin tarkistaa jokaisen BGP-yhteyteen liittyvän paketin autentikoinnin. [37, BGP4 s.182-183.]

Komennon syntaksi on: Router(config-router)# neighbor {ip-address|peer-group-name} password password

4.10.3 Loogisen portin käyttö BGP-yhteydessä

Naapuriyhteyden määrittäminen fyysisen portin IP-osoitteen mukaan aiheuttaa BGP-yhteyden katkeamisen naapuriin, jos yhteys porttiin katkeaa. BGP-reititin voi käyttää loogisen (loopback) portin IP-osoitetta yhteyden muodostamiseen. Looginen portti mahdollistaa toisen reitin käytön jos ensisijainen reitti katkeaa. Sisäiset BGP-reitittimet käyttävät usein loogisen portin IP-osoitetta BGP-yhteyden muodostamiseen, sillä monesti iBGP-reitittimien välillä on useampia vaihtoehtoisia reittejä IGP:n kautta opittuna. Komennon syntaksi:

Router(config-router)#neigbor {ip-address|peer-group-name} update-source interface-name



Kuva 16. Loogisen portin käyttö BGP-osoitteena. [37, s.236]

Kuvan 16 reitittimet ovat iBGP-naapureita. Naapurit solmivat BGP-yhteydet käyttäen loogisten porttien osoitetta, jotta IGP voi toimittaa virhetilanteissa vaihtoehtoisen reitin naapurille. Reitittimen A konfiguraatio:

```
Router(config)#interface loopback0
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config)# router bgp 1
Router(config-router)#neighbor 172.16.1.3 remote-as 1
Router(config-router)#neighbor 172.16.1.3 update-source loopback0
```

Sisäisenä reititysprotokollana toimii OSPF, joka mainostaa verkkoja kaikkien reitittimien välillä. Myös loogiset portit sisältyvät reittimainostuksiin. Reititinten A ja C välillä on kaksi vaihtoehtoista reittiä, joita voidaan hyödyntää vikatilanteissa, sillä naapurisuhteet on solmittu loogisen portin IP-osoitteita käyttäen. Reititin A käyttää reittipäivityksien lähettämiseen loopback0-portin IP-osoitetta ja on määrittänyt naapurikseen reitittimen C looback0-portin IP-osoitteen. [37, s.234-238.]

4.10.4 BGP-ajastimet

BGP käyttämiä ajastimia voidaan muokata joko globaalisti tai naapurikohtaisesti. Keepalive-vietejä lähetetään normaalisti 60s välein ja holdtime-ajastin on 180s. Hyvä nyrkkisääntö on pitää holdtime-ajastinta kolminkertaisena verrattuna keepalive-ajastimeen. Ajastimien muuttaminen globaalisti ja naapurikohtaisesti:

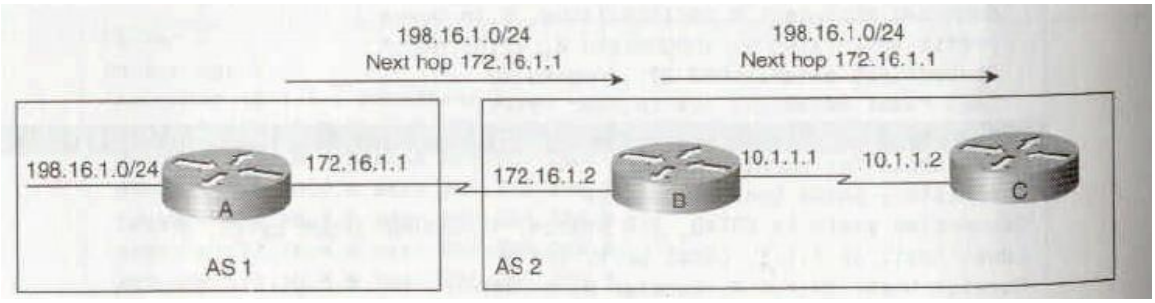
```
Router(config-router)#timers bgp keepalive holdtime
Router(config-router)#neighbor ip-address timers keepalive holdtime
```

Ajastimia muuttamalla voidaan nopeuttaa BGP:n konvergenssia. Ajastimia muuttamalla havaitaan nopeammin naapurit, joihin ei enää saada yhteyttä. BGP alustaa yhteyden vasta, kun holdtime-ajastin on kulunut loppuun. [37, s.279-282.]

4.10.5 Multihop ja Multipath

Eri autonomisten järjestelmien naapurit eivät ole aina suoraan yhteydessä. Naapureiden välissä voi olla reitittimiä tai naapurit voivat käyttää loogisia portteja BGP-yhteyttä varten, jolloin naapuri on vähintään kahden hypyn takana. BGP tarjoaa tuen eBGP-naapureille, jotka ovat useamman hypyn takana komennolla:

Router(config-router)#neighbor {ip-address|peer-group-name} ebgp-multihop maximum-hop-count



Kuva 17. EBGP multihop. [37, s.180]

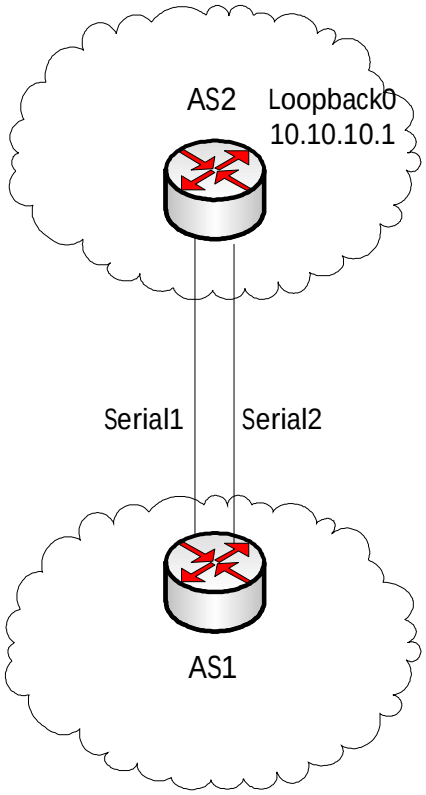
Kuvan 17 reitittimet A ja C ovat eBGP-naapureita, jotka eivät ole suoraan yhteydessä toisiinsa. Reitittimet ovat toisistaan kahden hypyn päässä, koska niiden välissä on yksi reititin. Ne eivät myöskään tiedä toisistaan ilman, että niiden välillä jaetaan reititystietoja reititysprotokollalla tai staattisten reittien kautta. Reitittimen A konfiguraatio:

```
Router(config)#ip route 10.1.1.0 255.255.255.252 172.16.1.2 serial0
Router(config)# router bgp 1
Router(config-router)#neighbor 10.1.1.2 remote-as 2
Router(config-router)#neighbor 10.1.1.2 ebgp-multihop 2
```

Konfiguraatio määrittelee, että reititin A pystyy tavoittamaan reitittimen C kahden hypyn päähän ja reitti C:lle on saatu määritelty staattisesti. Multihop-komentoa jouduttaisiin myös käyttämään, jos A ja B olisivat naapureita ja käyttäisivät yhteyteen loogisen portin IP-osoitteita, sillä ne olisivat kahden hypyn päässä toisistaan. [37, s.149-151.]

Multihop mahdollistaa kuorman jakamisen usean yhteyden ylitse eBGP-naapureiden kesken. Naapureiden tulee käyttää loopback-osoitteita eBGP-yhteyden muodostami-

seen. Sen lisäksi tarvitaan staattiset reitit, jotka osoittavat naapurin loopback-osoitteen löytyvän jokaisen linkin takaa. Esimerkki kuvan 18 AS1:n reitittimen konfiguraatiosta: [30, s. 233-234.]



Kuva 18. Multihopin käyttö kuorman jakamiseksi.

Router(config)#ip route 10.10.10.1 255.255.255.255 Serial1
Router(config)#ip route 10.10.10.1 255.255.255.255 Serial2
Router(config-router)#neighbor 10.10.10.1 remote-as
Router(config-router)#neighbor 10.10.10.1 ebgp-multihop 2
Router(config-router)#neighbor 10.10.10.1 update-source Loopback0

EBGP Multipath on toinen BGP:n tukema tekniikka kuorman jakamiseksi eBGP-naapureiden välillä. Reittien on oltava identtiset, jotta useampaa linkkiä voidaan hyödyntää. Reitin MED-arvoa tai muita parametreja eivät saa olla muokattuja tai Multipahtia ei voida toteuttaa. Komennon syntaksi, jossa number-of-paths kertoo maksimissaan asennettavien reittien määrän: [30, s.235-236.]

Router(config-router)#maximum-paths number-of-paths

4.10.6 Next-hop-self

Autonomisen järjestelmän BGP-reunareititin ei muuta eBGP-naapurilta saadun reitin Next-hop-osoitetta, vaan se lähettää tiedon reitistä ja myös sen seuraavan hypyn osoitteesta sellaisenaan iBGP-naapureille. Sisäisillä BGP-naapureilla tulee olla tieto siitä, miten Next-hop-osoitteeseen pääsee. Ongelma voidaan ratkaista mainostamalla IGP-prosessissa eBGP-naapureiden välistä linkkiä tai muuttamalla seuraavan hypyn osoitteeksi reunareitittimen portin IP-osoitteen, jolla se on yhteydessä iBGP-naapureihin. [37, s.180-182.]

```
Router(config)#neighbor {ip-address|peer-group-name} next-hop-self
```

Kuvassa reititin B mainostaa reitittimeltä A saatua reittiä iBGP-naapurille C Next-hop-osoitteella, joka on reitittimen A portin osoite. Reititin B voi mainostaa A:lta saatua reittiä Next-hop-osoitteella 10.1.1.1 komennolla:

```
Router(config)#neighbor 10.1.1.2 next-hop-self
```

4.10.7 Router-ID

BGP-reitittimen tunnisteena toimii korkein minkä tahansa portin IP-osoite. Jos reitittimelle on määritetty looginen portti, niin korkein loogisen portin IP-osoitteesta toimii reitittimen tunnisteena, vaikka jollakin fyysisellä portilla olisikin korkeampi IP-osoite. BGP-tunnistetta käytetään identifioimaan eri naapureiden BGP-yhteydet ja päivitykset. BGP-tunnisteen voi myös määrittää käsin komennolla: [37, s.91-94.]

```
Router(config-router)#bgp router-id ip-address
```

4.11 Reittiaggregaatio

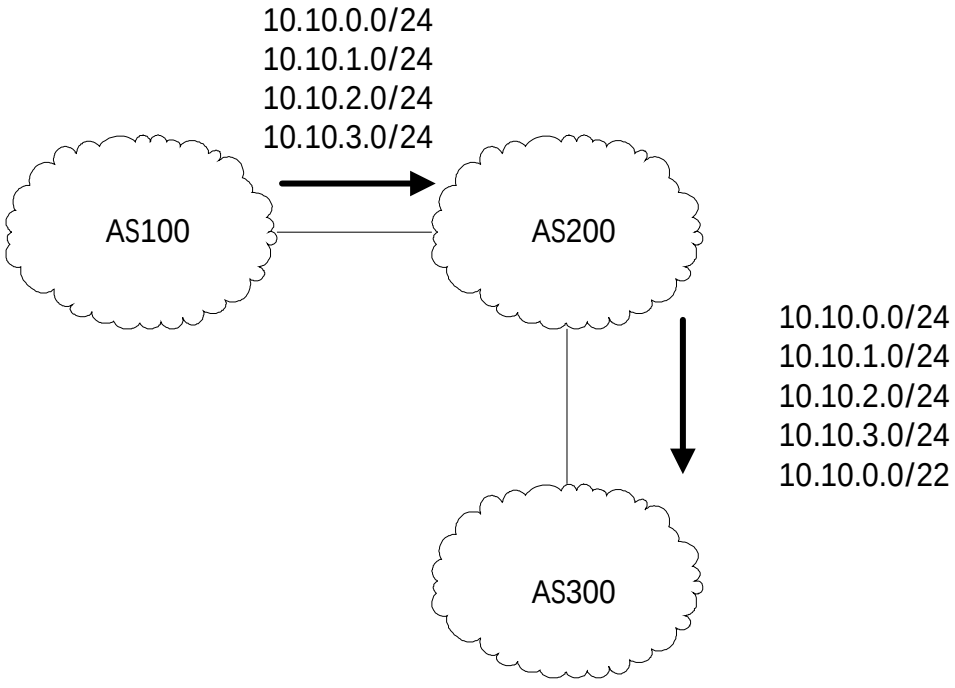
Reittien aggregaatio on tärkeää BGP-protokollalle, sillä sen avulla Internetin reititystaulut voidaan pitää siedettävän kokoisena. Aggregoinnin voi tehdä usealla eri tavalla. Kaikille niistä yhteistä on se, että summatulle reitille on löydyttävä täsmälleen sama prefiksi tai vähintään yksi summatun verkon spesifinen verkko-osoitteista. Summaami-

selle on myös se tyypillistä se, että summaaminen hävittää reitin alkuperän. BGP:n attribuuttia atomic-aggregate käytetään merkkaamaan summattuja reittejä, jotka piilottavat summaamiensa reittien todellisen alkuperän. BGP-prosessissa reittien summaamiseen käytettävän komennon syntaksi.

Router(config-router)#aggregate-address address mask

Router(config-router)#network 10.10.0.0 mask 255.255.255.0
Router(config-router)#network 10.10.1.0 mask 255.255.255.0
Router(config-router)#network 10.10.2.0 mask 255.255.255.0
Router(config-router)#network 10.10.3.0 mask 255.255.255.0
Router(config-router)#aggregate-address 10.10.0.0 255.255.252.0

Reititin lisää BGP-tauluun verkot 10.10.0.0 - 10.10.3.0/24, jotka se summaa verkoksi 10.10.10.0/22. Reititin mainostaa summatun verkon lisäksi myös jokaisen spesifisen verkon. Summattu verkko merkitään atomic-aggregate-attribuutilla. Tässä tapauksessa reititystietoja ei katoa, koska summatun ja spesifisten verkkojen alkuperä on sama.



Kuva 19. Reittien summaaminen.

Kuvassa 19 AS100 mainostaa verkkoja 10.10.0.0 - 10.10.3.0/24, jotka AS200 summaa ja lähettää spesifisten verkko-osoitteiden lisäksi summatun verkon AS300:lle. AS300 näkee summatun verkon 10.10.0.0/22 olevan alkuperäisin AS200:sta ja spesifististen reittien olevan alkuperäisin AS100:sta. Summaamisen seurauksena näyttäisi siltä, että AS200 omistaisi summatun verkon. AS300 näkee spesifisten verkkojen AS-polun (200, 100, i) ja summatulle reitille AS-polku on (200, i). Komennon parametri as-set näyttää summatulle reitille sen oikean alkuperän. AS300 näkisi summatun reitin AS-polun (200, 100, i) jos komennon yhteydessä olisi käytetty parametria as-set.

Router(config-router)#aggregate-address address mask as-set

Router(config-router)#aggregate-address address mask summary-only

BGP lisää automaattisesti summatulle reitille staattisen viittauksen loogiseen Null0-porttiin. Null0:aan reititetyt paketit tiputetaan. Jos AS100 lopettaisi verkon 10.10.10.2/24 mainostamisen ja AS300 haluaisi lähettää sinne dataa, niin se onnistuisi summattua reittiä käyttäen. Summattua reittiä mainostetaan jos reititystaulusta löytyy yksikin summatun verkon spesifinen verkko-osoite. AS300 tietää reitin verkkoon 10.10.0.0/22, joka sisältää verkon 10.10.2.0/24. AS200 ei kuitenkaan enää tiedä reittiä verkkoon 10.10.2.0/24, koska AS100 on vetänyt reitin pois. AS200:n reititystaulussa verkko 10.10.0.0/22 viittaa Null0:aan, jossa paketit tiputetaan.

Reittien summaaminen onnistuu myös staattisia reittejä mainostamalla.

Router(config)# ip route 10.10.0.0 255.255.252.0 Null0
Router(config)#router bgp 200
Router(config-router)#redistribute static
Router(config-router)#no auto-summary

Reititin luo halutun summatun reitin staattisesti ja laittaa sen viittaamaan Null0:aan. Staattiset summattu reitti jaetaan BGP:llä naapureille. On tärkeätä muistaa antaa komento no auto-summary, jotta jaettuja staattisia reittejä ei muuteta luokallisiksi osoitteiksi. Komennon redistribute static voisi myös korvata komennolla network 10.10.0.0 255.255.252.0, jolloin summattua reittiä mainostettaisiin ilman, että

staattisia reittejä jaettaisiin. Summattuja reittejä on myös mahdollista mainostaa vain tietyn reittien osajoukon kanssa tai ilman, että spesifisiä reittejä mainostetaan sen kanssa. [37, s.3-17.]

4.12 BGP Peer Group

Suuri määrä iBGP-naapureita aiheuttaa ongelmia verkon skaalautumisen suhteen varsinkin operaattoreiden verkoissa. Yrityksen verkon BGP-asennusta ja konfigurointia voi helpottaa käyttämällä BGP-ryhmiä. Ryhmään liitetään naapurit, joiden BGP-politiikat ovat samanlaisia. Ryhmien käyttä vähentää huomattavasti konfiguraation kuluvaa aikaa kun jokaiselle BGP-naapurille ei välttämättä tarvitse syöttää jokaista komentoa uudestaan. Komennon syntaksi.

```
Router(config-router)#neigbor peer-group-name peer-group-name
```

```
Router(config-router)#neigbor peer-group-name peer-group
Router(config)#access-list  10 deny 172.26.1.0 0.0.0.255
Router(config)#access-list  20 permit 172.26.50.0 0.0.0.255
Router(config)#route-map ESIMERKKI permit 5
Router(config-route-map)#match ip address 10
Router(config)#route-map ESIMERKKI permit 10
Router(config-route-map)#match ip address 20
Router(config-route-map)#set community 200:10
Router(config)#route-map ESIMERKKI permit 15

Router(config)#router bgp 200
Router(config-router)#network 172.26.1.0 mask 255.255.255.0
Router(config-router)#network 172.26.50.0 mask 255.255.255.0
Router(config-router)#neigbor EBGP peer-group
Router(config-router)#neigbor EBGP route-map ESIMERKKI out
Router(config-router)#neigbor EBGP send-community
Router(config-router)#neigbor EBGP update-source loopback0
Router(config-router)#neigbor EBGP ebgp-multihop 2
Router(config-router)#neigbor 10.10.10.1 peer-group EBGP
```

```
Router(config-router)#neigbor 10.10.10.1 remote-as 1
Router(config-router)#neigbor 10.10.20.2 peer-group EBGP
Router(config-router)#neigbor 10.10.20.2 remote-as 2
Router(config-router)#neigbor 10.10.30.3 peer-group EBGP
Router(config-router)#neigbor 10.10.30.3 remote-as 3
```

Esimerkissä jokainen eBGP-naapuri liitetään ryhmään EBGP ja ryhmälle on määritetty route map ESIMERKKI, joka kieltää verkon 172.26.1.0/24 mainostamisen ryhmän jäsenille. Route map merkkaa 172.26.50.0/24-verkon community-attribuutin arvolla 200:10. Route map sallii kaikki muut verkot ilman muutoksia polun attribuutteihin. Ryhmälle on määritelty route mapin lisäksi vielä komennot send-community, update-source ja ebgp-multihop. Ilman ryhmää komentoja jouduttaisiin antamaan neljä kappaletta per naapuri, eli yhteensä kaksitoista kappaletta ja ryhmää käyttämällä tarvitaan vain neljä. [3, s.124, s.265-269.]

4.13 BGP-Oletusreitti

BGP voi syöttää reititystauluun oletusreitin ja mainostaa sitä naapureille. Oletusreittiä mainostetaan tynkä-AS:lle, joilla ei ole muita yhteyksiä Internetiin. Oletusreittiä voidaan myös mainostaa, jos naapuri ei halua tarkempia reittejä muihin verkkoihin. BGP tarjoaa kolme eri tekniikkaa oletusreitin lisäämiseen BGP-reititystauluun.

Ensimmäisenä on oletusreitin lisääminen network-komentoa käyttäen. IP-reititystaulusta tulee löytyä reitti verkkoon 0.0.0.0/0, jos oletusverkko halutaan mainostaa network-komentoa käyttäen. Jos oletusverkko poistuu IP-reititystaulusta, lopetetaan sen mainostaminen myös BGP-naapureille.

```
Router(config)ip route 0.0.0.0 0.0.0.0 Null0
Router(config-router)#network 0.0.0.0
```

Oletusreitti syötetään IP-reititystauluun staattisesti, mutta se voisi tulla sinne yhtä hyvin esimerkiksi sisäisen reititysprotokollan kautta. Oletusreitti voidaan mainostaa naapureille network-komentoa käyttäen samalla tapaa kuin muitakin verkkoja mainostettaisiin.

```
Router(config)ip route 0.0.0.0 0.0.0.0 Null0
Router(config-router)#redistribute static
Router(config-router)#default-information originate
```

Toinen tapa on syöttää oletusreitti jakamalla staattiset reitit BGP-prosessiin. BGP tarvitsee tämän lisäksi vielä komennon default-information originate, jotta oletusreittiä voidaan mainostaa naapureille.

Kolmas tapa on käyttämällä komentoa.

```
Router(config-router)#neighbor ip-address default-originate [route-map route-map-name ]
```

Komennolla voidaan mainostaa oletusreittiä, vaikka sitä ei olisikaan IP-reititystaulussa. Komentoon voi liittää route mapin, joka tarkistaa löytyykö oletusreitti tai jokin muu haluttu reitti. Oletusreitti mainostetaan naapurille jos route map löytää IP-reititystaulusta halutun reitin. [38, Adding Default Routes to BGP.]

5 KAHDENTAMINEN

5.1 Hierarkia ja modulaarisuus

Tietoverkkojen jakaminen eri kerroksiin helpottaa topologian ja koko verkon suunnittelua. Kerrokset on jaettu niiden toiminnallisuuksien perusteella. Verkkoa on helpompi laajentaa, ja se on helpommin hallittavissa kun noudatetaan hierarkista lähestymistapaa verkon rakentamisessa. Tietoliikenneverkkojen arkkitehtuuri yrityksen sisällä voidaan jakaa karkeasti kolmeen eri kerrokseen.

Alimpana on pääsykerros, jonka tarkoituksena on tuottaa loppukäyttäjälle mahdollisuus liittyä verkkoon esimerkiksi kytkinporttien kautta. Pääsykerroksella voidaan tarjota porttikohtaisia turvatoimia, kuten esimerkiksi Mac-osoiterajoituksia. Internet-yhteys sijoitetaan yleensä erilliseen moduuliin, joka sijaitsee pääsykerroksella.

Keskimmäinen kerros on jakokerros. Kerroksen tärkeimpiä tehtäviä on yhdistää eri jakokerroksen osia toisiinsa ja summata liikenne ydinkerrokselle. Jakokerroksella myös toteutetaan suurin osa tietoliikennepolitiikoista, kuten esimerkiksi pääsylistat.

Ydinkerros on hierarkian ylin kerros. Sen tehtävänä on välittää liikennettä mahdollisimman nopeasti. Siellä ei toteuteta politiikoita tai tarjota pääsyä verkkoon. Ydinkerros yhdistää jakokerroksesta tulevan liikenteen ja sen kautta on pääsy kaikkialle verkossa. [39, s.121-131.]

Verkon osa-alueista pyritään tekemään modulaarisia. Se tarkoittaa, että verkko on rakennettu hierarkia ja redundanssi huomioon ottaen. Moduulit voidaan ajatella liikkuviksi osiksi, jotka voisi sijoittaa minne tahansa verkossa. Moduulilla on yleensä jokin tietty toiminto, kuten esimerkiksi Internet-yhteyden tarjoaminen. [39, s.133.]

5.2 Redundanssi

Kahdentamisen pyrkimyksenä on estää single point of failure (SPOF)-pisteet. Ne ovat pisteitä, jotka häiriöillään tai toimimattomuudella estävät muun verkon toiminnan. SPOF-piste voi lamauttaa koko verkon, vaikka muu verkon infrastruktuurista olisi kahdennettu. Kahdennuksella päästään eroon yhden pisteen aiheuttamista toimintahäiriöistä. Kahdentamisella tarkoitetaan tietoliikenneinfrastruktuurin yksittäisten osien tuplaamista, jotta toinen voi toimia varalla vikatilanteissa. Mikä tahansa tietoliikenteen osa voidaan kahdentaa. Kahdentaessa tulee myös ottaa huomioon infrastruktuurin maantieteellinen sijainti. Hyvänä käytäntönä voidaan pitää sitä, että kaikki laitteet on kahdennettuna kahteen eri maantieteelliseen sijaintiin, jotta suurikaan onnettomuus ei lamauta verkon toimintaa.

Kahdennus voidaan suorittaa jonkin verkkoalueen sisällä tai verkkoalueiden välillä. Esimerkiksi pääsy- ja jakokerrosten tietoliikennelinkit voidaan tuplata, jolloin kahdennus tapahtuisi verkkoalueiden välillä. Kahdentaminen lisää verkon mutkikkuutta ja kahdennusta suunnitellessa tuleekin ottaa huomioon, kuinka paljon siitä voidaan maksaa. Asiakkaan tarpeet on myös otettava huomioon kahdennusta tehtäessä. [39, s.145-146.]

Asiakkaalle pitää saada tuottoa kahdennuksesta, joko suoraan tai välillisesti. Redundantti ratkaisu nostaa tuotteiden ja palveluiden saatavuutta, joiden tavoitettavuuden menettäminen voi tuoda yritykselle tappioita. Internet-yhteyden kahdentaminen on tärkeää yrityksen imagolle. Nykypäivänä on tärkeää, että yritys verkostoituu ja on näkyvillä sosiaalisessa mediassa. Internet-yhteyden katkeaminen tarkoittaisi sitä, että asiakkaat eivät pääsisi esimerkiksi yrityksen kotisivuille. Internet-yhteys vaikuttaa myös sähköpostin toimintaan, extranet-palveluihin ja yrityksen VPN-tunneleihin. Päivän trendinä on myös pilvipalvelut, jotka sijaitsevat Internetissä palveluntarjoajien konesaleissa ja ne tarjoavat palveluita Internet-yhteyden yli.

5.3 Varareitit

Varareitit toimivat korvaavina reitteinä, jos pääasiallinen reitti vikaantuu. Varayhteyden tulee kulkea eri tietoliikennelaitteiden läpi kuin pääreitin. Tietoliikennelaitteen vikaantuminen estäisi myös varareitin käytön, jos se kulkisi saman laitteen läpi kuin pääreitti. Kahdennettua reittiä suunnitellessa tulee ottaa huomioon, kuinka paljon se pystyy välittämään liikennettä ja kuinka nopeasti verkko alkaa käyttää varayhteyttä. Yleensä varayhteys ei pysty välittämään yhtä suurta määrää liikennettä kuin pääasiallinen yhteys. Varayhteyden avulla voidaan helpottaa pääyhteyden taakkaa jakamalla liikennettä niiden välillä. [39, s.130-131.]

Internet-yhteyttä kahdentaessa tulee ottaa huomioon, että BGP ei voi taata kuorman tasaista jakoa linkkien kesken. Monesti toinen yhteyksistä on hitaampi, ja kaikki liikenne ohjataan vain pääreittiä pitkin ulos verkosta. Reitityspolitiikat voivat myös johtaa siihen, että vain toista linkeistä käytetään, jolloin toinen toimii vain kun pääyhteys vikaantuu.

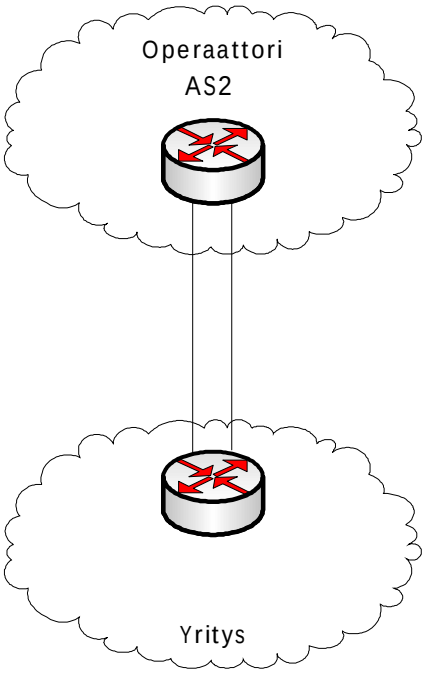
5.4 Topologioita

Internet-yhteyden kahdentamista varten tarvitaan siis BGP-protokolla ja yritykselle oma AS-numero. Seuraavaksi tulee pohtia, mikä on yrityksen ulkoinen reitityspolitiikka ja kuinka se toteutetaan. Politiikkaan kuuluu se, mitä reittejä yrityksen BGP-reitittimien halutaan ottavan vastaan ja mitä reittejä niiden halutaan mainostavan operaattorin BGP-reitittimille. Tulee myös miettiä, kuinka paljon halutaan kahdentaa ja kuinka vi-

kasietoinen verkosta halutaan. Internet-yhteyden kahdentamiseen voi käyttää erilaisia verkkotopologioita.

5.4.1 Yksikotinen tynkäverkko

Yksikotisella tarkoitetaan, että yrityksellä on vain yksi yhteys yhteen operaattoriin. Tämä topologia sisältää vain minimalistisen määrän kahdennusta, eikä sen toteuttamiseen tarvita BGP:n käyttöä. Pienet yritykset käyttävät tällaisia ratkaisuja. Internet-pääsyyn riittää operaattorin mainostama oletusreitti sisäisen reititysprotokollan avulla tai staattinen oletusreitti osoittamaan operaattorin reunareitittimeen. Kahdennettu tietoliikennelinkki suojaa vain siltä, jos toinen niistä vikaantuu. Reitittimen vikaantuessa katoaa yrityksen yhteys Internetiin. Tynkäverkolla tarkoitetaan verkkoa, johon pääsy vain yhden pisteen kautta, eli tässä tapauksessa yhden operaattorin kautta.

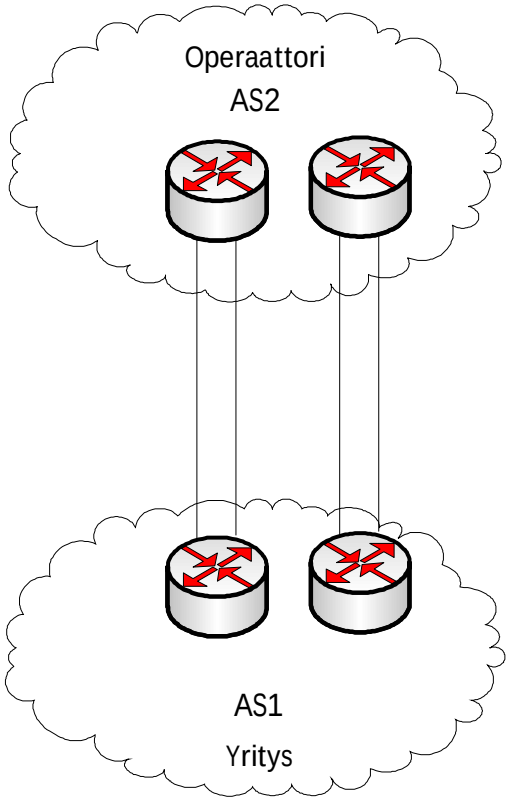


Kuva 20. Yksikotinen tynkäverkko.

5.4.2 Monikotinen tynkäverkko

Monikotisessa (Multihoming) tynkäverkossa on otettu huomioon mahdollinen operaattorin reitittimen vikaantuminen. Yritys on yhteydessä kahteen operaattorin reitittimeen ja yhden vikaantuminen ei vielä estä pääsyä Internetiin. Yrityksen puolella voi olla useampia reitittimiä eliminoimassa yhden pisteen ongelmaa. Internet-yhteys on kuitenkin yhden operaattorin varassa. Yrityksen Internet-yhteys katkeaa jos operaattorin yhtey-

det muihin järjestelmiin vikaantuu. Monesti tämä kuitenkin vaatii usean eri pisteen vikaantumista operaattorin verkossa. Monikotinen tarkoittaa sitä, että verkkoon voidaan päästä useampaa reittiä käyttäen. Monikotinen verkko voi olla myös tynkäverkko, jos se on vain yhteen operaattoriin yhteydessä, eli järjestelmästä on vain yksi ulospääsy.



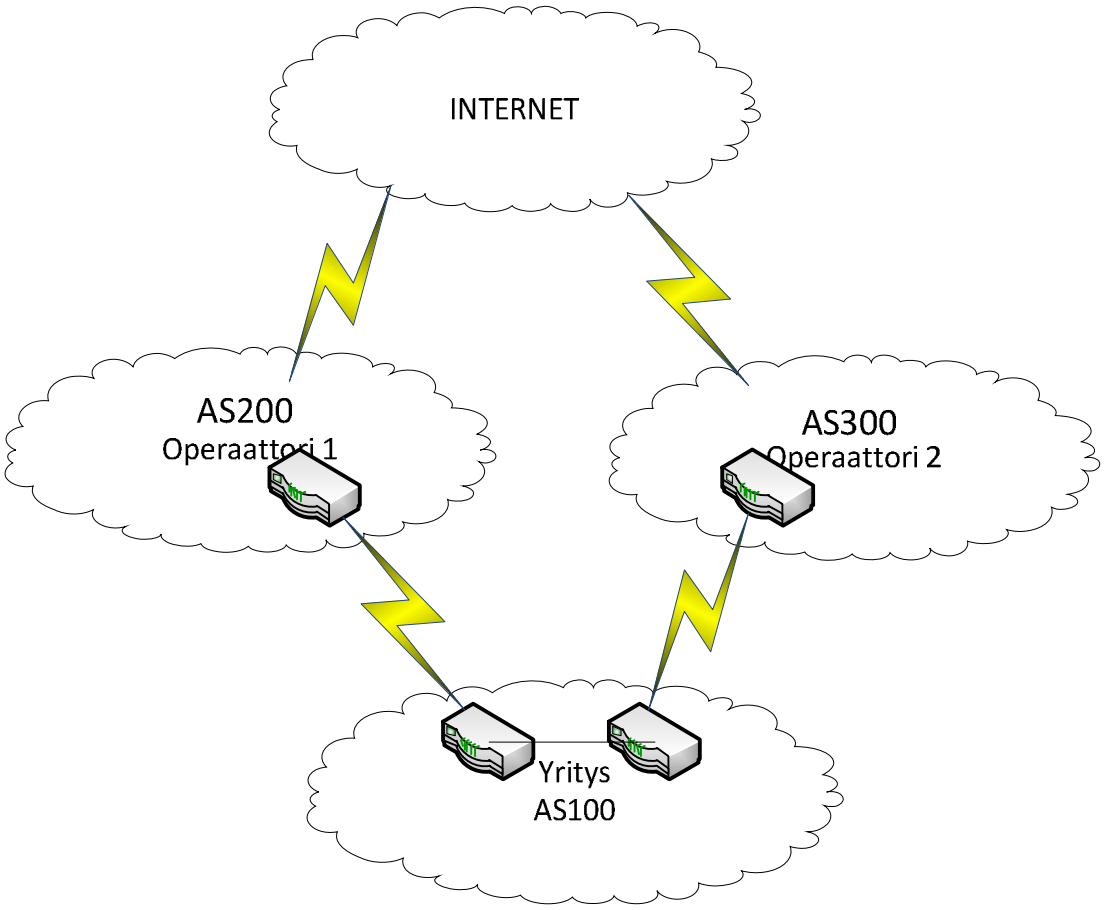
Kuva 21. Monikotinen tynkäverkko.

Tämä toteutus voi hyötyä BGP:n käytöstä. BGP:n avulla yritys voi kontrolloida, mitä linkkejä pitkin mihinkin verkkoon mennään, eli ulospäin lähtevän liikenteen kuormanjako on mahdollista. Tämä toteutus voidaan tehdä privaatteja AS-numeroita käyttäen. Operaattori näkee yrityksen BGP-reunareitittimen UPDATE-viestissä privaatin AS-numeron ja normaalikäytännön mukaan operaattori korvaa sen omalla julkisella AS-numerolla.

5.4.3 Monikotinen verkko

Monikotista verkkoa varten yritys tarvitsee julkisen AS-numeron, ja BGP:n käyttö on käytännössä pakollista. Tämän lisäksi yritys tarvitsee oman IP-osoiteavaruuden, jota käsiteltiin aikaisemmissa kappaleissa. Yrityksen BGP-reunareitittimet ovat yhteydessä kahden eri operaattorin BGP-reunareitittimiin. Yrityksen BGP-reitittimet olisi hyvä olla

iBGP-yhteydessä toisiinsa, jotta tietoa operaattoreilta saaduista reiteistä voidaan vaihtaa ja vikatilanteessa liikenne ohjataan käyttämään vain toista linkeistä. Monikotinen verkko useamman reunareitittimen tukemana on redundantein Internet-yhteyden kahdentamisen topologioista. Operaattoreihin voidaan olla useiden eri reitittimien kautta yhteydessä ja operaattoreiden määrääkin voidaan nosta useampaan kuin kahteen jos vain reitityspolitiikasta päästään sopuun. [30, s.221-229.]



Kuva 22. Monikotinen verkko.

5.5 Reitityspolitiikka

Yritys päättää itse, mitä reittejä se haluaa ottaa vastaan. Tyypillisiä reititysskenaarioita ovat pelkkä oletusreitti, oletusreitti ja tietty reittien osajoukko tai koko reititystaulu.

Pelkkä oletusreitti on helpoin toteuttaa yrityksen puolesta. Yritys ei voi valikoida reittejä tarkemmin, koska tietää vain oletusreitin muihin verkkoihin. Se myös vaikeuttaa Internet-linkkien liikenteen suunnittelua, sillä AS:n sisällä reitinvalinta tapahtuu IGP:n metriikan perusteella. Oletusreitin käyttö ei rasita BGP-reitittimiä, sillä reititystauluun tulee

vain yksi merkintä. Reittisuodatusta ei tarvitse tehdä, koska operaattorilta saadaan vain yksi reitti.

Oletusreitti ja valikoitu joukko operaattorien tuntemia reittejä antaa mahdollisuuden tarkempaan liikenteen määrittelyyn ja liikenteen ohjaamiseen eri Internet-linkkejä pitkin. Valikoidut reitit saadaan käytännössä niin, että operaattori mainostaa vain omia ja asiakkaidensa verkkoja tai niin, että operaattori mainostaa koko reititystaulun, josta halutut reitit valikoidaan eri suodatinlistoja käyttäen.

Operaattorilta voi halutessaan saada myös koko reititystaulun, mutta se on kaikkein työläin vaihtoehto yrityksen puolesta. Etuina ovat suuri määrä reittejä, joista voi aina valita kohdeverkkoon parhaimman reitin. Optimaalisin reititys on mahdollista vain jos tietää koko Internetin reititystaulun. Reitittimien prosessori ja muisti joutuvat kovan paineen alle käsitellessään suurta määrää reittejä. [35, s.249-252.]

5.6 Sisään tulevien prefiksien suodattaminen

Prefiksien suodattamisella tarkoitetaan tiettyjen verkko-osoitteiden valikoimista reitityspäivityksistä. Prefiksisuodatus on oltava määriteltynä, vaikka sisäänpäin tulevia reittejä olisikin suodatettu AS-polun tai muun valintakriteerin mukaan. Prefiksien suodattaminen tarkistaa jokaisen reitityspäivityksen ja hylkää sieltä listan määrittelemät prefiksit. Seuraavassa lista prefikseistä, jotka tulisi suodattaa sisään tulevista reitityspäivityksistä:

- RFC 1918-osoitteet, eli privaatit IP-osoitteet. Privaatteja IP-osoitteita ei pitäisi mainostaa Internetissä ja sen takia ne suodatetaan pois. Osoitealueeseen kuuluu verkot 10.0.0.0/8, 172.16.0.0/12 ja 192.168.0.0/16.
- Järjestelmän sisäiset osoitteet ovat systeemin paikallista käyttöä varten. Osoitealueeseen kuuluu verkko 127.0.0.0/8.
- Verkko 169.254.0.0/16, jota käytetään verkko-osoitteen määrittelyyn jos DHCP-palvelinta ei ole saatavilla.
- Verkko 0.0.0.0/8, verkkoa ei ole määritelty julkiseen käyttöön. Ei sisällytä oletusreittiä 0.0.0.0/0.
- Testiverkoille varattuja osoitteita ei tule jakaa Internetissä eteenpäin. Verkkoon kuuluu 192.0.2.0/24.

- D- ja E -luokan osoitteet, jotka ovat monilähetykseen (multicast) käytettäviä osoitteita. Verkot 240.0.0.0/4 ja 224.0.0.0/4.
- Oman autonomisen järjestelmän osoitteet tulee suodattaa pois saapuvista päivityksistä. Pidemmät tai yhtä pitkät prefiksit tulee suodattaa.

5.7 Uloslähtevien prefiksien suodattaminen

AS voi joutua välittämään liikennettä muille autonomisille järjestelmille, jos se mainostaa muita kuin omia reittejä ulospäin usealle eri autonomisen järjestelmän BGP-naapurille. Yritykset harvoin haluavat välittää liikennettä muille järjestelmille, joten ainoastaan yrityksen omia reittejä mainostetaan ulospäin. Suodattimista voi muodostaa useamman kerroksen ja onkin suositeltavaa käyttää useampaa suodatinta. Useamman suodattimen käyttö ehkäisee virheellisen reititystiedon vuotamisen ulos verkosta. Prefiksilistassa sattuneen virheellisen konfiguraation takia AS voi vahingossa mainostaa sille kuulumattomia verkkoja. Virheellisen tiedon leviäminen voidaan estää jos käytössä on prefiksilistan lisäksi AS-polkulista, joka sallii vain AS:n omistamien reittien mainostamisen. [30, s.229-231.]

5.8 Kuorman jakaminen

Kuorman jakaminen voi olla hyvinkin hankalaa BGP:tä käytettäessä kahden eri operaattorin välillä. BGP valitsee parhaan reitin verkkoon, eikä sitä ole suunniteltu käyttämään useampaa reittiä. BGP pystyy jakamaan kuormaa jos reittipolitiikat määritetään hyvin ja linkkien käyttöastetta tarkkaillaan. Politiikkaa muutetaan aina tarpeen mukaan ohjaamaan liikennettä linkiltä toiselle. Sisään tulevan ja uloslähtevän liikenteen politiikat ovat toisistaan riippumattomia.

Sisään tulevaa liikennettä voi pyrkiä jakamaan linkkien kesken pilkkomalla saatua osoiteavaruutta pienemmäksi ja mainostamalla pilkottuja verkkoja eri linkkejä käyttäen. Pilkkomisen tarkoituksena on saada enemmän valinnanvaraa kuormanjakoa varten. Kahta eri verkkoa mainostamalla linkkien kuormaa ei voi jakaa tarkemmin, koska on vain kaksi reittiä, joiden perusteella muut järjestelmät tekevät reitityspäätöksen. Yritys voi mainostaa pilkottuja verkkoja kumpaakin linkkiä pitkin, mutta muuttaa toista linkkiä pitkin mainostaessa reitin prioriteettia esimerkiksi lisäämällä omaa AS-numeroa AS-

polkulistaan. Pilkottujen verkkojen lisäksi tulee mainostaa koko verkon summaavaa prefiksiä molempia linkkejä pitkin, jotta yrityksen verkon tavoitettavuus muualta olisi taattu.

Pilkottujen verkkojen mainostaminen ei ole taattua, koska se on täysin operaattorin politiikoista riippuvainen asia. Operaattori voi olla hyväksymättä pilkottuja verkkoja ja sallia vain summatun verkon. On tärkeää muuttaa reittien parametreja hillitysti, koska pienelläkin muutoksella voi olla suuri vaikutus linkkien käyttöasteiden tasoittumiseen. AS-numeron lisäämisen lisäksi yritys voi koittaa hyödyntää operaattoreiden käyttämiä community-arvoja liikenteen tasaamiseksi linkkien välillä.

Verkkojen pilkkominen ja niiden mainostaminen vain yhdelle operaattorille onnistuisi, sillä yrityksen verkko on vain tämän operaattorin takana ja kaikki liikenne joutuu kulkemaan sen läpi. Spesifisiä verkko-osoitteita pystytään hyödyntämään, vaikka operaattori mainostaisi vain yrityksen verkon summattua osoitetta eteenpäin, koska operaattorin järjestelmässä valinta tehtäisiin tarkemman verkko-osoitteen perusteella. MED-arvoa voi myös pyrkiä hyödyntämään, jos yritys on vain yhteen operaattoriin yhteydessä. MED-arvolla voidaan pyrkiä vaikuttamaan operaattorin tekemiin reitityspäätöksiin ja ohjata liikennettä tasaisesti linkkien kesken. Viimeinen sana jää kuitenkin operaattorille, joka voi politiikallaan määrittää miten liikenne ohjataan asiakkaan, eli tässä tapauksessa yrityksen verkkoon.

Uloslähtevää liikennettä on helpompi jakaa linkkien kesken, paitsi jos operaattorilta saadaan vain oletusreitti. Operaattoreilta saa halutessaan suuren määrän reittejä, joita pystyy käyttämään kuorman tasaamiseen. Useat reitit takaavat sen, että kuormaa voidaan jakaa hienovaraisesti. Jokaisen saadun reitin voi määrittää halutessaan käyttämään tiettyä linkkiä. Uloslähtevää liikennettä voidaan jakaa linkkien kesken esimerkiksi vaikuttamalla reittien Local-pref-arvoon. [30, s.231-233.]

5.9 Yliheitto ja testaaminen

Internet-yhteyden toiminta tulee testata kun asennus on saatu valmiiksi. Käytännössä tämä tarkoittaa yhteyden toiminnan testaamista, kun tietyt linkit ajetaan alas. Alasajon jälkeen tarkastellaan siirtyykö liikenne varareitille suunnitellusti. Tärkeimmät testattavat kohteet ovat Internet-linkit sekä yrityksen BGP-reitittimien väliset linkit. Järjestelmä

voidaan siirtää tuotantokäyttöön, kun testit ovat osoittautuneet positiivisiksi ja kaikki toimii suunnitellusti.

Yrityksen tulee varata aikaa yliheittoon kun vanhoista IP-osoitteista siirrytään uusiin. Vanha yhteys tulee säilyttää uuden rinnalla, jotta vanhoja IP-osoitteita voidaan käyttää. Kaiken vaihtaminen kerrallaan ei tule onnistumaan helposti, eikä siihen ole mitään syytä ryhtyä. Siirto uusiin osoitteisiin tulee tapahtua vaiheittain.

Yrityksen uusi Internet-reuna-arkkitehtuuri rakennetaan vanhan yhteyden rinnalle. Uusi arkkitehtuuri konfiguroidaan heti käyttämään uusia osoitteita

DMZ-alueella (demilitarized zone) sijaitsevat yrityksen palvelimet, jotka näkyvät Internetiin. Näillä palvelimilla on julkiset IP-osoitteet, joiden avulla ne kommunikoivat ulkomaailmaan. DMZ-alueen palvelimet kannattaa siirtää yksitellen uusien IP-osoitteiden alle. Vanhan DMZ:n rinnalle tulee luoda uusi DMZ-alue, joka käyttää siis uusia julkisia IP-osoitteita.

Yliheittoa tehdessä tulee ottaa huomioon, että nimenselvitys uusille IP-osoitteille on kunnossa. Nimipalvelulle tulee ilmoittaa uudet IP-osoitteet ja palvelinten nimet, jotka niitä käyttävät. Siirtymävaiheessa voidaan muuttaa NAT:lla (Network Address Translation) vanhoilla IP-osoitteilla tulleet yhteyspyynnöt käyttämään uusia IP-osoitteita. Tämä siksi, että kaikki nimipalvelut eivät välttämättä saa uusinta tietoa käyttöönsä, ja sen seurauksena liikennettä voi vielä tulla vanhaa IP-osoitetta käyttäen.

Kaikki vanha IP-osoitteistus tulee vaihtaa. Julkisia IP-osoitteita käytetään palvelimien lisäksi mm. palomuureilla, VPN-tunneleissa, NAT-säännöissä ja reitittimen välisillä linkeillä. Palomuurien sääntökannat tulee päivittää vastaamaan nykytilannetta. Päivitettäviä asioita ovat mm. vanha julkinen IP-osoitteistus, NAT-säännöt, jotka käyttävät vanhoja julkisia IP-osoitteita ja palomuurisäännöt, joissa pääsy on annettu vanhoja osoitteita käyttäen. VPN-laitteiden ja –tunneleiden IP-osoitteistus tulee myös vaihtaa. Lisäksi on otettava huomioon, että VPN-tunneleita muutettaessa on huolehdittava myös toisen pään konfiguroinnin muuttamisesta samanaikaisesti. Tunnelin toisen pään konfigurointi on asiakkaan vastuulla, ja heihin tulee olla yhteydessä, kun vaihto suoritetaan. Vanhan VPN-laitteistuksen rinnalle olisi hyvä saada myös uuteen verkkoon vastaava

kokoonpano, jotta tunnelit voidaan siirtää yksikerrallaan uuteen järjestelmään. Jokainen tunneli joudutaan siirtämään kerralla, jos rinnalla ei ole toista VPN-laitteistoa. Yrityksen kannattaa uusia vanha VPN-laitteisto Internet-yhteyttä kahdentaessa. Rinnakkainen järjestelmä helpottaa siirtoa ja mahdollistaa tunneleiden siirron yksi kerrallaan.

Yrityksellä voi olla myös käytössä palveluita, joihin pääsy on annettu käyttämällä yrityksen julkista IP-osoitetta. Näihin palveluihin tulee myös ilmoittaa uudet käytössä olevat IP-osoitteet, jotta palvelut toimivat, kun IP-osoitteet on lopullisesti vaihdettu.

Kaikki muutokset tulee dokumentoida ja vanhat IP-osoitteisiin liittyvät dokumentit päivittää. Internet-yhteyden kahdentamiseen liittyvä yliheitto vaatii paljon mekaanista työtä ja yliheitto viekin suurimman osan projektiin käytettävästä ajasta.

6 Esimerkkikonfiguraatio

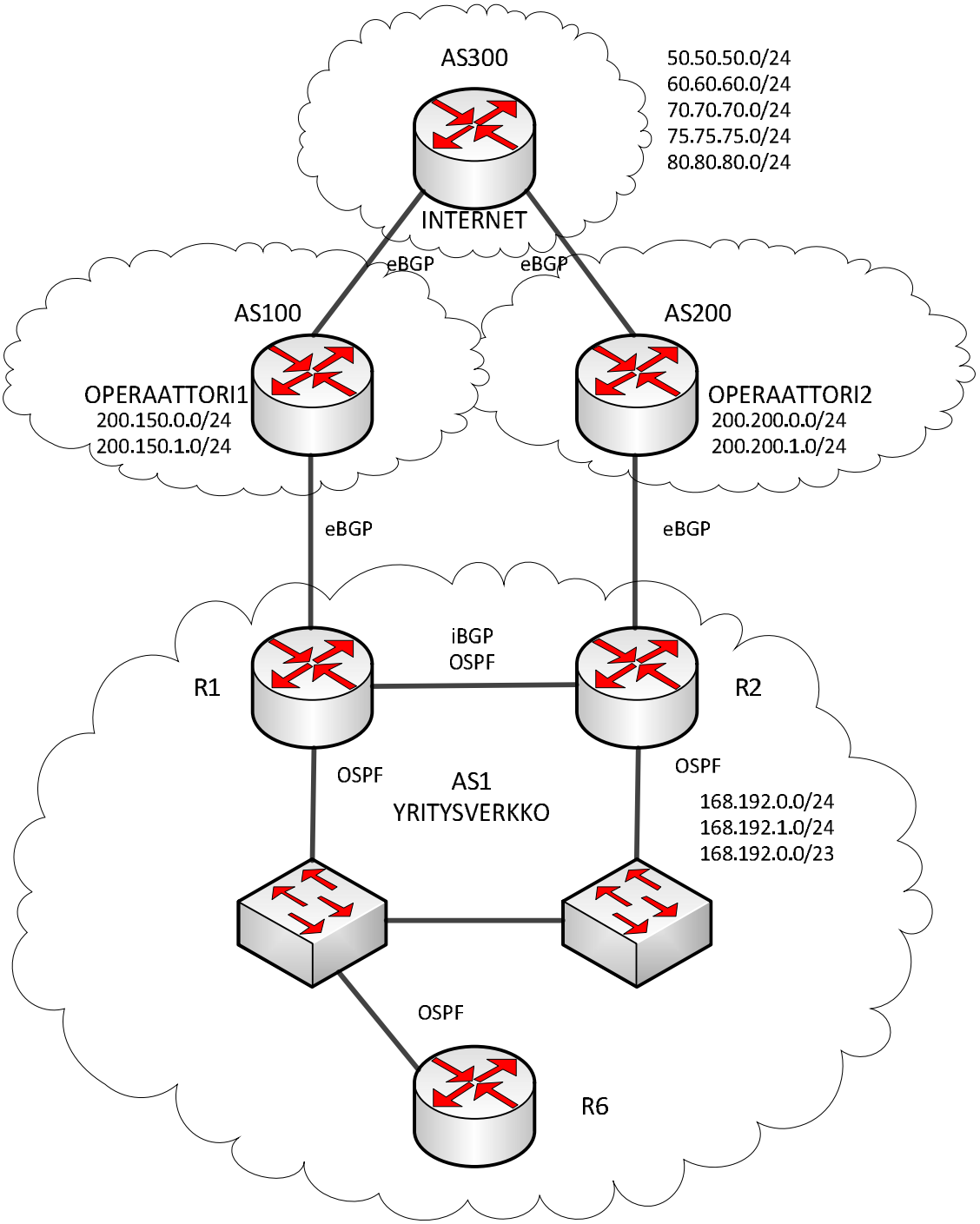
Seuraavassa on esimerkkikonfiguraatio kahdennetusta Internet-yhteydestä yrityksen kannalta. Esimerkissä operaattoreiden konfiguraatiot ovat pelkistettyjä ja niiden ainoa tehtävä on tarjota BGP-yhteys järjestelmien välillä. Tämän lisäksi operaattorit syöttävät BGP-reititykseen joitakin reittejä, joiden attribuutteja yrityksen BGP-reitittimet muokkaavat. Operaattorit eivät syötä yritykselle oletusreittiä BGP:n kautta. Esimerkki tehtiin verkkosimulaatio-ohjelmistolla GNS3.

6.1 Topologia

Topologioita on erilaisia ja tämä on vain yksi esimerkki siitä, kuinka Internet-yhteys voitaisiin kahdentaa. Reunareitittimien olisi hyvä sijaita maantieteellisesti eri paikoissa ja ulkoisten yhteyksien olisi hyvä olla eriytettyinä eri kaapelivienteihin. Tietoliikenteessä käytettävät valokuidut saattavat mennä samassa putkessa ja sen takia olisikin hyvä, jos useamman käytettävän yhteyden tietoliikennekanavat saataisiin käyttämään eri fyysistä reittiä.

Kuvassa 22 on esillä verkon aktiivilaitteet, autonomiset järjestelmät, linkit sekä verkot, joita mainostetaan BGP-prosessiin. Kuvan 22 reitintä R6 voidaan pitää esimerkiksi

kahdennettuna palomuurilaitteistona, joka sijaitsee verkon reunalla. Kahdennettu palomuuri on siis korvattu reitittimellä tässä topologiassa.



Kuva 22. Esimerkkitopologia.

Yritysverkon sisäisenä reititysprotokollana toimii OSPF, joka välittää AS1 reititinten välillä tiedon järjestelmässä käytettävistä IP-osoitteista järjestelmän sisällä. OSPF tarjoaa oletusreitin ulos yritysverkosta. Reitittimet R1 ja R2 jakavat OSPF-prosessiin oletusrei-

tin, joka esimerkissä välittää reitittimelle R6. Reititin R6 voidaan mieltää kahdennetuksi palomuuriksi, jonka takana yrityksen sisäverkko ja muut verkot sijaitsevat. Kahdennettu palomuuri olisi kahdennettujen verkkokorttien kautta yhteydessä molempiin kuvan 22 kytkimiin. Esimerkissä reititin R6 on vain toiseen kytkimistä yhteydessä, jolloin kahdennus ei yllä R6:lle asti, jos siihen menevä ainoa linkki katkeaa. Verkon kytkimet tarjoavat vaihtoehtoisen reitin linkkivikojen sattuessa. Linkkejä ei ole kahdennettu tietoliikennelaitteiden välillä. Esimerkissä näkyvän yritysverkon tietoliikennelaitteistoa voidaan pitää Internet-reuna-arkkitehtuurina.

Yritysverkko on BGP:n kautta yhteydessä kahteen eri operaattoriin. Operaattorit eivät suodata liikennettä millään tavalla. Esimerkissä reitittimet R1 ja R2 muokkaavat operaattoreilta ja muualta Internetistä tulleita reittejä. Reittien attribuutteja muokataan niin, että kuorma jaetaan karkeasti linkkien ylitse.

6.2 Naapurimääritykset

Naapurimääritykset aloitetaan määrittelemällä BGP-prosessi, jonka jälkeen naapurisuhteet määritetään neighbor-komentoa käyttäen. Esimerkissä käytetään BGP-ryhmiä reitittimillä R1 ja R2 naapurisuhteiden määrittelyssä. Reitittimien käytössä on kaksi eri ryhmää IBGP ja EBGP. IBGP-ryhmä on sisäisille BGP-naapureille ja EBGP-ryhmä on käytössä ulkoisille naapureille. Reitityspolitiikka on sama AS100 ja AS200 kautta tuleville reiteille, joten määritykset ovat käytännössä samat reitittimien R1 ja R2 välillä.

```
R1(config-router)#neighbor 172.26.1.200 peer-group IBGP
R1(config-router)#neighbor IBGP peer-group
R1(config-router)#neighbor IBGP remote-as 1
R1(config-router)#neighbor IBGP update-source Loopback0
R1(config-router)#neighbor IBGP version 4
R1(config-router)#neighbor IBGP next-hop-self
R1(config-router)#no synchronization
```

Reititin R1 määrittelee iBGP-naapurinsa, R2:n, käyttäen ryhmää IBGP. R1 ja R2 käyttävät loogisen portin, loopback0, IP-osoitetta BGP-yhteyden muodostamiseen. R1 solmii

naapurisuhteen R2:n loogisen portin IP-osoitteeseen ja mainostaa R2:lle BGP-viestejä omasta loogisesta portista. Reitittimet R1 ja R2 sijaitsevat samassa järjestelmässä, AS1, ja käyttävät BGP:n versiota 4. Reitittimet käyttävät BGPv4:sta oletusarvoisesti, eikä sitä tarvitse määrittää erikseen konfiguraatioissa. R1 ja R2 käyttävät omaa BGP-osoitettaan, kun ne mainostavat eBGP-naapurilta opittuja reittejä sisäverkkoon. Synkronointi on otettu pois käytöstä, sillä BGP-reittejä ei haluta jakaa sisäisen reititysprotokollan prosessiin, koska AS1 ei välitä tietoliikennettä muille järjestelmille.

Vastaavat konfiguraatiot löytyvät myös reittimeltä R2, jossa ne eroavat ainoastaan kätetyn IP-osoitteen puolesta.

6.3 Sisäverkon reititys

OSPF-reititys on tehty esimerkissä yksinkertaiseksi. Kaikki yritysverkon reitittimet sijaitsevat OSFP:n alueella 0, joka toimii OSPF-reitityksessä runkoverkkona. R1 ja R2 jakavat OSPF-prosessiin oletusreitin. OSPF-reititys aktivoidaan jokaiselle järjestelmän sisäiselle verkolle, jotta OSPF-prosessin kautta pystytään tavoittamaan jokainen verkon IP-osoite. R1 ja R2 mainostavat myös omien loogisten porttien IP-osoitteita, joiden mainostaminen on tärkeää BGP-naapurussuhteen solmimisen kannalta.

```
R1(config-router)#network 10.0.0.0 0.0.0.3 area 0
R1(config-router)#network 10.10.10.0 0.0.0.255 area 0
R1(config-router)#network 10.100.100.0 0.0.0.255 area 0
R1(config-router)#network 168.192.0.1 0.0.0.0 area 0
R1(config-router)#network 172.26.1.100 0.0.0.0 area 0
R1(config-router)#default-information originate always
```

Reititys on aktivoitu tarkkoja maskeja käyttäen. Sen voisi myös tehdä käyttämällä luokallisia maskeja, jolloin komentojen määrää voisi hieman supistaa. Konfiguraatio määrittelee myös, että oletusreitti jaetaan aina, vaikka reititin ei itse omistaisi oletusreittiä.

6.4 EBGP-määritys

Ulkoiset BGP-naapurit määritetään käyttämällä fyysisen portin IP-osoitetta. Ulkoiselle BGP-naapurille luodaan vastaavasti BGP-ryhmä, kuten tehtiin myös iBGP-naapurille.

```
R1(config-router)#neighbor EBGP peer-group
R1(config-router)#neighbor EBGP remote-as 100
R1(config-router)#neighbor 10.0.1.2 peer-group EBGP
R1(config-router)#network 10.100.100.0 mask 255.255.255.0
R1(config-router)# network 168.192.0.0 mask 255.255.255.0
R1(config-router)# network 168.192.1.0 mask 255.255.255.0
R1(config-router)# aggregate-address 168.192.0.0 255.255.254.0
```

AS1 omistaa verkon 168.192.0.0/23, mutta haluaa mainostaa tämän verkon lisäksi myös saman verkon prefiksejä tarkemmalla maskilla. BGP-prosessiin syötetään verkon 168.192.0.0/24, 168.192.1.0/24, 10.100.100.0/24. Tämän lisäksi R1 ja R2 mainostavat summattua reittiä 168.192.0.0/23, joka koostuu verkoista 168.192.0.0/24 ja 168.192.1.0/24. Käytännössä saman olisi voinut tehdä network-komentoa käyttäen. Verkko 10.100.100.0/24 on syötetty BGP-prosessiin vain testin vuoksi. Kahta tai useampaa verkkoa mainostetaan siksi, että voitaisiin jakaa tuleva liikennettä linkkien kesken. AS1 haluaa mainostaa vain verkkoja 168.192.0.0/24 ja 168.192.1.0/24 ulospäin. Tämä onnistuu suodatustekniikoita käyttäen.

6.5 Reititystietojen muokkaaminen ja suodattaminen

AS1 haluaa mainostaa ulos vain omia verkkojaan. AS1:n määrittelemä politiikka kieltää AS200:n BGP-prosessiin injektoimien reittien hyväksymisen, mutta kaikki muu kelpuutetaan. AS1 tasaa Internet-linkkien kuormaa Local Pref -arvoa käyttäen, kun liikenne lähtee ulos järjestelmästä. AS1 jakaa kuormaa Internet-linkkien kesken AS-polkua muokkaamalla, jonka avulla voidaan vaikuttaa sisään tulevan liikenteen käyttäytymiseen.

Suodatus tapahtuu kahdella eri tasolla - prefiksilistalla ja AS-path-listalla. Useamman suodattimen käyttö tekee reitityspolitiikan toteuttamisesta varmempaa. Reittitietojen

on läpäistävä molemmat suodattimet, jotka ovat esimerkkiverkossa AS-path-lista ja prefiksilista.

```
R1(config)#ip prefix-list TOEBGP seq 5 permit 168.192.0.0/23 le 24
R1(config)#ip prefix-list TOEBGP seq 10 deny 0.0.0.0/0 le 32
```

AS1:n reitittimien käyttämä prefiksilista *TOEBGP* määrittelee, että prefiksin 168.192.0.0/23-24, mainostaminen ulos järjestelmästä sallitaan ja loput prefiksit kielletään. Verkko 168.192.0.0/23 on AS1:n omistama verkko ja vain sitä sekä sen tarkempia prefiksejä halutaan mainostaa eBGP-naapureille.

```
R1(config)#ip as-path access-list 10 permit ^$
```

AS-path-lista 10 määrittelee, että vain järjestelmän sisällä BGP-prosessiin syötetyt verkot sallitaan.

```
R1(config)#route-map PREPEND permit 10
R1(config-route-map)# match ip address prefix-list PREPENDPREFIX
R1(config-route-map)#set as-path prepend 1 1 1
R1(config)#route-map PREPEND permit 15

R1(config)#ip prefix-list PREPENDPREFIX seq 5 permit 168.192.0.0/24
```

Lähtevään liikenteeseen liitetään route map *PREPEND,* joka käyttää muokattavien prefiksitietojen valintaan prefiksilistaa *PREPENDPREFIX.* Route map muokkaa valintakriteerit täyttävien reittien AS-polkua niin, että R1 asettaa AS-polkuun oman AS-numeronsa kolme kertaa, jolloin AS-polun pituus kasvaa. AS-polun pituutta muuttamalla voidaan vaikuttaa muiden järjestelmien reitityspäätöksiin, jos ne eivät muokkaa reititystietoihin liittyviä muita polun attribuutteja. Normaalitilanteessa reiteistä valitaan se, jolla on lyhkäisin AS-polun pituus. R2 muokkaa prefiksien 168.192.1.0/24 ja 168.192.0.0/23 AS-polkun pituutta lisäämällä polun loppuun oman AS-numeronsa kolmeen kertaan. Näkymä reitittimen INTERNET reititystaulusta AS-polun muokkaamisen jälkeen:

```
   Network          Next Hop    Metric  LocPrf  Weight  Path
*> 168.192.0.0/24   10.0.4.1                    0       200 1 i
*> 168.192.0.0/23   10.0.3.1                    0       100 1 i
*> 168.192.1.0/24   10.0.3.1                    0       100 1 i
```

Tulosteesta käy ilmi, että AS1:n mainostamiin verkkoihin käytetään kahta eri polkua. AS100:n kautta kulkee AS1:n prefiksit 168.192.0.0/23 ja 168.192.1.0/24, koska R1 ei ole lisännyt näitä verkkoja koskeviin päivityksiin AS-polun pituutta. R1 on suotuisampi reitti, koska AS-polun pituus on lyhyempi. Vastaavasti prefiksiin 168.192.0.0/24 kuljetaan AS200:n kautta, koska R2 ei lisännyt verkkoprefiksiä koskevaan päivitykseen AS-polun pituutta. Seuraavassa ote operaattorin reititystaulusta, jossa AS-polun muokkaaminen näkyy selkeämmin.

```
   Network          Next Hop    Metric  LocPrf  Weight  Path
*> 168.192.0.0/24   10.0.3.2                    0       300 200 1 i
*                   10.0.1.1                0   0       1 1 1 1 i
*> 168.192.0.0/23   10.0.1.1                0   0       1 i
*> 168.192.1.0/24   10.0.1.1                0   0       1 i
```

R1 muokkaa verkon 168.192.0.0/24 AS-polkua, mutta R2 ei. Tästä seuraa se, että OPERAATTORI1 reitittää kyseiseen verkkoon menevän liikenteen reitittimen INTERNET kautta, koska R1:ltä saatu polku on pidempi. Muut AS1:n mainostamat verkot reititetään R1:n kautta.

Saapuvaa liikennettä suodattava AS-path-lista 20 määrittelee, että AS200:n BGP-prosessiin syöttämiä reittejä ei haluta ottaa vastaan, mutta kaikki muu kelpuutetaan.

```
R1(config)#ip as-path access-list 20 deny _200$
R1(config)#ip as-path access-list 20 permit .*
```

Saapuvaa liikennettä suodatetaan lisäksi prefiksilistalla *FROMEBGP*, joka suodattaa saapuvista reiteistä pois privaatit verkot, monilähetykseen varatut osoitteet ja muut Internet-reitityksessä kielletyt osoitteet.

```
R1(config)#ip prefix-list FROMEBGP seq 5 deny 0.0.0.0/8 le 32
R1(config)#ip prefix-list FROMEBGP seq 10 deny 10.0.0.0/8 le 32
R1(config)#ip prefix-list FROMEBGP seq 15 deny 172.16.0.0/12 le 32
R1(config)#ip prefix-list FROMEBGP seq 20 deny 192.168.0.0/16 le 32
R1(config)#ip prefix-list FROMEBGP seq 25 deny 127.0.0.0/8 le 32
R1(config)#ip prefix-list FROMEBGP seq 30 deny 169.254.0.0/16 le 32
R1(config)#ip prefix-list FROMEBGP seq 35 deny 192.0.2.0/24 le 32
R1(config)#ip prefix-list FROMEBGP seq 40 deny 224.0.0.0/3 le 32
R1(config)#ip prefix-list FROMEBGP seq 50 deny 172.160.0.0/16 le 32
R1(config)#ip prefix-list FROMEBGP seq 55 permit 0.0.0.0/0 le 32
```

Lista on vain esimerkki, eikä se sisällä täydellistä tietoa kiellettävistä osoitteista. Vastaavia listoja on nähtävissä eri organisaatioiden Internet-sivuilla. Listat ovat julkista tietoa ja ne edistävät turhan reititystiedon karsimista BGP-reitityksestä.

AS1 politiikka määrittää, että saapuvan liikenteen reittien attribuutteja muokataan, jotta lähtevää liikennettä voidaan jakaa linkkien kesken.

```
R1(config)#route-map LOCALPREFIN permit 5
R1(config-route-map)#match ip address prefix-list LOCPREFIN
R1(config-route-map)#set local-preference 300
R1(config)#route-map LOCALPREFIN permit 10
```

```
R1(config)#ip prefix-list LOCPREFIN seq 5 deny 50.50.50.0/24
R1(config)#ip prefix-list LOCPREFIN seq 10 deny 60.60.60.0/24
R1(config)#ip prefix-list LOCPREFIN seq 15 permit 70.70.70.0/24
R1(config)#ip prefix-list LOCPREFIN seq 20 permit 80.80.80.0/24
```

Ulkoisilta BGP-naapureilta tuleviin BGP-viesteihin liitetään route map *LOCALPREFIN*, joka käyttää muokattavien prefiksitietojen valintaan prefiksilistaa *LOCPREFIN*. Route map muokkaa valintakriteerit täyttävien reittien Local Pref -arvoa niin, että R1 asettaa verkoille 70.70.70.0/24 ja 80.80.80.0/24 arvon 300. Verkkoja 50.50.50.0/24 ja 50.50.50.0/24 ei muokata, vaan ne saavat oletusarvona Local Pref -arvon 100. R2

asettaa reiteille 50.50.50.0/24 ja 60.60.60.0/24 Local Pref -arvon 200. Reitittimen R1 reititystaulun näkymä koskien muokattavia verkkoja:

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i50.50.50.0/24	172.26.1.200	0	200	0	200 300 ?
*	10.0.1.2			0	100 300 ?
*>i60.60.60.0/24	172.26.1.200	0	200	0	200 300 ?
*	10.0.1.2			0	100 300 ?
*> 70.70.70.0/24	10.0.1.2		300	0	100 300 ?
*> 80.80.80.0/24	10.0.1.2		300	0	100 300 ?

Tulosteesta käy ilmi, että verkot 50.50.50.0/24 ja 60.60.60.0/24 kulkevat AS200:n kautta, jonka BGP-yhteyden IP-osoite on seuraavan hypyn osoitteena. Verkot 70.70.70.0/24 ja 80.80.80.0/24 kulkevat AS100:n kautta.

Politiikan määrittelemät suodattimet on vielä lisättävä naapurimäärityksiin.

```
R1(config)#neighbor EBGP prefix-list FROMEBGP in
R1(config)#neighbor EBGP prefix-list TOEBGP out
R1(config)#neighbor EBGP route-map LOCALPREFIN in
R1(config)#neighbor EBGP route-map PREPEND out
R1(config)#neighbor EBGP filter-list 20 in
R1(config)#neighbor EBGP filter-list 10 out
```

6.6 Virhetilanteesta selviytyminen

Linkin katkeaminen AS1:n sisäverkon puolella ei vaikuta BGP-reititykseen, mutta se saattaa aiheuttaa lyhyen katkoksen sisäverkon päätelaitteille, jotka haluaisivat keskustella Internetissä olevan laitteen kanssa. Katkoksen pituus riippuu käytössä olevasta tekniikasta. OSFP:ssä rajoittava tekijä on laskurit, joiden mukaan naapuri määritetään kuolleeksi, ja jonka jälkeen verkko voi konvergoitua.

Tärkeintä on se, että järjestelmän iBGP-reitittimet pystyvät vaihtamaan BGP-viestejä ja säilyttämään yhteyden. Tärkeää on myös yhteyden säilyttäminen muualle sisäverk-

koon. On vaarana, että syntyy kaksi eri BGP-aluetta, jos esimerkiksi jos R2:n molemmat sisäverkon puoleiset linkit poikkeisivat. Seurauksena oli se, että R2 mainostaisi järjestelmän sisäisiä verkkoja, vaikka se ei olisikaan niihin yhteydessä. Siitä taas saattaa aiheutua mustia aukkoja BGP-reitityksessä, jos R2:n kautta kulkevat reitit ovat ensisijaisia reittejä autonomiseen järjestelmään AS1. Esimerkkitopologiassa annetuilla konfiguraatioilla verkko 168.192.0.0/24 kulkee R2:n kautta. Seurauksena on kaiken liikenteen katoaminen kyseiseen verkkoon pyrittäessä.

Linkin katkeaminen välillä R2-OPERAATTORI2 estää hetken verkkoon 168.192.0.0/24 menevän liikenteen. Liikenne ohjataan reitittimen R1 kautta, kun BGP havaitsee linkin R2-OPERAATTORI2 katkenneen ja konvergoituu tämän jälkeen. Seuraavassa tuloste reitittimen INTERNET reititystaulusta, kun edellä kuvattu on tapahtunut.

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 168.192.0.0/24	10.0.3.1			0	100 1 1 1 1 i
*> 168.192.0.0/23	10.0.3.1			0	100 1 i
*> 168.192.1.0/24	10.0.3.1			0	100 1 i

Tulosteesta käy ilmi, että kaikki liikenne on siirtynyt käyttämään R1:n kautta kulkevaa linkkiä. Vastaavasti AS1 lähettää kaiken Internet-liikenteen R1:n kautta.

Testit suoritettiin tarkkailemalla ping-pakettien katoamista reitittimillä R1 ja R6, kun linkkejä katkaistiin. Testit tulisi suorittaa jokaiselle linkille, tietoliikennelaitteelle ja ottaen huomioon kaikki erilaiset virheskenaariot. Edellinen testi oli esimerkki yksinkertaisesta tapauksesta ja sen tuloksista. Kaikkia testejä ei ole mielekästä raportoida, sillä virhekombinaatioita voi olla lukuisia. Testin tuloksista kuitenkin selviää, että BGP selviytyy ja osaa ohjata liikenteen toiselle linkille, kun yksi linkeistä katkeaa.

7 Yhteenveto

Työn tavoitteet täytettiin ja Helsingin Energialle saatiin toimitettua kahdennettu Internet-yhteys. Yhteys on tuotantokäytössä, mutta yliheittoon liittyvät työt ovat vielä käynnissä.

Työssä opin tuntemaan BGP-protokollan käyttäytymistä syvemmin ja sain paremman käsityksen Internetin rakenteesta sekä BGP-reitityspolitiikoista. Kahdentaminen ja BGP-reititys voidaan toteuttaa monella eri tapaa ja jokaiselle yritykselle löytyy omansa.

Internet-yhteyden kahdentaminen on helppo tapa nostaa yrityksen palveluiden tavoitettavuutta ja saatavuutta. Kahdentaminen ei välttämättä ole iso työ, mutta yliheitto ja asiaan kuuluva dokumentointi syö paljon aikaa. Kahdentamiseen tulisi kiinnittää enemmän huomiota ja käytännössä jokaisen yrityksen kannattaisi kahdentaa Internet-yhteytensä jollakin tapaa.

Lähteet

1 Graham, Buck. 2000. Tcp/Ip Addressing: Designing and optimizing your IP addressing scheme. Morgan Kaufmann.

2 H. Jonathan, Chao & Bin, Liu. 2007. High Performance Switches And Routers. Wiley-IEEE Press.

3 Doyle, Jeff & Carroll, Jennifer. 2005. Routing TCP/IP. Cisco Press

4 Pastor-Satorras, Romualdo & Vespiqnani, Alessandro. 2004. Evolution and Structure of the Internet: A Statistical Physics Approach. Cambridge University Press.

5 Chinoy, Bilal. 1992. Dynamics of Internet Routing Information. Verkkodokumentti. <http://www.caida.org/publications/papers/1992/diri/route-dynam.pdf>. Cooperative Association for Internet Data Analysis. Päivitetty Syyskuussa 1992. Luettu 10.4.2012.

6 Broido, A. & Claffy, K. 2001. Complexity of Global Routing Policies. Verkkodokumentti. <http://www.caida.org/publications/papers/2001/CGR/cgr.pdf>. Cooperative Association for Internet Data Analysis. Päivitetty Kesäkuussa 2001. Luettu 10.4.2012.

7 Hawkinson, J. 1996. RFC 1930, Guidelines for Creation, Selection, and Registration of an Autonomous System (AS).

8 Uijterwaal, Henk & Wilhelm, Rene. 2005. ANS Missing In Action: A Comparison of RIR Statistics and RIS Reality. Verkkodokumentti. <http://www.ripe.net/ripe/docs/ripe-353>. RIPE. Päivitetty Syyskuussa 2005. Luettu 14.4.2012

9 Huston, Geoff. 2006. Exploring Autonomous System Numbers. Verkkodokumentti. <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html>. The Internet Protocol Journal - Volume9, Number 1. Päivitetty Maaliskuussa 2006. Luettu 13.4.2012.

10 Verkkodokumentti. 2011. RIPE Info Sheet. <http://www.ripe.net/lir-services/ncc/infosheet.pdf>. Päivitetty 6.1.2011. Luettu 13.4.2012.

11 Blokzijl, R., Lindqvist, K. & Yilmaz, F. 2010. Policy Development Process in RIPE. Verkkodokumentti. <http://www.ripe.net/ripe/docs/ripe-500>. RIPE. Päivitetty Syyskuussa 2010. Luettu 14.4.2012

12 Alaettinoglu, C., Villamizar, C., Gerich, E., Kssens, D., Meyer, D., Bates, T., Karrenberg, D. & Terpstra, M. 1999. RFC 2622, Routing Policy Specification Language (RPSL).

13 Meyer, D., Schmitz, J., Orange, C., Prior, M. & Alaettinoglu, C. 1999. RFC 2650, Using RPSL in Practice.

14 APNIC, ARIN, LACNIC, RIPE NCC. 2005. Internet Assigned Numbers Authority (IANA) Policies for Allocation of IPv4 Blocks to Regional Internet Registries. Verkkodokumentti. <http://www.ripe.net/ripe/docs/ripe-344>. RIPE. Päivitetty Huhtikuussa 2004. Luettu 14.4.2012.

15 Afrinick, APNIC, ARIN, LACNIC, RIPE NCC. 2006. Assigned Numbers Authority (IANA) Policy For Allocation of IPv6 Blocks To Regional Internet Registries. Verkkodokumentti. < http://www.ripe.net/ripe/docs/ripe-376>. RIPE. Päivitetty Huhtikuussa 2006. Luettu 16.4.2012.

16 Carr, B., Sury, O., Martinez, J., Davidson, A., Evans, R., Yilmaz, F. & Wijte, I. 2009. IPv6 Address Allocation and Assignment Policy. Verkkodokumentti. <http://www.ripe.net/ripe/docs/ripe-481>. RIPE. päivitetty Syyskuussa 2009. Luettu 15.4.2012.

17 Shahbazian, E. 2008.Aspects of Network and Information Security. IOS Press

18 Rekhter, Y. 1993. RFC 1518, An Architecture for IP Address Allocation with CIDR.

19 RIPE NCC. 2010. IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region. Verkkodokumentti. <http://www.ripe.net/ripe/docs/ripe-498>. RIPE. Päivitetty Lokakuussa 2010. Luettu 13.4.2012.

20 Braun, H., Ford, P. & Rekhter, Y. 1993. CIDR and the evolution of the Internet. Verkkodokumentti. <http://www.caida.org/publications/papers/1993/cei/inet93.cidr.pdf>. Päivitetty Maaliskuussa 1993. Luettu 14.4.2012.

21 Fuller, V., Li, T., Yu, J. & Varadhan, K. 1993. RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy.

22 Hubbard, K., Kosters, M., Conrad, D., Karrenber, D. & Postel, J. 1996. RFC 2050, Internet Registry IP Allocation Guidelines.

23 Shakkottai, S., Fomenkov, M., Koga, R., Krioukov, D. & Claffy, K. 2010. Evolution of the Internet AS-Level Ecosystem. Verkkodokumentti. <http://www.caida.org/publications/papers/2010/AS_evolution/AS_evolution.pdf>. Päivitetty Maaliskuussa 2010. Luettu 15.4.2012.

24 FICIX. Verkkodokumentti. <http://www.ficix.fi/tekniikka.php>. Luettu 16.4.2012

25 Rekhter, Y., Li, T. & Hares, S. 2006. RFC 4271, A Border Gateway Protocol 4 (BGP-4).

26 Beijnum, Iljitsch. 2002. Building Reliable Network with the Border Gateway Protocol. O´Reilly Media.

27 Castelli, Matthew J. 2001. Network Consultants Handbook . Cisco Press.

28 Chen, E. 2000. RFC 2918, Route Refresh Capability for BGP-4.

29 Medhi, Deepankar. 2007. Network Routing: Algorithms, Protocols, And Architectures. Morgan Kaufmann.

30 Zhang, Randy. 2003. Bgp Design and Implementation. Cisco Press.

31 Rekhter, Y. & Li, T. 1995. RFC 1771, A Border Gateway Protocol 4 (BGP-4).

32 Cisco BGP Commands. Verkkodokumentti. <http://www.cisco.com/en/US/docs/ios/12_1/iproute/command/reference/1rdbgp.html#wp1021824>. Cisco. Luettu 18.4.2012.

33 BGP Best Path Selection Algorithm. Verkkodokumentti. < http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094431.shtml>. Cisco. Luettu 18.4.2012.

34 Sedayao, Jeff. 2001. Cisco Ios Access Lists. O´Reilly Media.

35 Conlan, Patrick J. 2009. Cisco Network Professional's Advanced Internetworking Guide (CCNP Series). Sybex.

36 BGP Case Studies. Verkkodokumentti. <http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c95bb.shtml#synch>. Cisco. Luettu 16.4.2012.

37 Parkhurst, William R. 2001. Cisco BGP-4 Command and Configuration Handbook. Cisco Press

38 Odom, W., Healy, R. & Donohue, D. 2009. CCIE Routing and Switching Certification Guide. Cisco Press.

39 Oppenheimer, Priscilla. 2010. Top-Down Network Design. Cisco Press

R1 konfiguraatio

```
R1#sh run
Building configuration...

Current configuration : 3431 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!

no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
```

```
!
interface Loopback0
 ip address 172.26.1.100 255.255.255.255
!
interface Loopback1
 ip address 10.100.100.1 255.255.255.0
!
interface Loopback2
 ip address 168.192.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 10.0.1.1 255.255.255.252
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.255 area 0
 network 10.100.100.0 0.0.0.255 area 0
 network 168.192.0.1 0.0.0.0 area 0
 network 172.26.1.100 0.0.0.0 area 0
 default-information originate always
```

```
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 network 10.100.100.0 mask 255.255.255.0
 network 168.192.0.0 mask 255.255.255.0
 network 168.192.1.0 mask 255.255.255.0
 aggregate-address 168.192.0.0 255.255.254.0
 neighbor IBGP peer-group
 neighbor IBGP remote-as 1
 neighbor IBGP update-source Loopback0
 neighbor IBGP version 4
 neighbor IBGP next-hop-self
 neighbor EBGP peer-group
 neighbor EBGP remote-as 100
 neighbor EBGP prefix-list FROMEBGP in
 neighbor EBGP prefix-list TOEBGP out
 neighbor EBGP route-map LOCALPREFIN in
 neighbor EBGP route-map PREPEND out
 neighbor EBGP filter-list 20 in
 neighbor EBGP filter-list 10 out
 neighbor 10.0.1.2 peer-group EBGP
 neighbor 172.26.1.200 peer-group IBGP
 no auto-summary
!
ip forward-protocol nd
ip route 168.192.0.0 255.255.255.0 Null0
ip route 168.192.1.0 255.255.255.0 Null0
!
ip as-path access-list 10 permit ^$
ip as-path access-list 20 deny _200$
ip as-path access-list 20 permit .*
!
```

```
no ip http server
no ip http secure-server
!
!
ip prefix-list FROMEBGP seq 5 deny 0.0.0.0/8 le 32
ip prefix-list FROMEBGP seq 10 deny 10.0.0.0/8 le 32
ip prefix-list FROMEBGP seq 15 deny 172.16.0.0/12 le 32
ip prefix-list FROMEBGP seq 20 deny 192.168.0.0/16 le 32
ip prefix-list FROMEBGP seq 25 deny 127.0.0.0/8 le 32
ip prefix-list FROMEBGP seq 30 deny 169.254.0.0/16 le 32
ip prefix-list FROMEBGP seq 35 deny 192.0.2.0/24 le 32
ip prefix-list FROMEBGP seq 40 deny 224.0.0.0/3 le 32
ip prefix-list FROMEBGP seq 50 deny 172.160.0.0/16 le 32
ip prefix-list FROMEBGP seq 55 permit 0.0.0.0/0 le 32
!
ip prefix-list LOCPREFIN seq 5 deny 50.50.50.0/24
ip prefix-list LOCPREFIN seq 10 deny 60.60.60.0/24
ip prefix-list LOCPREFIN seq 15 permit 70.70.70.0/24
ip prefix-list LOCPREFIN seq 20 permit 80.80.80.0/24
!
ip prefix-list PREPENDPREFIX seq 5 permit 168.192.0.0/24
!
ip prefix-list TOEBGP seq 5 permit 168.192.0.0/23 le 24
ip prefix-list TOEBGP seq 10 deny 0.0.0.0/0 le 32
!
!
!
route-map LOCALPREFIN permit 5
 match ip address prefix-list LOCPREFIN
 set local-preference 300
!
route-map LOCALPREFIN permit 10
!
```

```
route-map PREPEND permit 10
 match ip address prefix-list PREPENDPREFIX
 set as-path prepend 1 1 1
!
route-map PREPEND permit 15
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

R2 konfiguraatio

```
R2#sh run
Building configuration...

Current configuration : 3462 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
!
interface Loopback0
 ip address 172.26.1.200 255.255.255.255
!
interface Loopback1
 ip address 10.200.200.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.252
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 10.0.2.1 255.255.255.252
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.255 area 0
 network 10.200.200.0 0.0.0.255 area 0
 network 172.26.1.200 0.0.0.0 area 0
 default-information originate always
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 network 10.200.200.0 mask 255.255.255.0
 network 168.192.0.0 mask 255.255.255.0
 network 168.192.1.0 mask 255.255.255.0
 network 168.192.100.0 mask 255.255.255.0
 aggregate-address 168.192.0.0 255.255.254.0
 neighbor IBGP peer-group
 neighbor IBGP remote-as 1
 neighbor IBGP update-source Loopback0
 neighbor IBGP version 4
 neighbor IBGP next-hop-self
 neighbor EBGP peer-group
```

```
 neighbor EBGP remote-as 200
 neighbor EBGP prefix-list FROMEBGP in
 neighbor EBGP prefix-list TOEBGP out
 neighbor EBGP route-map LOCALPREFIN in
 neighbor EBGP route-map PREPEND out
 neighbor EBGP filter-list 20 in
 neighbor EBGP filter-list 10 out
 neighbor 10.0.2.2 peer-group EBGP
 neighbor 172.26.1.100 peer-group IBGP
 no auto-summary
!
ip forward-protocol nd
ip route 168.192.0.0 255.255.255.0 Null0
ip route 168.192.1.0 255.255.255.0 Null0
ip route 168.192.100.0 255.255.255.0 Null0
!
ip as-path access-list 10 permit ^$
ip as-path access-list 20 deny _200$
ip as-path access-list 20 permit .*
!
no ip http server
no ip http secure-server
!
!
ip prefix-list FROMEBGP seq 5 deny 0.0.0.0/8 le 32
ip prefix-list FROMEBGP seq 10 deny 10.0.0.0/8 le 32
ip prefix-list FROMEBGP seq 15 deny 172.16.0.0/12 le 32
ip prefix-list FROMEBGP seq 20 deny 192.168.0.0/16 le 32
ip prefix-list FROMEBGP seq 25 deny 127.0.0.0/8 le 32
ip prefix-list FROMEBGP seq 30 deny 169.254.0.0/16 le 32
ip prefix-list FROMEBGP seq 35 deny 192.0.2.0/24 le 32
ip prefix-list FROMEBGP seq 40 deny 224.0.0.0/3 le 32
ip prefix-list FROMEBGP seq 50 deny 172.160.0.0/16 le 32
```

```
ip prefix-list FROMEBGP seq 55 permit 0.0.0.0/0 le 32
!
ip prefix-list LOCPREFIN seq 5 permit 50.50.50.0/24
ip prefix-list LOCPREFIN seq 10 permit 60.60.60.0/24
ip prefix-list LOCPREFIN seq 15 deny 70.70.70.0/24
ip prefix-list LOCPREFIN seq 20 deny 80.80.80.0/24
!
ip prefix-list PREPENDPREFIX seq 5 permit 168.192.1.0/24
ip prefix-list PREPENDPREFIX seq 10 permit 168.192.0.0/23
!
ip prefix-list TOEBGP seq 5 permit 168.192.0.0/23 le 24
ip prefix-list TOEBGP seq 10 deny 0.0.0.0/0 le 32
!
!
!
route-map LOCALPREFIN permit 5
 match ip address prefix-list LOCPREFIN
 set local-preference 200
!
route-map LOCALPREFIN permit 10
!
route-map PREPEND permit 10
 match ip address prefix-list PREPENDPREFIX
 set as-path prepend 1 1 1
!
route-map PREPEND permit 15
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
```

```
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

OPERAATTORI1 konfiguraatio

```
OPERAATTORI1#sh run
Building configuration...

Current configuration : 1108 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname OPERAATTORI1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
```

(18)

```
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
!
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.252
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 10.0.3.1 255.255.255.252
 speed 100
 full-duplex
!
interface FastEthernet1/0
 ip address 10.60.60.1 255.255.255.252
 speed 100
 full-duplex
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 redistribute static
 neighbor 10.0.1.1 remote-as 1
```

```
 neighbor 10.0.3.2 remote-as 300
 no auto-summary
!
ip forward-protocol nd
ip route 200.150.0.0 255.255.255.0 Null0
ip route 200.150.1.0 255.255.255.0 Null0
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

OPERAATTORI2 konfiguraatio

```
OPERAATTORI2#sh run
Building configuration...
```

(18)

```
Current configuration : 1108 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname OPERAATTORI2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
!
interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.252
 speed 100
```

(18)

```
 full-duplex
!
interface FastEthernet0/1
 ip address 10.0.4.1 255.255.255.252
 speed 100
 full-duplex
!
interface FastEthernet1/0
 ip address 10.60.60.2 255.255.255.252
 speed 100
 full-duplex
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 redistribute static
 neighbor 10.0.2.1 remote-as 1
 neighbor 10.0.4.2 remote-as 300
 no auto-summary
!
ip forward-protocol nd
ip route 200.200.0.0 255.255.255.0 Null0
ip route 200.200.1.0 255.255.255.0 Null0
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
```

```
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

INTERNET konfiguraatio

```
INTERNET#sh run
Building configuration...

Current configuration : 1235 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname INTERNET
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
```

(18)

```
memory-size iomem 5
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
interface Loopback0
 ip address 75.75.75.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.0.3.2 255.255.255.252
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 10.0.4.2 255.255.255.252
 speed 100
 full-duplex
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 network 75.75.75.0 mask 255.255.255.0
```

(18)

```
 redistribute static
 neighbor 10.0.3.1 remote-as 100
 neighbor 10.0.4.1 remote-as 200
 no auto-summary
!
ip forward-protocol nd
ip route 50.50.50.0 255.255.255.0 Null0
ip route 60.60.60.0 255.255.255.0 Null0
ip route 70.70.70.0 255.255.255.0 Null0
ip route 75.75.75.0 255.255.255.0 Loopback0
ip route 80.80.80.0 255.255.255.0 Null0
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

(18)