VARMENNETUT YHTEYDET

Mari Sairanen

Opinnäytetyö
Toukokuu 2011

Tietotekniikka
Tekniikka ja liikenne

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) SAIRANEN, Mari	Julkaisun laji Opinnäytetyö	Päivämäärä 16.05.2011
	Sivumäärä 98	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)

Työn nimi
VARMENNETUT YHTEYDET

Koulutusohjelma
Tietotekniikka

Työn ohjaaja(t)
NARIKKA, Jorma

Toimeksiantaja(t)
TeliaSonera Finland Oyj
KÄSSI, Saku

Tiivistelmä

Tänä päivänä tietoliikenneyhteydet ovat yrityksille elintärkeät, jopa hetkellinen katkos yhteyksissä voi aiheuttaa mittavia rahallisia tappioita. Varmennetuilla yhteyksillä pyritään takaamaan toimivat tietoliikenneyhteydet esimerkiksi laiterikon tai kaapelivian sattuessa.

Työssä perehdyttiin kahteen reititysprotokollaan ja kahteen redundantti-protokollaan, joita voidaan hyödyntää toteutettaessa redundantteja verkkoratkaisuita. Työssä keskityttiin pääasiassa L3-tason varmennukseen.

Teoriaan perehtymisen jälkeen suunniteltiin ja rakennettiin testausympäristö ja suunniteltiin konfiguraatiot kahden eri laitevalmistajan laitteille. Samalla mietittiin, millaisia vikatilanteita pystytään luomaan ja testaamaan mahdollisimman todenmukaisesti.

Testausvaiheessa tutkittiin toteutetun verkon konvergoitumista eri protokollilla ja laitteilla. Testausten jälkeen analysoitiin tuloksia ja verrattiin eri ratkaisujen toimivuutta.

Avainsanat (asiasanat)
BGP, OSPF, VRRP, HSRP, Reititys, redundantit yhteydet

Liitteenä 26 sivua konfiguraatioita.

Author(s)
SAIRANEN, Mari

Type of publication
Bachelor´s / Master's Thesis

Date
16.05.2011

Pages
98

Language
Finnish

Confidential

( ) Until

Permission for web publication
(X)

Title
TITLE
REDUNDANT CONNECTIONS

Degree Programme
Information Technology,

Tutor(s)
NARIKKA, Jorma

Assigned by
TeliaSonera Finland Oyj
KÄSSI, Saku

Abstract

Internet connections are nowadays essential to companies. Even a momentary breakage on connection may cause large financial deficit. Redundant connections aim at assuring functional connections when a hardware failure or cable fault occurs.

In this thesis two routing protocols and two redundant protocols were familiarized withwhich can be exploited in redundant networks. The main focus of this thesis was on concentrating on redundancy of Layer 3.

After the theory part of the thesis a testing environment was designed and built. Configurations for two different routers were designed. At the same time it was considered what kind of fault situations could be created and tested as realistic as possible.

In a testing phase the convergence of the network was studied using different protocols and routers. After the testing phase the results were analyzed and various implementations were compared.

Keywords
BGP, OSPF, VRRP, HSRP, Routing, Redundant connections

As appendix 26 configuration pages.

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

AD	Administrative Distance
AS	Autonomous System
BGP	Border Gateway Protocol
CPE	Customer-premises equipment
EGP	Exterior Gateway Protocol
HSRP	Hot StandBy Router Protocol
ICMP	Internet Control Message Protocol
IETF	The Internet Engineering Task Force
IGP	Interior Gateway Protocol
IOS	Internetwork Operating System
IPv4	IP versio 4
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
LAN	Local Area Network
LSDB	Link State Database
MAC	Media Access Control
MED	Multi-exit Discriminator
OSPF	Open Shortest Path First
PE	Provider Edge
PI	Provider Independent
PVST	Per Vlan Spanning Tree
RFC	Request for comments
RTP	Real Time Transport Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

1 TYÖN LÄHTÖKOHDAT

1.1 Toimeksiantaja

TeliaSonera Oyj on pohjoismainen tietoliikenneoperaattori. Konserni tarjoaa verkkoyhteyksiä ja televiestintäpalveluja. Suomessa aiemmin toiminut Sonera on ollut edelläkävijä yritysten tietoliikenneratkaisujen ja palvelujen toimittajana. Työntekijöitä koko konsernissa oli vuoden 2009 lopulla 29 734. Suomessa työntekijöitä oli 4 981. (TeliaSonera Annual Report 2009.)

TeliaSoneran suurimmat alueet ovat matkaviestintä (Mobility Services), laajakaistapalvelut (Broadband Services) sekä TeliaSoneran osakeomistukset Venäjällä, Turkissa ja Euraasiassa. Kannattavan kasvun ja maiden rajat ylittävien synergiaetujen varmistamiseksi TeliaSonera on organisoitu kolmeen kansainväliseen liiketoiminta-alueeseen. Liiketoiminta-alueet kantavat täyden vastuun oman liiketoimintansa tuloksesta. Ruotsissa ja Suomessa on erillinen myyntiyksikkö, joka vastaa kaikesta myynnistä yritysasiakkaille. (TeliaSonera Annual Report 2009.)

Broadband Services tarjoaa viestintä- ja viihdepalveluja kotitalouksille ja yrityksille johtavilla Pohjoismaiden ja Baltian alueella. Sen palveluja ovat puhe-, laajakaista-, data- ja TV-palvelut. Broadband Services myös operoi konsernin yhteistä runkoverkkoa. (TeliaSonera Annual Report 2009.)

Mobility Services tarjoaa matkaviestinpalveluja, kuten puhe- ja datapalveluja, johtavilla brändeillä Pohjoismaiden ja Baltian alueella. Palvelut sisältävät matkaviestinpohjaiset puhepalvelut ja matkapuhelimella tai kannettavalla tietokoneella käytettävät langattomat datapalvelut. (TeliaSonera Annual Report 2009.)

Monilla Euraasian markkinoilla TeliaSonera on johtava matkaviestinpalvelujen tarjoaja. TeliaSoneralla on johtavilla tai vahvoilla brändeillä toimivia enemmistöomisteisia tytäryhtiöitä kahdeksalla markkina-alueella sekä vähemmistöosuus Venäjällä ja Turkissa toimivista johtavista operaattoreista.
(TeliaSonera Annual Report 2009.)

1.2 Taustaa

Työn tavoitteena oli perehtyä tietoliikenneverkon varmistamiseen käytettäviin metodeihin lähinnä loogisella tasolla WAN-ympäristöissä. Työssä oli tarkoitus käydä läpi kahden laitevalmistajan tarjoamia ratkaisuja ja tietoliikenneprotokollia. Tarkoituksena oli myös selvittää verkon konvergoitumisaikoja eri ratkaisumalleilla.

Toimiva tietoverkko on yrityksen toiminnalle äärimmäisen tärkeää. Yritykset ovat siirtäneet paljon jokapäiväisiä toimintojaan verkkoon ja monet yritykset ovat maantieteellisestikin hajaantuneet jopa globaalilla tasolla. Joissakin tapauksissa jopa puolen tunnin katkos yrityksen verkkoyhteyksissä voi vaikuttaa haitallisesti liiketoimintaan. Tietoliikenneyhteyksien varmistamisella taataan liiketoiminnan jatkuminen laiterikkojen, kaapelivikojen yms. aikana.

Varmennettuja yhteyksiä voidaan käyttää myös kuormanjakamiseen tarvittaessa. Suomessa yleisin tapa toteuttaa tietoliikenneverkko on ostaa palvelu joltakin operaattorilta. Tällöin asiakkaalle toimitettava reititin on operaattorin omistuksessa ja hallinnoitavissa. Näin ollen varmistuksen toteutuksesta WAN-liikenteen osalta huolehtii operaattori. Suomessa operaattoreilla on tarjolla useita mahdollisuuksia yhteyksien varmistamiseen.

Suunniteltaessa varmennusta tulee usein vastaan single point of failure, eli yksi piste, jossa katkos voi aiheuttaa katkoksen koko yhteydelle, vaikka muilta osin yhteys olisikin kahdennettu. Tämä pyritään välttämään rakentamalla kahdennus mahdollisimman pitkälle.

Ensimmäinen askel, josta lähdetään varmennusta suunnittelemaan, on lähiverkon varmennus. Mikäli lähiverkossa sijaitsee kriittisiä palvelimia, on syytä varmentaa yhteys palvelimiin käyttämällä kahta verkkokorttia palvelimessa. Seuraavaksi on syytä paneutua suunnittelemaan kytkinverkon topologia niin, että siitä saadaan redundantti. Yleisesti kytkinverkoissa käytetään spanning tree -protokollaa, jonka avulla saadaan rakennettua varmistettu ja silmukkavapaa kytkinverkko. Tässä työssä

paneudutaan lähinnä wan-liikenteen varmentamiseen ja siinä käytettäviin protokolliin.

Yksi tapa varmentaa Internet-yhteys, on multihoming-eli moniverkkoliityntä. Tällöin asiakkaalla on yhteys kahdelta tai useammalta operaattorilta, jolloin voidaan varmistaa verkon toimivuus, vaikka toisen operaattorin runkoverkko kaatuisi tai siellä esiintyisi vakavia häiriöitä. Yleensä nämä yhteydet toteutetaan käyttäen protokollana BGP:tä, joka on tarpeeksi vakaa reititysprotokolla. Valittaessa operaattoreita kannattaa ottaa huomioon runkoverkon laajuus ja mahdolliset ulkomaanyhteydet. Multihoming-yhteys kannattaa toteuttaa käyttämällä PI-osoiteavaruutta eli operaattori-riippumatonta osoiteavaruutta. (Niemi 2008.)

2 MULTICAST

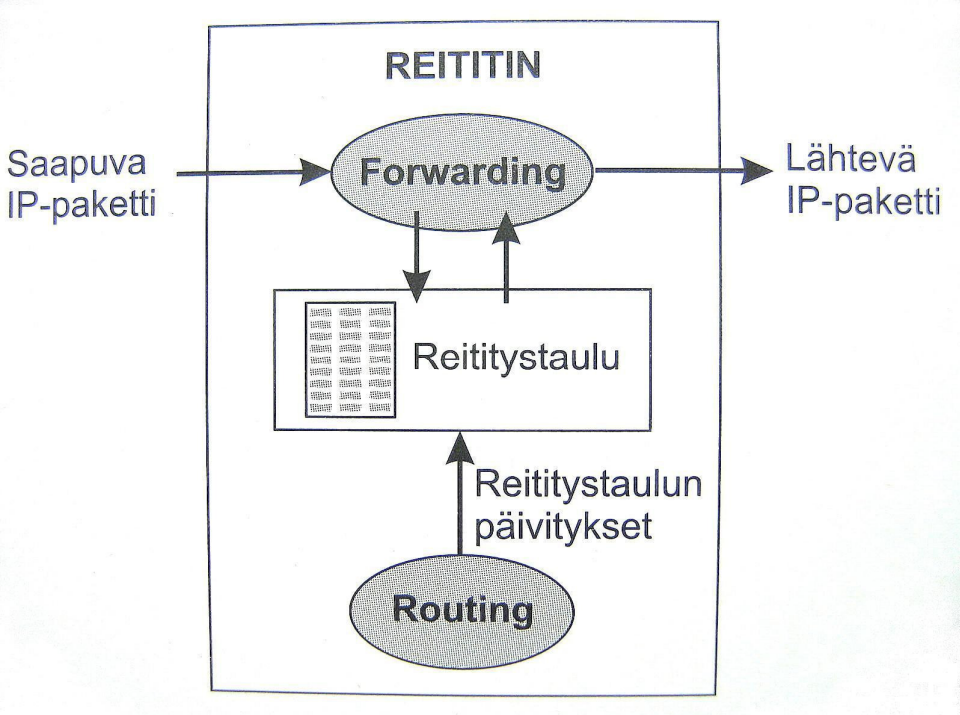
IPv4-protokollassa on olemassa kolme lähetysmuotoa: unicast, multicast ja broadcast. Unicast tarkoittaa kohdennettua lähetystä, multicast ryhmälähetystä ja broadcast yleislähetystä. Tässä luvussa kerrotaan tarkemmin multicast-lähetyksestä, koska monet protokollat käyttävät multicast-lähetyksiä viestintään.

Kimmo Kaarion (2002, 60.) mukaan ryhmälähetyksissä kunkin ryhmälähetys-osoitteeseen lähetetyn IP-paketin vastaanottaa jokainen reititin, joka on ilmoittautunut kyseisen ryhmälähetys-osoitteen määrittelemään ryhmälähetys-ryhmään. Ryhmiin ilmoittaudutaan käyttämällä IGMP-protokollaa. Ethernet-ryhmälähetykset ulottuvat vain kyseiseen Ethernet-verkkoon, kun taas IP-tason ryhmälähetykset voivat periaatteessa levitä maailmanlaajuisesti. Ryhmälähetykset perustuvat vastaanottajan toimintaan, kun vastaanottaja on liittynyt haluamiinsa ryhmälähetys-ryhmiin, verkon aktiivilaitteet, kuten reitittimet, osaavat välittää kunkin ryhmän viestit kaikille ryhmän jäsenille. Ryhmälähetysten vahvuutena on se, ettei sanomia tarvita kuin yksi kullakin Ethernet-tason linkillä ja paketteja ei lähetetä kenellekään turhaan, kuten broadcast-lähetyksissä. (Kaario 2002.)

3 REITITYS

3.1 Yleistä

Tässä työssä käsitellään IP-maailman reititystä ja -reititysprotokollia. Perehdytään aluksi reitityksen perusteisiin teoriatasolla. Kimmo Kaarion (2002, 82.) mukaan reitityksellä tarkoitetaan mekanismeja, joilla IP-paketti löytää lähteestä kohteeseen paketista löytyvien osoitetietojen perusteella. IP reititys jakaantuu kahteen eri prosessiin: IP-pakettien mekaaniseen välitykseen reitittimen sisääntuloliitynnästä oikeaan ulos menevään liityntään reititystaulun perusteella (forwarding) sekä protokolliin, joilla reititystaulujen tietoja välitetään IP-verkon reitittimien kesken (routing). Kuviossa 1 havainnollistetaan reitittimen toimintaa. (Kaario 2002.)



KUVIO 1. Periaatekuva reitittimen toiminnasta. (Kaario 2002, 82.)

Seuraavassa perehdytään reitityksen perusterminologiaan ja reitityksen käsitteisiin:

- Staattisella reitityksellä tarkoitetaan reittejä, joiden kohteet määritellään manuaalisesti reitittimellä. Tällöin verkon saavutettavuus ei ole riippuvainen verkon olemassaolosta tai verkosta itsestään. Eli, vaikka kohde ei olisi aktiivisena, reitit pysyvät reititystaulussa ja liikenne lähetetään kohteeseen.

- Oletusreitityksellä tarkoitetaan reittiä, jolle reititin lähettää paketit, joiden kohdetta ei löydy reititystaulusta. Tämä on helpoin tapa muodostaa reititys domainille, jolla on yksi ainoa poistumispiste.

- Dynaamisella reitityksellä tarkoitetaan reititystä, jossa reititin oppii reitit käyttäen jotakin reititysprotokollaa. Tässä tapauksessa verkon saavutettavuus on riippuvainen verkon olemassaolosta ja verkon tilasta. Eli, mikäli kohdeverkko on alhaalla, reitti poistetaan reititystaulusta ja kohteeseen ei lähetetä paketteja.

Verkossa reitityksestä huolehtii reititin, IP-pakettien reititys tapahtuu hyppy hypyltä eli reititin on kiinnostunut ainoastaan siitä, mihin suuntaan IP-paketti välitetään seuraavaksi. Verkon suorituskyvyn ja virhetilanteista toipumisen kannalta on hyvin suuri merkitys sillä, mikä reititysprotokolla valitaan. (Kaario 2002, 82.)

3.2 Reititystaulu

Reititin muodostaa tuntemistaan reiteistä reititystaulun, jonka mukaan reititin tekee reitityspäätöksen.
Reitittimen reititystaulu pitää sisällään seuraavat tiedot:

1) Kohdeosoite: Tässä on joko täydellinen osoite tai verkko-osoite

2) Seuraavan hypyn osoite: Tämä on joko seuraavan reitittimen osoite tai ko. reitittimeen suoraan liitetyn verkon osoite, esim. Ethernet-porttiin kytketyn palomuurin osoite

3) Reittien kustannukset (cost:t) ja AD:t eli adminstrative distancet

Alla tuloste toiminnassa olevan Ciscon reitittimen reititystaulusta. Tulosteen yläosassa kerrotaan merkkien selitykset, esimerkiksi lyhenne C reitin edessä tarkoittaa connected-verkkoa. "Gateway of last resort" kertoo oletusreitin ja sen jälkeen on varsinainen reititystaulu. Oletusreitti on reitti, jota käytetään, mikäli paketin kohdeosoitteelle ei löydy reittiä reititystaulusta. Taulussa on reitti yhtä riviä kohden. Kirjaimella alkava rivi on varsinainen reitti: B tarkoittaa BGP-protokollan kautta opittua reittiä ja C (Connected) taas reittiä, joka on suoraan yhteydessä reitittimeen. Tähti kirjaimen edessä merkitsee oletusreittiä. Kirjaimen jälkeen tulee luonnollisesti verkko ja sen prefiksi, esimerkiksi 10.0.0.0/8. Numerot hakasuluissa ovat administrative distance eli AD ja metric. Näiden jälkeen tulee reititin jolle paketti tulee lähettää eteenpäin ja fyysinen portti josta paketti lähtee seuraavalle reitittimelle. Mikäli reitittimeen olisi konfiguroitu esimerkiksi RIP-protokolla, nähtäisiin reititystaulusta myös aika jolloin reitti vanhenee. (Tutoriaalit: Cisco IOS-pikaopas 2009.)

```
Router#sh ip route
Codes: C -connected, S -static, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
       E1 -OSPF external type 1, E2 -OSPF external type 2
       i -IS-IS, su -IS-IS summary, L1 -IS-IS level-1, L2 -IS-IS level-2
       ia -IS-IS inter area, * -candidate default, U -per-user static route
       o -ODR, P -periodic downloaded static route

Gateway of last resort is 10.43.3.154 to network 0.0.0.0
     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.143.0 is directly connected, Vlan999
     172.22.0.0/30 is subnetted, 2 subnets
B       172.22.231.24 [20/0] via 10.43.3.154, 1w6d
C       10.43.3.152/30 is directly connected, FastEthernet0.100
C       10.43.68.164/30 is directly connected, Vlan999
C       10.43.68.160/30 is directly connected, Vlan999
```

```
B       10.43.5.212/30 [20/0] via 10.43.3.154, 1w6d
C    192.168.0.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 10.43.3.154
```

3.3 Reititysprotokollat

Aki Anttilan (2001, 285.) mukaan reititysprotokollat voidaan jakaa erilaisten ominaisuuksien perusteella erilaisiin perheisiin. Karkeimmalla tasolla voidaan tehdä niin, että määritellään jako verkon sisäisiin ja verkkojen välillä toimiviin protokolliin. Toisaalta taas reititysprotokollat voidaan jakaa kahteen ryhmään niiden toimintaperiaatteiden mukaan. (Anttila 2001, 85.)

Reititysprotokollat levittävät tietojaan naapurireitittimille mainostusviesteillä ja kullakin protokollalla on omanlaisensa mainostukset, joten vain samalla protokollalla varustetut reitittimet voivat ymmärtää niitä. Internet muodostuu autonomisista järjestelmistä. Autonomisella järjestelmällä tarkoitetaan yhtenäistä aluetta, joka on yhtenäisen hallinnon alla ja jossa käytetään yhtenäistä reitityspolitiikkaa. Näiden alueiden reunoilla olevien reitittimien on osattava tulkita kaikkien siihen liittyneiden autonomisten järjestelmien reititysprotokollia. Myös yhden autonomisen järjestelmän sisällä voidaan käyttää useampia reititysprotokollia. Reititysprotokollat voivat vaihtaa keskenään reititystietoja, mutta se ei ole suositeltavaa. Mikäli tähän ratkaisuun päädytään, on konfiguraatio suunniteltava huolella, ettei reitityssilmukoita pääse syntymään. (Anttila 2001, 286 - 287.)

Autonomisen järjestelmän sisällä käytettäviä protokollia kutsutaan IGP-protokolliksi (Interior Gateway Protocol) ja autonomisten järjestelmien välillä käytettäviä protokollia EGP-protokolliksi (Exterior Gateway Protocol). EGP-protokollia käytetään yleensä operaattoreiden runkoverkoissa. IGP-protokollia ovat RIP, RIPv2, IGRP, EIGRP, OSPF ja IS-IS. EGP-protokollia ovat taas EGP ja BGP versiot 1-4. BGP:stä lisää luvussa 3.4.

Toimintaperiaatteiden mukaan reititysprotokollat voidaan jakaa etäisyysvektori- ja linkkitila-protokolliin. (Anttila 2001, 286 - 287.)

3.3.1 Etäisyysvektoriprotokollat

Etäisyysvektoriprotokollien toiminta perustuu siihen, että ne kuuntelevat naapureidensa lähettämiä mainostuksia ja muodostavat reititystaulunsa niiden perusteella. Reittimainostuksien informaatio pitää sisällään ainoastaan etäisyyksiä eri kohteisiin. (Kaario 2002, 88.). Etäisyysvektoriprotokollia ovat mm. RIP, RIPv2, EIGRP ja IGRP. Seuraavana kuvataan etäisyysvektoriprotokollien perustoiminnan vaiheet Aki Anttilan (2001, 292 - 293.) mukaan:

1) Reititin mainostaa tuntemiaan verkkoja naapureille lähettämällä etäisyysvektorin, jossa kerrotaan, mikä on niiden tuntema etäisyys kyseisiin verkkoihin.

2) Ilmoituksen vastaanottava reititin lisää jokaisen verkon etäisyyteen etäisyyden, joka on mainostavan ja mainostuksen vastaanottavan reitittimen välillä.

3) Seuraavaksi vastaanottava reititin tutkii verkko kerrallaan, löytyykö siihen liittyvä tieto jo reititystaulusta:
    a. Jos verkko löytyy ja nyt vastaanotettu etäisyys on suurempi, ei tehdä mitään, mikäli mainostaja on jokin muu reititin. Mikäli mainostaja on alkuperäinen reititin, päivitetään uusi etäisyys reititystauluun.
    b. Jos verkko löytyy ja vastaanotettu etäisyys on pienempi, päivitetään reititystauluun uudet tiedot.
    c. Jos verkko löytyy ja vastaanotettu etäisyys on sama kuin aikaisemmin, päivitetään reitin elinaikalaskuri, mikäli mainostaja on sama, jonka kautta reitti on opittu aikaisemmin.

4) Tämän jälkeen mainostusta jatketaan edelleen eteenpäin säännöllisin väliajoin, väliaika riippuu reititysprotokollasta.

5) Jos reititin ei saa mainostusta johonkin reittiin liittyen ennalta määrätyssä ajassa, se asettaa tällaisen reitin saavuttamattomaksi reititystaulussaan.

Etäisyysvektoriprotokollia ei nykyään suositella käytettäväksi etenkään suurissa verkoissa muutamien perusongelmien takia. Tällaisia ongelmia ovat mm. reitityssilmukoiden syntyminen, huono skaalautuvuus ja heikko kustannuslaskelman tarkkuus. (Anttila 2001, 292 - 293.)

3.3.2 Yhteystilaprotokollat

Yhteystilaprotokollia ovat OSPF ja IS-IS. Yhteystilaprotokollien toiminnan perusajatuksena on, että verkon kaikki reitittimet tuntevat koko verkon topologian. Jokainen reititin laskee topologiatietokannan perusteella reititystaulunsa. Topologiatietokanta muodostuu reitittimien toisilleen välittämistä yhteystilailmoituksista. Tietojen vaihtaminen edellyttää aina naapuruussuhteen muodostamista reitittimien välille. Alla yhteystilaprotokollien mekanismit reitittimien välisessä toiminnassa:

1. Naapuruussuhteen muodostaminen suoritetaan siinä vaiheessa, kun reititin käynnistyy tai kun linkki joidenkin reitittimien välissä on ollut tarpeeksi pitkään poikki, jolloin naapuruussuhde on katkennut

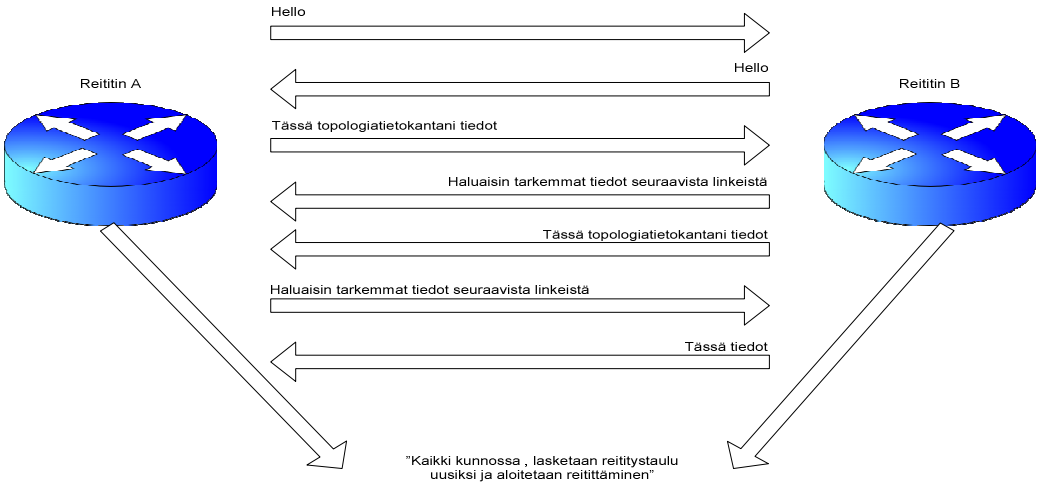
2. Alkuperäisen topologiatietokannan kuvaus ja tarvittavien tietojen välittäminen naapurireitittimelle

3. Yhteystilailmoitusten säännöllinen välittäminen

4. Ilmoitusten välittäminen, mikäli verkon topologia muuttuu

(Anttila 2001, 319 – 320.)

Kuviossa 2 on esitetty tapa, jolla reitittimet rakentavat topologiatietokantansa.



KUVIO 2. Periaatekuva topologiatietokannan rakentamisesta. (Anttila 2001, 321.)

Vaikka yhteystilaprotokollat toimivat luotettavammin suurissa verkoissa, on niissäkin puutteita. Muistin tarve on yksi ongelmista. Mikäli kyseessä on suuri verkko, vie topologiatietokanta paljon muistia reitittimessä. Myös reititystaulun laskenta vaikuttaa reitittimen suorituskykyyn. Hyviä puolia taas ovat verkon nopea konvergoituminen ja tuki tarkemmalle etäisyyden määritykselle. (Anttila 2001, 325 – 326.)

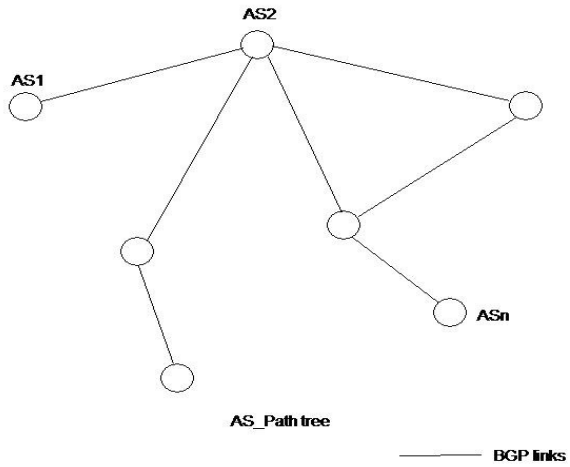
Luvussa 3.4 perehdytään tarkemmin BGP:hen ja luvussa 3.5 OSPF:ään, jotka ovat tänä päivänä yleisimmät IP-verkoissa käytetyt reititysprotokollat.

3.4 BGP

BGP on Internetin yleisimmin käytetty reititysprotokolla, jota voidaan kutsua polkuvektori-protokollaksi. BGP-1-versio on määritelty ensimmäisen kerran RFC 1105 vuonna 1989. Nykyisin käytettävä versio BGP-4 on määritelty dokumentissa RFC 1771. BGP on helposti skaalautuva ja ei-laiteriippuvainen protokolla, joka tukee luokatonta reititystä. BGP:n toiminta perustuu reititykseen autonomisten systeemien

eli AS:n välillä. Tosin BGP toimii myös autonomisen alueen sisällä. AS:n välillä toimiessaan käytetään nimitystä eBGP (External BGP)ja AS:n sisällä iBGP (Internal BGP). Alueiden sisällä toimivaa BGP:tä käytetään niissä tilanteissa, kun alueen läpi halutaan välittää BGP-sanomia. (Anttila 2001, 290 - 291.)

Kahden AS:n välistä yhteyttä voidaan kuvata polkuna ja kokoelmasta polkuja muodostuu reitti määrättyyn kohteeseen. Taatakseen reitityssilmukoista vapaan AS:n sisäisen reitityksen BGP käyttää hyväkseen polku-tietoja. Kuvio 3 havainnollistaa verkon AS-polkujen muodostaman puurakenteen, jossa jokainen AS on identifioitu uniikilla AS-numerolla. (Halabi 2001, 111.)



KUVIO 3. AS-polun puurakenne. (Halabi 2001, 112.)

3.4.1 Naapuruuden muodostaminen

Ennen kuin BGP-reitittimet voivat vaihtaa keskenään reititystietoja, on niiden muodostettava ns. peering-yhteys. Peering-yhteyttä muodostettaessa BGP perustaa TCP-istunnon reitittimien välille. Käytettäessä kuljetusprotokollana TCP:tä varmistetaan siirron luotettavuus ja itse reititysprotokollasta saadaan yksinkertai-

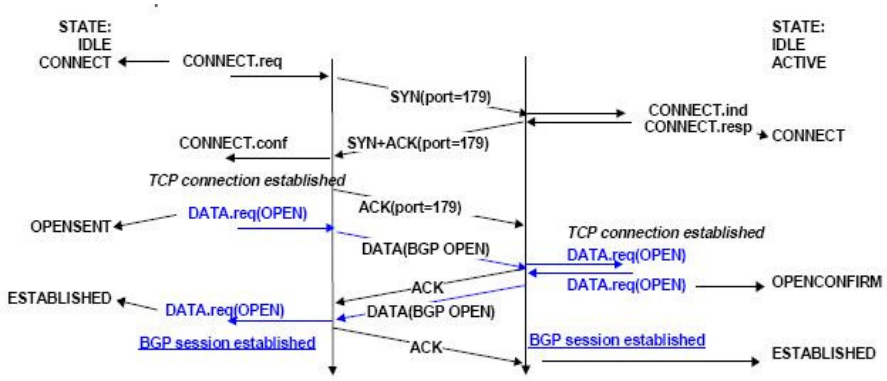
sempi. BGP:lle on varattu käyttöön portti 179. BGP käy käynnistyessään läpi seuraavat tilat:

1. Idle – Etsitään naapureita.
2. Connect – Kolmivaiheinen TCP-kättely naapurin kanssa on valmis.
3. Active – Yrittää muodostaa TCP-yhteyttä tai yhteyden muodostus on epäonnistunut.
4. OpenSent – BGP Open -viesti on lähetetty.
5. OpenConfirm – Vastaus BGP Open -viestiin saatu.
6. Established – BGP-naapuruus on kunnossa ja reititysinformaation vaihtaminen voidaan aloittaa.

BGP:n kommunikoinnissa käyttämät sanomat:

- OPEN – tällä sanomalla avataan sessio naapurien välille
- UPDATE – tätä sanomaa käytetään reittitietojen välittämiseen
- NOTIFICATION – tätä viestiä käytetään informoidessa naapureita sessiossa tapahtuneista virheistä
- KEEPALIVE – tällä sanomalla ylläpidetään naapureiden väliset peering-sessiot

Kuvio 4 havainnollistaa BGP:n peering-session muodostumisen TCP:n kolmivaiheisella kättelyllä.



KUVIO 4. BGP:n peering-session kolmivaiheinen TCP-kättely. (Luoma 2008.)

3.4.2 Attribuutit

Kun verkkoa mainostetaan, siihen liitetään erilaisia BGP-attribuutteja. Attribuutit ovat joukko parametreja, joita käytetään ilmaisemaan tarkempaa tietoa tarkasteltavasta prefiksistä. Attribuutit voidaan jakaa neljään eri luokkaan, jotka ovat:

- Well-known, mandatory: nämä liitetään jokaiseen Update-viestiin ja kaikkien BGP:tä puhuvien laitteiden on tunnistettava nämä

- Well-known, discretionary: nämä on jokaisen BGP:tä puhuvan laitteen tunnistettava, mutta näitä ei ole pakko sisällyttää Update-viesteihin

- Optional, transitive: nämä eivät ole välttämättä kaikkien tunnistettavissa, mutta siitä huolimatta ne tulee mainostaa naapureille

- Optional, nontransitive: nämäkään attribuutit eivät ole välttämättä kaikkien BGP:tä puhuvien laitteiden tunnistettavissa ja mikäli päivitysviesti sisältää tunnistamattomaksi luokiteltuja attribuutteja, ei niitä mainosteta naapureille

(Halabi 2001, 125-126.)

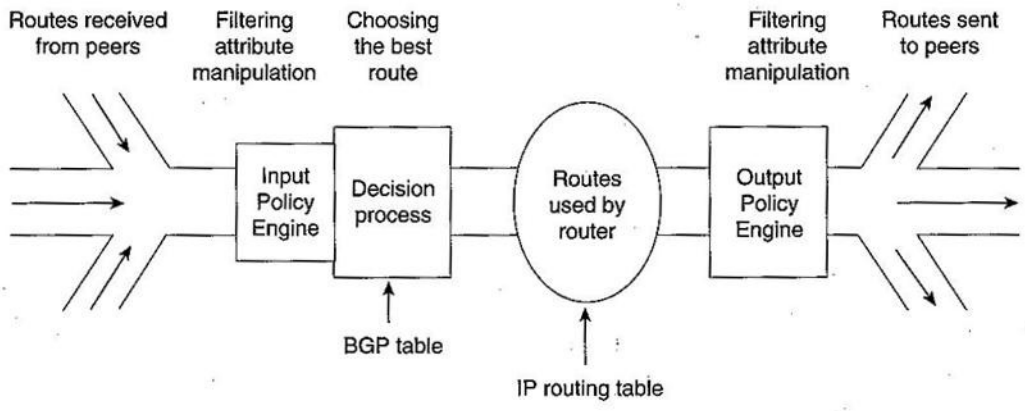
Taulukossa 1 on lueteltuna BGP-attribuutit, niiden luokka ja kuvaus.

TAULUKKO 1. BGP Attribuutit. (Stewart 2008, 442.)

Attribuutti	**Luokka**	**Kuvaus**
Aggregator	Optional, transitive	Router ID ja reitittimen AS summaroituna
AS_Path	Well-known, mandatory	Lista AS:sta, joiden läpi reitti tulee
Atomic Aggregate	Well-known, discretionary	Summarointi pitää sisällään useamman AS:n
Cluster ID	Optional, nontransitive	Sisältää reittiheijastimien ryhmätunnisteita.
Community	Optional, transitive	Reitin merkkaus (route tag)
Local Preference	Well-known discretionary	iBGP naapureille välitettävä ulkoisen polun metriikka
Multiple Exit Discri-minator(MED)	Optional, nontransitive	eBGP naapureille tieto, mitä kautta AS:ään tullaan sisään
Next Hop	Well-known, mandatory	Ulkoinen peer naapuri-AS:ssä
Origin	Well-known, mandatory	Pienintä origin-arvoa suositaan, määrittää, mitä kautta tietty verkko on injektoitu BGP:hen
Originator ID	Optional, nontransitive	Identifioi reittiheijastimen
Weight	Optional, not communi-cated to peers	Hallinnollinen attribuutti Ciscon IOS:ssa

3.4.3 BGP:n reitinvalinta

BGP vaihtaa naapureiden kesken reittitietoja update-viesteillä. BGP asettaa viesteissä saadut reitit erilliseen BGP-tauluun. Mikäli BGP-taulusta löytyy useampi reitti kohteeseen, BGP ei mainosta niitä kaikkia naapureille, vaan suorittaa parhaan polun valinnan. BGP asettaa ensimmäisen voimassa olevan polun parhaaksi poluksi. Tämän jälkeen BGP vertaa parasta polkua seuraavaan polkuun BGP-taulussa, kunnes on käynyt kaikki voimassa olevat polut läpi. BGP-prosessi tutkii seuraavissa taulukoissa mainittuja parametreja järjestyksessä eli mikäli reitittimellä on valittavana kaksi reittiä samalla local preferencen arvolla, se vertaa seuraavaksi reittien AS-polkuja. Parametrien vertaamista jatketaan niin kauan, kunnes eroavaisuus löytyy. Näistä parempi polku siirretään reititystauluun. Reititystauluun asennetaan myös voimassa olevat paikalliset reitit, näin ollen reititystaulusta löytyy lopullinen tieto käytettävistä reiteistä. Kuvio 5 havainnollistaa reitittimellä tapahtuvan BGP:n parhaan polun valinta-prosessin.



KUVIO 5. BGP:n reitinvalintaprosessi. (Halabi 2001, 153.)

Taulukossa 2 esitellään parametrit, joiden perusteella Ciscon IOS:lla toimiva reititin, johon on konfiguroitu BGP, valitsee parhaan polun.

TAULUKKO 2. Ciscon polunvalintakriteerit. (BGP Best Path Selection Algorithm 2006.)

1. Weight, painoarvo	Korkeimman weight-arvon reittiä pidetään parhaana.
2. Local preference	Korkein local preference-arvo
3. Paikallinen reitti	BGP-prosessiin injektoitu reitti (network-komento tai redistribuutattu IGP prosessista)
4. AS Path, AS polku	Lyhin AS-polku
5. Origin, alkuperä	Alin origin-attribuutin arvo
6. MED (multi-exit discriminator)	Alin MED-arvo
7. eBGP over iBGP	Valitaan eBGP:llä opittu reitti
8. IGP metric (IGP metriikka)	Valitaan reitti, jolla on pienin IGP:n metriikka BGP:n next hop-osoitteeseen
9. Multipath	Päätellään, käytetäänkö multipath-ominaisuutta, mikäli ominaisuus on käytössä, lisätään samanarvoiset reitit reititystauluun.
10. Vanhin ulkoinen BGP-reitti	Valitaan pisimpään voimassa ollut BGP-reitti.
11. BGP router ID, BGP-tunniste	Valitaan reitti, jolla on pienin BGP-tunniste.
12. Cluster List, ryhmittymä lista	Suositaan reittiä, jonka cluster-lista on lyhin.
13. Peering osoite, peeraus osoite (naapurin osoite)	Suositaan reittiä, joka tulee naapurilta, jonka peeraus-osoite on pienin

Taulukossa 3 esitellään Juniperin käyttämät reitinvalintakriteerit BGP-prosessissa.

TAULUKKO 3. Juniperin polunvalintakriteerit. (BGP Katsaus 2010.)

1. Next-hop:n saavutettavuus	Mikäli next hop on saavuttamattomissa, reittiä ei oteta reititystauluun
2. Korkein local preference	Reititin valitsee korkeimman local preferencen omaavan reitin
3. Lyhin AS-polku	Reititin valitsee lyhyimmän AS-polun omaavan reitin
4. Origin, alkuperä	Reititin valitsee reitin, jolla on pienin origin-arvo
5. Alin MED-arvo	Reititin valitsee reitin, jolla on pienin MED-arvo
6. Tarkka ulkoinen polku	Reititin valitsee suoraan eBGP:llä opitun reitin ennemmin kuin ulkoisen reitin, joka on opittu iBGP:n kautta
7. Pienin IGP-reitin metriikka	Reititin valitsee reitin, jonka next hop on opittu IGP:n kautta pienimmällä metriikalla
8. Maksimi määrä IGP-hyppyjä	Reititin valitsee IGP reitin, jonka BGP next hop on ratkaistu mahdollisimman monen next hop:n kautta
9. Lyhin reittiheijastimen cluster-lista	Reititin valitsee reitin, jonka cluster-lista on lyhin
10. Pienin Router ID	Reititin valitsee reitin, jonka RID on pienin arvo. Mutta reittejä, jotka tunnetaan eri AS:n kautta, ei vertailla
11. Pienin peeraus-osoite	Reititin valitsee reitin, joka on opittu naapurilta, jolla on pienin peeraus-osoite

3.4.4 Reitityspolitiikka

Kun puhutaan reitityspolitiikasta, puhutaan tavasta, jolla mainostettavia ja vastaanotettuja verkkoja käsitellään. Peering-yhteyksillä voidaan käyttää erilaisia tapoja liikenteen suodattamiseen ja näitä ovat:

- Pääsylistat (standardi ja laajennettu)
- Prefiksi-listat
- AS Path-lista
- Community-lista
- Route-map:t

PÄÄSYLISTAT

Standardi-pääsylistalla voidaan rajoittaa liikennettä lähettäjän IP-osoitteen perusteella. Laajennetulla pääsylistalla puolestaan voidaan rajoittaa liikennettä sekä lähettäjän että vastaanottajan IP-osoitteen perusteella ja lisäksi porttinumeroiden perusteella. Pääsylistat käydään läpi ylhäältä alaspäin, kunnes vastaava rivi löytyy. Mikäli mikään riveistä ei osu tarkasteltavaan verkkoon tms., on Ciscon reitittimillä ekplisiittinen deny-rivi viimeisenä, jolloin tarkastelun kohde hylätään. Eksplisiittinen deny-rivi ei välttämättä näy konfiguraatiossa.

Standardi pääsylista on muotoa:

access-list (list-number) (permit | deny) (ip-address) (subnet-mask)

Esimerkki reittien suodatuksesta standardi-pääsylistalla:

access-list 50 deny 10.10.10.0 0.0.0.255
router bgp 65500
neighbour 10.1.1.1 remote-as 65490
neighbour 10.1.1.1 distribute-list 50 out

Laajennettu pääsylista voidaan konfiguroida seuraavasti:

Access-list (list-number) (deny | permit) [protocol] (prefix) (prefix-wildcard) (network-mask) (network-mas-wildcard)

Esimerkki reittien suodatuksesta laajennetulla pääsylistalla:

```
hostname Router 100
 !
 router bgp 100
!---Output suppressed.
  neighbor 172.16.1.2 remote-as 200
  neighbor 172.17.1.2 distribute-list 101 in
 !
 !
 access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0
```

(How to Block One or More Networks From a BGP Peer 2006.)

PREFIKSI-LISTAT

Prefiksi-listoja voidaan käyttää korvaamaan pääsylistat liikenteen suodatuksessa. Suodatus voidaan tehdä joko prefiksin IP-osoitteen tai pituuden mukaan. Prefiksi-listat ovat käytössä joustavampia kuin pääsylistat ja niiden konfigurointi on käyttäjäystävällisempää, koska voidaan käyttää sekvenssinumeroita. Prefiksi-lista konfiguroidaan seuraavalla tavalla:

ip prefix-list list-name [seq sequence-value] {deny | permit network/length} [ge ge-value] [le le-value] (Configuring BGP 2011a n.d.)

Esimerkki reittien suodatuksesta prefiksi-listalla:

```
hostname Router 100
 !
 router bgp 100
  neighbor 172.16.1.2 remote-as 200
  neighbor 172.16.1.2 prefix-list cisco in
 !
ip prefix-list cisco seq 10 permit 0.0.0.0/0 le 19
```

(How to Block One or More Networks From a BGP Peer 2006.)

AS PATH-LISTA

Reittien suodattamista voidaan tehdä myös AS-Path-listalla. Tämä tapa on erityisen kätevä, kun on suodatettava tietyn tai tiettyjen AS:n reitit.

ip as-path access-list access-list-number *{permit | deny}* as-regexp

Tältä AS Path-listan mukainen konfiguraatio näyttää reitittimellä:

router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list 1 out
neighbor 193.1.12.10 filter-list 2 in
*ip as-path access-list 1 permit _109_*
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
(Configuring BGP 2011b n.d.)

COMMUNITY-LISTA

Community-listalla suodatetaan reittejä community-attribuutin perusteella. Nykyään monissa reitittimissä on konfiguroituna rivi: *ip bgp-community new-format*, jolloin voidaan ottaa käyttöön communityn uusi muoto. Tällöin community-lista voidaan esittää muodossa 65500:xx, jossa 65500 on AS-numero ja xx muuttuva arvo.

ip community-list community-list-number {permit | deny} community-number

Jos community-arvoja asetetaan listaan samalle riville useita peräkkäin, on kaikkien arvojen osuttava hakukriteeriin. Mikäli taas samalla listan nimellä tai numerolla asetetaan community-arvoja eri riveille, riittää, että yksi niistä vastaa hakukriteereitä. (White 2004, luku 6.)

Tältä community-lista näyttää reitittimen konfiguraatiossa:

ip community-list 1 permit 65500:3

ROUTE-MAP

Route-map kokoaa yhteen edellä mainitut suodatustavat ja se on tehokas ja joustava tapa toteuttaa reitityspolitiikkaa. Route-map voi pitää sisällään sekä match-että set-lauseita, joilla voidaan asettaa ehtoja ja määrittää attribuuttien arvoja.
Alla route map:n syntaksi Ciscon reitittimessä:

neighbor {ip-address | peer-group-name} route-map map-name {in | out}

Alla kaksi route-map:a konfiguroituna Ciscon retittimellä.

```
router bgp 100
 network 171.60.0.0
 network 172.60.0.0
 neighbor 200.69.232.70 remote-as 200
 neighbor 200.69.232.70 route-map set-as-path out
!
route-map set-as-path 10 permit
 match address 1
 set as-path prepend 100 100
!
route-map set-as-path 20 permit
 match address 2
!
access-list 1 permit 171.60.0.0 0.0.255.255
access-list 1 permit 172.60.0.0 0.0.255.255
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

Esimerkissä route-map set-as-path on sidottu BGP-prosessissa naapurille 200.69.232.20 outbound-suuntaan. Ensimmäisessä route-map-lausekkeessa verrataan tarkasteltavaa verkkoa access-list 1:ssä mainittuihin verkkoihin ja mikäli tuloksena on osuma, tehdään as-polulle ns. prependaus, eli pidennetään sitä keinotekoisesti kahdella. Toinen route-map:n lauseke ja access-list 2, ovat niille verkoille, jotka eivät osu vertailussa access-list 1:n verkkoihin. (Configuring BGP 2011c n.d.)

3.5 OSPF

Yksi yleisimmistä yhteystilaprotokollista on OSPF. OSPF on määritelty RFC2328-dokumentissa, joka on laajimpia yksittäisiä RFC-dokumentteja. OSPF-protokollaan liittyviä käsitteitä ovat hierarkisuus, alueet, erityyppiset yhteystilailmoitukset ja erilaiset reitittimien roolit. OSPF:ää käyttävät reitittimet muodostavat aluksi naapuruussuhteen käyttämällä Hello-nimistä prosessia. Tämän jälkeen reitittimet vaihtavat tietokantojensa sisältöä käyttäen tietokannan kuvaus-, tietuepyyntö- ja tietuepäivityksiä. Kaikki OSPF:n sanomat kuljetetaan IP-protokollan päällä ja käytettävä protokollanumero on 89. (Anttila 2001, 326.)

Protokollan toiminnan perusta on LSDB- eli Link State Database-tietokanta (yhteystilatietokanta). Tietokannassa on kuvattuna kunkin linkin tila. Kuvaus voi sisältää liitynnän IP-osoitteen, verkkomaskin, liittyneen verkon tyypin ja liitynnän suhteen ympäröiviin reitittimiin. LSDB:n ylläpito hoidetaan ryhmälähetys-päivityksillä. OSPF:lle varatut ryhmälähetys-osoitteet (multicast-osoitteet) ovat 224.0.0.5 ja 224.0.0.6, ensimmäinen osoite on kaikille OSPF-reitittimille ja jälkimmäinen verkon pääreitittimelle. (Anttila 2001, 326.)

3.5.1 OSPF-alueet

Mikäli kyseessä on iso OSPF-verkko, on järkevää jakaa se eri alueisiin eli areoihin. Tällöin alueen sisällä olevien reitittimien linkkitaulu ei kasva liian suureksi. OSPF:n aluehierarkia on kaksitasoinen, ylin taso on runkoalue, johon kaikilla muilla alueilla tulee olla liityntä. Yleensä liityntä on fyysinen, mutta se voidaan muodostaa tarvittaessa jonkin muun alueen kautta. Liikenne alueiden välillä kulkee aina runkoalueen kautta. Alueisiin jakamisella päästään eroon tyypillisestä linkkitilaprotokolliin liittyvästä ongelmasta, suuren verkon reitittimelle kohdistamista muisti- ja prosessorivaatimuksista. Tällöin kunkin alueen reitittimen ei tarvitse tuntea kuin oman alueensa reitit. OSPF:n aluetyyppejä ovat:

1. Normaali alue, tämän alueen reitittimet tuntevat reitit jokaiseen autonomiseen osa-alueeseen ja niihin verkkoihin, jotka on opittu jonkin toisen reititysprotokollan kautta.
2. Tynkäalue (Stub Area), tämän alueen reitittimet tuntevat kaikki autonomisen osa-alueen osa-alueet ja niiden verkot, mutta tälle alueelle ei välitetä muiden reititysprotokollien kautta opittuja reittejä.

3. Täysin tynkä alue (Totally Stub Area), tämän alueen reitittimet tuntevat ainoastaan oman alueensa verkot. Tämä on Ciscon oma laajennus OSPF:ään.

4. Ei niin tynkä alue (Not So Stubby Area), tällainen alue muodostetaan, mikäli OSPF:n tietoja halutaan vaihtaa toisen reititysprotokollan kanssa hitaan linkin yli, tällöin päivityssanomien määrä ja koko vähenee.

(Anttila 2001, 326 - 330.)

Alueet voivat sisältää erityyppisiä verkkoja, OSPF tukee neljää eri verkkotyyppiä:

1. Lähiverkot, kaikki näihin liittyvät reitittimet kuulevat lähiverkon kautta toisilleen lähetetyt sanomat.

2. Point-to-Point-tai Point-to-Multipoint-verkot. Point-to-Point verkoissa on yhteys ainoastaan kahden reitittimen välillä. Point-to-Multipoint-verkossa on taas yksi fyysinen yhteys ulos, joka on jaettu useammaksi loogiseksi yhteydeksi.

3. NBMA-verkot (Non-Broadcast Multiple Access) ovat muun muassa Frame Relay- ja ATM-verkot. Näissä verkoissa useammalla laitteella on yhteys samaan verkkoon, mutta ne eivät näe toisilleen suunnattua liikennettä. Näissä verkkotyypeissä on omat mekanisminsa päivityssanomien levitykselle.

(Anttila 2001, 326 - 330.)

3.5.2 Reitittimien roolit

OSPF-protokollaa käyttävillä reitittimillä on myös erilaisia rooleja:

1. Sisäinen reititin, tämä reititin kuuluu vain yhteen alueeseen, tämä tyyppi ei sisällä mitään erityistä toiminnallisuutta.
2. Runkoreititin toimii runkoalueen sisällä, tälläkään ei ole mitään erityistä toiminnallisuutta.
3. Aluerajareititin (Area Border Router) toimii kahden alueen välillä. Näitä voi olla useita kahden alueen välillä ja samoin yksi reititin voi toimia runkoalueen ja usean muun alueen välillä. Tämän reitittimen tehtäviin kuuluu välittää ja myös suodattaa reititystietoja alueiden välillä.
4. AS-rajareititin toimii autonomisten alueiden välillä, tämäkin reititin välittää ja suodattaa reititystietoja autonomisten järjestelmien välillä. Lisäksi sen tehtäviin kuuluu hoitaa normaalin IP-liikenteen välitys järjestelmästä toiseen.

(Anttila 2001, 326 - 330.)

3.5.3 OSPF- algoritmin toiminta

Reititystaulu muodostetaan yhteystilatietokannan perusteella. Seuraavassa esitellään lyhyesti yhteystila-algoritmin eteneminen:

1. Reitittimen käynnistyessä tai sen reititystietoihin tullessa muutoksia, se lähettää verkkoon yhteystilamainostuksen, joka sisältää tarvittavat tiedot uudesta tilanteesta. Ja koska kyseessä on OSPF, vain muuttuneet tiedot välitetään muille reitittimille.

2. Samassa alueessa olevat reitittimet välittävät muuttuneen tiedon muille alueen OSPF-reitittimille. Eli toisin sanoen alkuperäinen sanoma kopioidaan ja lähetetään eteenpäin.

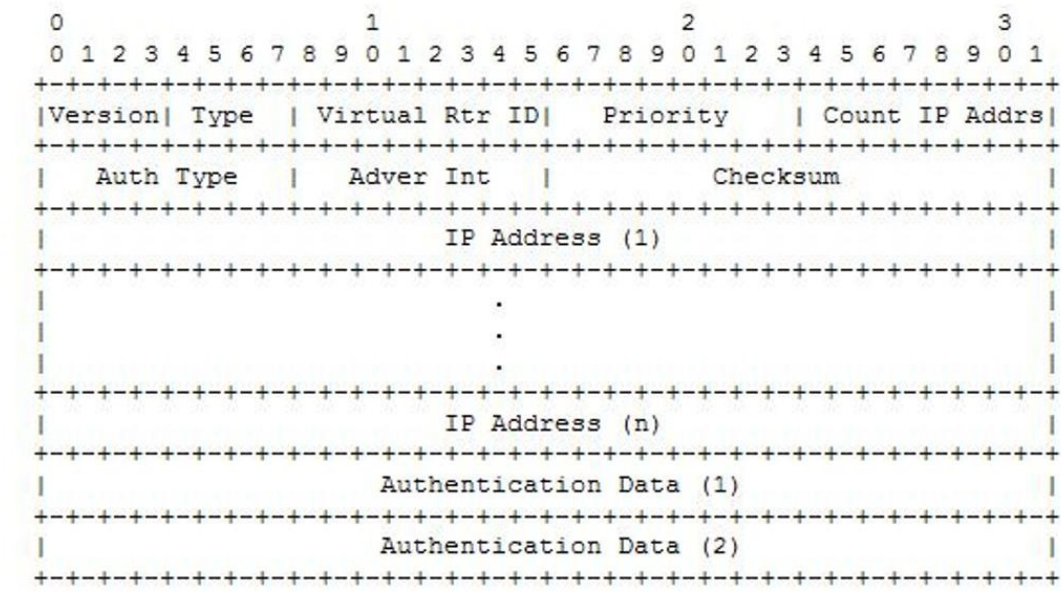
3. Kun alueen kaikilla reitittimillä on identtiset tiedot alueesta, kukin reititin laskee paikallisesti lyhyimmän polun verkkonsa kaikkiin kohteisiin. Laskennassa käytetään Dijkstran algoritmia, tätä algoritmia käyttämällä voidaan varmistua, että reitityssilmukoita ei synny hajautetusta laskennasta huolimatta. Reititystaulu päivitetään laskennan perusteella.
4. Kun verkossa tapahtuu muutoksia, lähetetään yhteystilamainostuksia edellä kuvatulla tavalla ja verkon reittien laskenta uusitaan. Jos muutoksia ei tapahdu, reitittimet tarkkailevat toistensa tiloja jatkuvasti, jotta kaatuneet reitittimet voidaan ottaa huomioon. Nämä tarkkailu-viestit ovat nimeltään Hello-viestejä. (Anttila 2001, 326 - 330.)

3.6 VRRP

OSPF:n tehtävänä on ylläpitää reittejä ja toipua linkkien kaatumisesta, sen tehtävänä ei kuitenkaan ole varmistaa varsinaisten reitittimien toimintaa. Tähän tarkoitukseen on olemassa VRRP (Virtual Router Redundancy Protocol) ja Ciscon oma protokolla, HSRP (Hot Stanby Routing Protocol). VRRP on IETF:n standardoima, laitevalmistajariippumaton protokolla. VRRP on määritelty RFC2338:ssa. VRRP:n tehtävänä on muodostaa reititinryhmiä, jotka varmistavat toisiaan. Yleensä kyseessä on kahden reitittimen pari, mutta ryhmässä voi olla useampikin reititin.

VRRP on OSI-mallin kuljetuskerroksen protokolla ja sille on allokoitu ryhmälähetysosoite (multicast-osoite) 224.0.0.18. Myös VRRP:n toiminta perustuu hello-viestien lähettämiseen. VRRP-kehys kulkee verkossa IP-kehyksen sisällä. (Kaario 2002, 103.)

Kuviossa 6 on kuvattu VRRP:n kehysrakenne.



KUVIO 6. VRRP:n kehysrakenne. (Virtual Router Redundancy Protocol RFC2338 1998.)

Kehys alkaa versionumeron ilmaisemalla kentällä (Version) ja se voi olla maksimissaan 2. Seuraava kenttä määrittelee VRRP-paketin tyypin (Type), joka on numeroltaan 1, Advertisement, ja se on ainoa määritelty tyyppi. Mikäli vastaanotetaan paketti tuntemattomalla tyyppinumerolla, se hylätään. Seuraava kenttä on VRID eli virtuaalireitittimen numero, tämä kertoo, minkä virtuaalireitittimen tietoja kyseisessä paketissa kuljetetaan. Prioriteettikenttä (Priority) kertoo paketin lähettäjän prioriteetin kyseisen virtuaalireitittimen master-reititintä valitessa. VRRP-reititin, joka omistaa virtuaalireitittimelle assosioidun IP-osoitteen, saa korkeimman mahdollisen prioriteettiarvon, joka on 255. Täten kyseinen reititin valitaan master-reitittimeksi aina kun se on toimintakunnossa. Oletusarvo varareitittimien prioriteettikentälle on 100. Seuraavassa kentässä (Count IP Addrs) kerrotaan kyseisessä VRRP-mainostuksessa olevien IP-osoitteiden lukumäärä. Tätä seuraava kenttä (Auth Type) kertoo käytetyn autentikointimenetelmän. Mikäli kentässä on arvo 0, autentikointia ei käytetä. Arvolla 1 käytössä on selkokielinen salasana ja arvolla 2 ilmaistaan, että käytetään IP-protokollan keinoja. Mainostusväli (Adver Int) kertoo peräkkäisten mainostusten välisen ajan sekunneissa, oletusarvoisesti se on 1.

Mitä pidempi mainostusväli on, sitä hitaammin reitittimet toipuvat virhetilanteessa. Seuraavassa kentässä ilmaistaan tarkistussumma (Checksum). IP-osoitteiden lista (IP Address) kertoo yhden tai useamman kyseiseen virtuaalireitittimeen assosioidun IP-osoitteen. Viimeisessä kentässä on autentikointidata (Authetication Data), tälle kentälle on käyttöä vain, jos käytetään selkokielistä salasanaa. (Kaario 2002, 105.)

Oleellista VRRP:n toiminnassa on virtuaalisen IP-osoitteen lisäksi virtuaalinen MAC-osoite. VRRP-reitittimet lähettävät toisilleen sanomia liityntöjen oikeilla MAC-osoitteille, mutta verkon käyttäjille virtuaalireitittimen pitää näkyä virtuaalisella MAC-osoitteella. Ethernet-verkossa virtuaalinen MAC-osoite on aina muotoa 00-00-5E-00-01-{VRID}, jossa VRID on virtuaalireitittimen tunniste ja se voi maksimissaan olla 255. (Kaario 2002, 104.)

Esimerkki Ciscon sekä primääri- että sekundääri-reitittimien konfiguraatiosta:

```
interface FastEthernet0/1
ip address 10.10.10.3 255.255.255.0
vrrp 11 ip 10.10.1.1
vrrp 11 priority 110
vrrp 11 authentication cisco
vrrp 11 track 1

interface FastEthernet0/1
ip address 10.10.10.3 255.255.255.0
vrrp 11 ip 10.10.1.1
vrrp 11 priority 105
vrrp 11 authentication cisco
vrrp 11 track 1
```

IP-osoitteet ovat konfiguroitu fyysisiin liityntöihin, VRRP:n alle konfiguroidaan virtuaalinen IP, joka on samasta aliverkosta, kuin fyysisten liityntöjen IP-osoitteet. Priority-konfiguraatiolla määritellään toinen reitittimistä primääriksi. Primääri-reititin on aina korkeamman priority-arvon omaava reititin. Authentication-rivillä määritellään avain, jonka on oltava sama molemmissa reitittimissä. Avaimella varmistutaan siitä, että kyseessä on oikea reititinpari.
Seuraavaksi esimerkki Juniperin primääri-reitittimen konfiguraatiosta:

```
ge-0/0/0 {
    gigether-options {
        auto-negotiation;
    }
    unit 0 {
        description Customer_LAN;
        family inet {
            address 10.10.10.2/24 {
            vrrp-group 10 {
                virtual-address 10.10.10.1;
                priority 110;
                preempt;
                accept-data;
                authentication-type simple;
                authentication-key "$9$0P-HIhr7NV4aUjHnCtOcSrev"; ## SECRET-
DATA
                track {
                    interface ge-3/0/0 {
                        priority-cost 10;
                    }
                }
            }
        }
    }
}
```

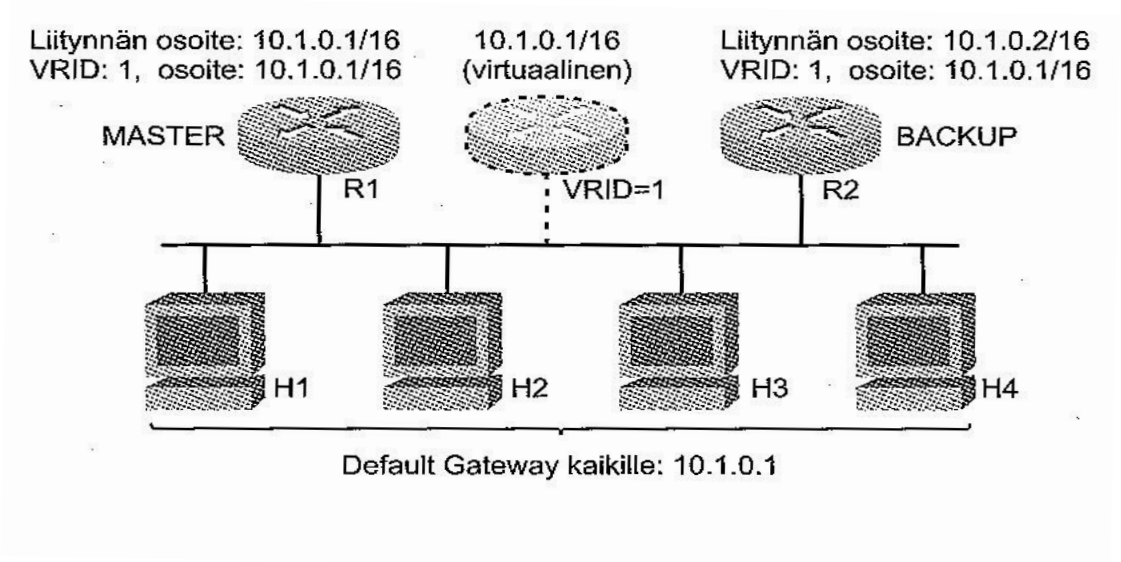
Esimerkki Juniperin sekundääri-reitittimen konfiguraatiosta:

```
ge-0/0/0 {
    unit 0 {
        description LAN;
        family inet {
            address 10.10.10.3/24 {
                vrrp-group 10 {
                    virtual-address 10.10.10.1;
                    priority 105;
                    preempt;
                    accept-data;
                    authentication-type simple;
                    authentication-key "$9$/u4CCA0eK8-VYuO4JZU.mtuO"; ## SECRET-
DATA
                    track {
                        interface ge-3/0/0 {
                            priority-cost 10;
                        }
                    }
                }
            }
        }
```

```
    }
}
```

VRRP:N TOIMINTA

Kuviossa 7 on esitetty tyypillinen tapa käyttää VRRP:tä varmennukseen. Topologiassa neljä samaan aliverkkoon kuuluvaa laitetta käyttää oletusreitittimenään reititintä, jonka IP-osoite on 10.1.0.1. Tämä osoite on fyysisesti reititin R1:llä ja tästä voidaan päätellä, että se toimii ensisijaisena VRRP-reitittimenä eli master-reitittimenä ollessaan toiminnassa. Master-reititin lähettää tietyin väliajoin multicast-viestejä, joissa se ilmoittaa olevansa hengissä. Jos R1 jostain syystä kaatuu eikä pysty lähettämään multicast-viestejä tai mahdollinen track-interface menee alas, ottaa reitittin R2 hoitaakseen R1:n tehtävät. (Kaario 2002, 104.)



KUVIO 7. Tyypillinen VRRP-varmennuksen toteutus. (Kaario 2002,104.)

3.7 HSRP

HSRP on Ciscon oma protokolla, jolla tehdään varmennus kahdella tai useammalla reitittimellä. HSRP on määritelty RFC 2281:ssä. Protokollan toiminta perustuu virtuaalisiin IP- ja MAC-osoitteisiin. HSRP-ryhmässä on aina primäärireititin ja backup-reititin, joka on standby-tilassa valmiina ottamaan paketinvälityksen tehtäväkseen, mikäli primäärireititin jostain syystä kaatuu. Primäärireititin valitaan lähettämällä

multicast-viestejä, joissa välitetään reitittimen prioriteettiarvo, joka oletusarvoisesti on 100. Primäärireitittimeksi valitaan korkeimman prioriteetin omaava reititin.

HSRP-protokollaa käyttävät reitittimet vaihtavat keskenään seuraavia viestejä:

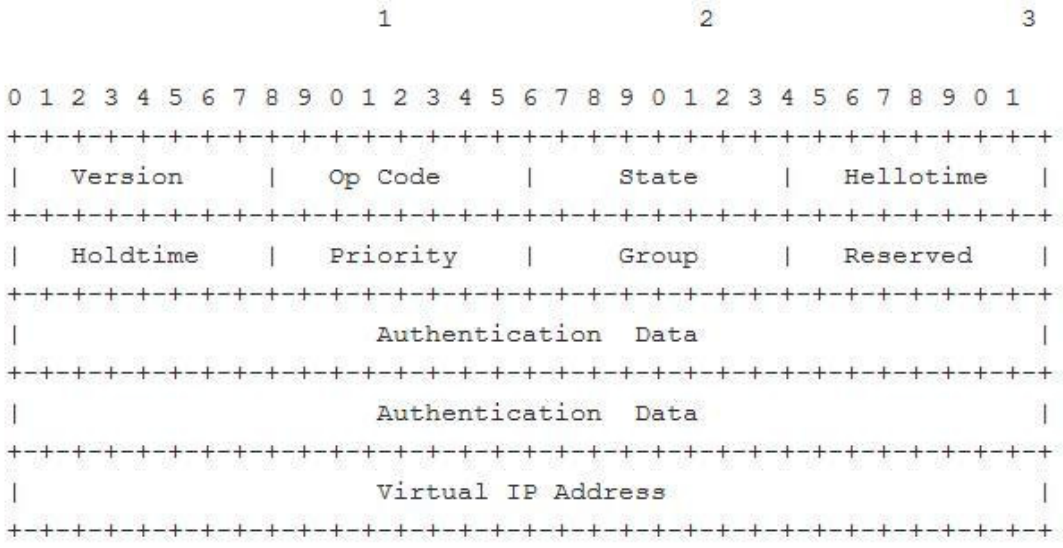
- Hello-kertoo toisille HSRP-reitittimille HSRP:n tilan prioriteetin, näiden viestien oletusintervalli on 3 sekuntia
- Coup-varareititin muuttaa tilansa aktiiviseksi
- Resign-aktiivinen eli primäärireititin lähettää viestin, kun on sammumassa tai kun saa Hello-viestin korkeamman prioriteetin omaavalta reitittimeltä

Reititin, johon on konfiguroitu HSRP, on jossain seuraavista tiloista:

- Active-reititin suorittaa paketinvälitystä eli on näin ollen primäärireititin
- Standby-reititin on valmistautunut ottamaan paketinvälitys-tehtävät, mikäli primäärireititin vikaantuu
- Speaking and listening-reititin lähettää ja ottaa vastaan Hello-viestejä
- Listening-reititin ottaa vastaan Hello-viestejä

(Using HSRP for Fault-Tolerant IP Routing 2009.)

Kuviossa 8 on esitetty HSRP:n kehysrakenne.



KUVIO 8. HSRP:n keshysrakenne. (Cisco Hot Standby Router Protocol RFC 2281, 1998.)

Kehyksen ensimmäinen kenttä (Version) kertoo HSRP:n version. Seuraava kenttä (Op Code) ilmaisee, mikä kolmesta HSRP-viestistä on kyseessä (0 – Hello, 1 – Coup, 2 – Resign). State-kenttä ilmaisee viestin lähettäneen reitittimen sen hetkisen tilan (0 – Initial, 1 – Learn, 2 – Listen, 4 – Speak, 8 – Standby, 16 – Active). Hellotime-kenttä kertoo arvioidun aikavälin reitittimen lähettämien Hello-viestien välillä. Kuten nimestä voi päätellä, kenttä on merkityksellinen vain Hello-viestissä. Seuraava kenttä on Holdtime ja tämäkin kenttä on merkityksellinen vain Hello-viestissä. Kenttä kertoo ajan, kuinka kauan kyseessä oleva Hello-viesti on voimassa. Holdtime:n pitäisi olla kolme kertaa Hellotime. Priority-kenttää käytetään active- ja standby-reitittimien valinnassa, suurimman priority-arvon omaava reititin valitaan active-reitittimeksi. Mikäli reitittimillä on sama priority-arvo, valitaan active-reitittimeksi laite, jolla on suurempi IP-osoite. Group-kenttä kertoo reitittimelle konfiguroidun HSRP-ryhmän ja se voi olla 0-255. Authentication data-kenttä sisältää selkokielisen, 8 merkkiä sisältävän salasanan, mikäli autentikointi on konfiguroitu käyttöön. Viimeinen kenttä kertoo kyseessä olevan ryhmän virtuaali-IP:n. (Cisco Hot Standby Router Protocol RFC 2281, 1998.)

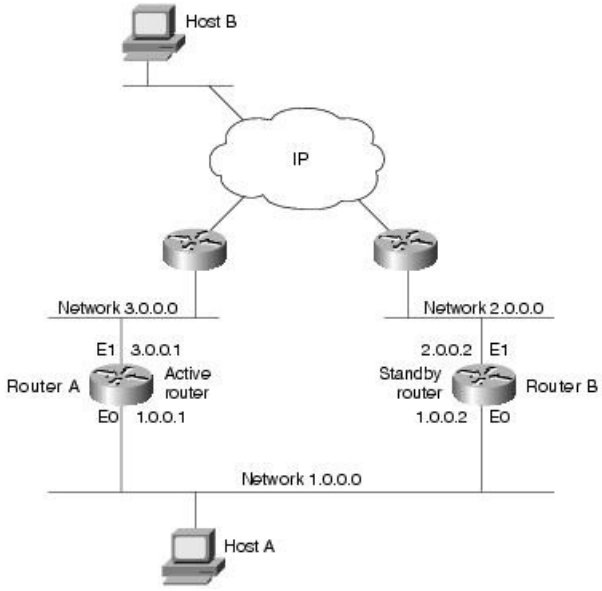
Esimerkki Ciscon reitittimen konfiguraatiosta:

```
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
standby 1 ip 10.10.10.1
standby 1 priority 110
standby 1 preempt
standby 1 track ATM0/0/0

interface FastEthernet0/0
ip address 10.10.10.3 255.255.255.0
standby 1 ip 10.10.10.1
standby 1 priority 105
standby 1 preempt
standby 1 track ATM0/0/0
```

Edellä esitellyissä konfiguraatioissa fyysisille liitynnöille on määritetty IP-osoitteet. Virtuaalinen IP-osoite määritetään käskyllä standby 1 ip, virtuaalinen IP-osoite toimii lähiverkossa olevien laitteiden oletus yhdyskäytävänä. Tässä konfiguraatiossa HSRP-ryhmä on määritelty yhdeksi. Mikäli standby-ryhmää ei erikseen määritellä, on se nolla. Priority-käskyllä määritetään reitittimille primääri/sekundääri-roolit. Reititin, jonka priority-arvo on suurempi, on primääri-reititin. Primääri-reititin huolehtii liikenteen välityksestä normaalitilanteessa. Primääri-reitittimen vikaantuessa, liikenne kääntyy sekundääri-reitittimelle. Oletusarvona Ciscon reitittimillä on priority 100. Preempt-käskyllä mahdollistetaan, että kyseinen reititin voi ottaa primärireitit-timen aseman, mikäli sen prioriteetti-arvo on ryhmän suurin. Käskyyn voidaan sisällyttää myös attribuutti, jolla määritellään viive roolien vaihtamiselle, tällä viiveellä annetaan käytössä olevalle reititysprotokollalle aikaa konvergoitua. Track-käskyllä määritellään liityntä, jonka tilaa seurataan. Mikäli primääri-reitittimen interface ATM0/0/0 jostain syystä putoaa alas, vähennetään ko. reitittimen priority-arvoa kymmenellä, tällöin pääreitittimen priority on pienempi, kuin sekundääri-reitittimen ja sekundääri-reititin ottaa primääri-reitittimen tehtävät. (Using HSRP for Fault-Tolerant IP Routing 2009.)

HSRP:N TOIMINTA

Kuviossa 9 Router A on primäärireititin eli active-reititin ja Router B standby-reititin. Normaalitilanteessa reitittimet lähettävät multicastina Hello-viestejä tietyin väliajoin ja odottavat niihin vastausta. Kun Router A vikaantuu, Router B odottaa edellisessä Hello-viestissä määritellyn Holdtime-ajan uutta Hello-viestiä Router A:lta ja jos Holdtime-aika menee umpeen, lähettää Router B multicastina Coup-viestin, jossa ilmaistaan, että Router B:n tila muuttuu stanby:sta aktiiviseksi. (Using HSRP for Fault-Tolerant IP Routing 2009.)



KUVIO 9. Esimerkki verkosta, jossa on HSRP käytössä. (Using HSRP for Fault-Tolerant IP Routing 2009.)

4 VERKKO JA KONFIGURAATIOT

4.1 Yleistä

Työssä oli tarkoituksena testata eri protokollien ja reitittimien kahdennuksen toimivuutta. Alkuperäisen suunnitelman mukaan oli tarkoitus testata konfiguraatioiden toimivuutta operaattorin runkoverkkoa vasten, mutta tästä suunnitelmasta jouduttiin luopumaan tietoturvasyistä. Päädyttiin rakentamaan erillinen testausympäristö, josta ei ole pääsyä ulkopuolisiin verkkoihin.

Käytettävissä oli Ciscon ja Juniperin laitteita. Toimivuutta testattiin seuraavilla yhdistelmillä:

- Ciscon reitittimet, protokollina HSRP ja BGP
- Pääreititin Juniper, varareititin Cisco, protokollina BGP ja VRRP
- Pääliittymänä Juniperin reititin ja varalaitteena Ciscon reititin, protokollina BGP ja OSPF, lan:ssa olevissa kytkimissä protokollina OSPF ja HSRP

Testaukset suoritettiin kahdella eri topologialla, kuvat topologioista(kuviot 11 ja 16) on esitetty kyseisten testien yhteydessä.

Testauksessa käytetyt laitteet ja laitteissa olevat ohjelmistot:
mariedger01: Cisco 3750-24TE; IOS c3750me-i5-mz.122-25.EY4
mariedger02: Cisco 3620; IOS c3620-i-mz.112-16.P
maricper01: Cisco WS-C3550-12G; IOS c3550-i5q3l2-mz.121-22.EA1a ja Juniper SRX210-LM; JUNOS release 10.0R1.8
maricper02: Cisco WS-C3550-12G; IOS c3550-ipservices-mz.122-44.SE6 ja Cisco 1812; IOS c181x-advipservicesk9-mz.124-6.T11.bin
mariswi01 ja -02: cisco WS-C3550-12G; IOS c3550-i5q3l2-mz.121-22.EA1a ja c3550-ipservices-mz.122-44.SE6
switch: cisco WS-C2950G-24, IOS EI c2950-i6q4l2-mz.121-22.EA11.bin
Metroverkkoa simuloiva kytkin: HP Procurve 2610-24; R.11.22

TESTAUSSUUNNITELMA

Liikenteen kääntyminen varayhteydelle testattiin seuraavilla tavoilla jokaisella laite- ja protokolla-yhdistelmällä:

- suljetaan BGP-naapuruus edge-laitteelta, jolloin simuloidaan edgen hajoaminen
- pääliittymä virrattomaksi, tällä simuloidaan reitittimen hajoamista tai virtakatkosta
- pääliittymän wan-portin kuitu irti, tällä simuloidaan fyysisen runkoyhteyden rikkoontuminen
- pääliittymän lan-portin kuitu irti, tällä saadaan simuloitua lan-portin vikaantuminen, asiakkaan lan-kuidun/kuparin katkeaminen tai lan:ssa olevan kytkimen hajoaminen

Aiemmin on havaittu, että parhaiten oikeaa vikatilannetta simuloi nimenomaan kuitujen/kuparin irrottaminen eikä niinkään reitittimen portin sulkeminen ohjelmallisesti.

Jokainen edellä mainituista testeistä tehtiin kolme kertaa.

Liikenteen tarkasteluun käytettiin testi-PC:llä olevaa Wireshark-ohjelmaa. Jokaisessa testissä testi-PC:ltä ajettiin jatkuvaa pingiä mariedger01:n loopback0:n IP-osoitteeseen. Testi-PC:n IP-osoitteeksi oli määritetty 192.168.100.100 ja default gatewayksi 192.168.100.1, mikä on sekä HSRP:n että VRRP:n virtuaalinen osoite.

Samoihin mittauksiin otettiin myös mukaan liikenteen kääntyminen takaisin pääyhteydelle, kun simuloitu vikatilanne oli ohi.

Reitittimien konfiguraatiot pyrittiin pitämään mahdollisimman karsittuina, vaikka kyseessä olikin pieni verkko.
BGP:n timereiden aikoja päädyttiin muuttamaan jo suunnitteluvaiheessa, default-arvot timereille ovat 60 sekuntia (keepalive) ja 180 sekuntia (holdtime) ja joissakin

tapauksissa jopa yli kolmen minuutin konvergoitumisaika on liikaa. BGP:n timereiksi valittiin 10 sekuntia (keepalive) ja 30 sekuntia (holdtime), jotka ovat melko yleisesti käytössä. Aiemman kokemuksen perusteella voidaan todeta, että kyseessä olevat ajastimet toimivat suuremmissa yritysverkoissa, joissa tämän tyyppisiä varmennus-ratkaisuja käytetään, hyvin. Mikäli ajastimia pienennetään liian pieniksi, voivat heiluvat reitit aiheuttavat ylimääräistä reittitietojen päivitystä ja näin ollen vaikuttaa verkon ja laitteiden suoritus- ja läpäisykykyyn. Kyseisillä ajastimilla konfiguroidun verkon konvergoitumisaika vaihtelee karkeasti ottaen 20 - 40 sekunnin välillä.

BGP:n reitityspolitiikka suunniteltiin siten, että route-map:lla manipuloitiin BGP:n attribuutteja; local preferenceä ja AS-polkua. Sekä local preference että AS-polku-attribuutit ovat BGP:n yleisiä reitinvalinta-parametreja, joten ne toimivat samalla tavalla sekä Ciscon että Juniperin laitteissa. Parametreilla säädetään reittien mainostuminen normaalitilanteessa, eli kun molemmat liittymät ovat toiminnassa, siten, että liikenne kulkee pääyhteyden kautta.

Pääliittymällä asetetaan mariedger01:ltä mainostuvien reittien local prefence-arvoksi 200, jolloin pääliittymä mainostaa iBGP-naapureille ulkoisia reittejä local preferencellä 200. Varayhteys saa samat ulkoiset reitit oman wan-linkkinsä kautta local preferencen oletusarvolla, joka on 100. Näin ollen varayhteyden BGP-taulussa on kaksi reittiä ulkoisiin verkkoihin. Varayhteyden reititin vertaa BGP-taulun reittejä ja asettaa niistä paremman reititystauluunsa. Seuraavassa tulosteessa on BGP-taulu maricper02:lta, kun tilanne on normaali. Kuten tulosteesta voidaan havaita, BGP-taulussa on kaksi riviä esim. verkolle 172.16.1.1/32, toinen pääliittymän kautta (Next Hop 192.168.100.2) ja toinen varayhteyden wan-linkin kautta (Next Hop 10.10.11.2).

```
maricper02#sh ip bgp
BGP table version is 27652, local router ID is 172.16.1.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal,
              r RIB-failure, S Stale
Origin codes: i -IGP, e -EGP, ? -incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i10.10.10.0/30    192.168.100.2            0    100      0 ?
*                   10.10.11.2                            0 65000 ?
```

```
* i10.10.11.0/30    10.10.10.2              200      0       65000 ?
*                   10.10.11.2          0            0       65000 ?
*>                  0.0.0.0             0            32768   ?
*>i10.10.100.0/30 10.10.10.2            0    200     0       65000 ?
*                   10.10.11.2          0            0       65000 ?
*>i172.16.1.1/32   10.10.10.2          0    200     0       65000 ?
*                   10.10.11.2                       0       65000 ?
*>i172.16.1.2/32   192.168.100.2       0    100     0       ?
*> 172.16.1.3/32    0.0.0.0             0            32768   ?
*>i172.16.2.1/32    10.10.10.2              200      0       65000 ?
*                   10.10.11.2          0            0       65000 ?
* i192.168.100.0    192.168.100.2       0    100     0       ?
*>                  0.0.0.0             0            32768   ?
```

Seuraavassa tulosteessa näkyy maricper02:n reititystaulu, josta voidaan havaita, että reititystauluun on asennettu vain pääyhteyden kautta mainostuva prefiksi, koska sen local preferencen arvo on parempi.

```
maricper02#sh ip rou
Codes: C -connected, S -static, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
       E1 -OSPF external type 1, E2 -OSPF external type 2
       i -IS-IS, su -IS-IS summary, L1 -IS-IS level-1, L2 -IS-IS level-2
       ia -IS-IS inter area, * -candidate default, U -per-user static route
       o -ODR, P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/32 is subnetted, 4 subnets
B       172.16.1.1 [200/0] via 10.10.10.2, 00:12:40
C       172.16.1.3 is directly connected, Loopback0
B       172.16.2.1 [200/0] via 10.10.10.2, 00:12:40
B       172.16.1.2 [200/0] via 192.168.100.2, 00:12:40
     10.0.0.0/30 is subnetted, 3 subnets
B       10.10.10.0 [200/0] via 192.168.100.2, 00:12:40
C       10.10.11.0 is directly connected, GigabitEthernet0/12
B       10.10.100.0 [200/0] via 10.10.10.2, 00:12:40
C    192.168.100.0/24 is directly connected, Vlan1
maricper02#
```

Vastaavasti taas varayhteydellä edgelle mainostettavien verkkojen AS-polkua prependataan (pidennetään) kolmella, jolloin pääyhteyden ollessa toiminnassa sitä kautta mainostuvilla verkoilla on lyhyempi AS-polku ja näin ollen ko. reitit asetetaan

edge-laitteiden reititystauluihin. Seuraavassa tulosteessa BGP- ja reititystaulut molemmilta edgeiltä verkon normaalitilassa, eli kun sekä maricper01 että maricper02 on toiminnassa.

```
mariedger01#sh ip bgp
BGP table version is 3304, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal,
              r RIB-failure, S Stale
Origin codes: i -IGP, e -EGP, ? -incomplete

   Network          Next Hop            Metric     LocPrf  Weight  Path
*  10.10.10.0/30    10.10.10.1           0                   0      65499 ?
*>                  0.0.0.0              0                  32768   ?
*>i10.10.11.0/30    10.10.100.2          0          100     0       ?
* i10.10.100.0/30   10.10.100.2          0          100     0       ?
*>                  0.0.0.0              0                  32768   ?
*> 172.16.1.1/32    0.0.0.0              0                  32768   ?
*> 172.16.1.2/32    10.10.10.1           0                  0       65499 ?
*> 172.16.1.3/32    10.10.10.1                              0       65499 ?
*>i172.16.2.1/32    10.10.100.2           0         100     0       ?
*> 192.168.100.0    10.10.10.1            0                 0       65499 ?
```

```
mariedger02#sh ip bgp
BGP table version is 30, local router ID is 172.16.2.1
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
*  10.10.10.0/30    10.10.11.1                      0      65499 65499 65499 65499 ?
*>i                  10.10.100.1     0      100      0      ?
*  10.10.11.0/30    10.10.11.1      0               0      65499 65499 65499 65499 ?
*>                  0.0.0.0         0               32768  ?
* i10.10.100.0/30   10.10.100.1     0      100      0      ?
*>                  0.0.0.0         0               32768  ?
*>i172.16.1.1/32    10.10.100.1     0      100      0      ?
*  172.16.1.2/32    10.10.11.1                      0      65499 65499 65499 65499 ?
*>i                 10.10.10.1      0      100      0      65499 ?
*>i172.16.1.3/32    10.10.10.1      0      100      0      65499 ?
*                   10.10.11.1      0               0      65499 65499 65499 65499 ?
*> 172.16.2.1/32    0.0.0.0         0               32768  ?
*>i192.168.100.0    10.10.10.1      0      100      0      65499 ?
*                   10.10.11.1      0               0      65499 65499 65499 65499 ?
```

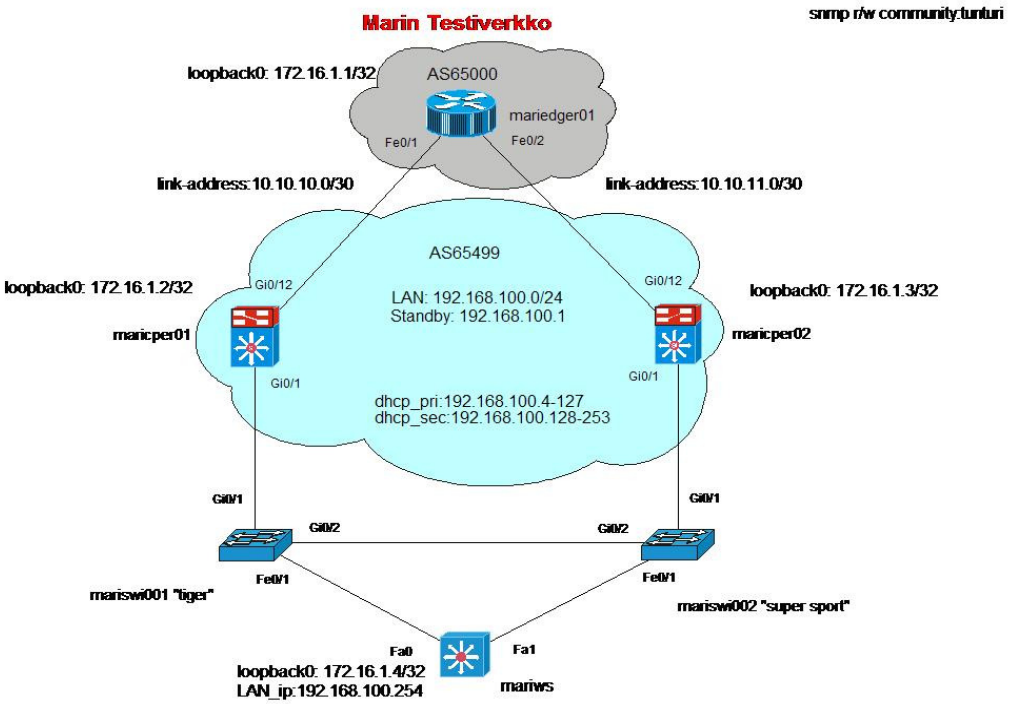
```
mariedger01#sh ip rou
Codes: C -connected, S -static, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
```

```
      E1 -OSPF external type 1, E2 -OSPF external type 2, E -EGP
      i -IS-IS, su -IS-IS summary, L1 -IS-IS level-1, L2 -IS-IS level-2
      ia -IS-IS inter area, * -candidate default, U -per-user static route
      o -ODR, P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/32 is subnetted, 4 subnets
C       172.16.1.1 is directly connected, Loopback0
B       172.16.1.3 [20/0] via 10.10.10.1, 00:14:12
B       172.16.2.1 [200/0] via 10.10.100.2, 06:34:13
B       172.16.1.2 [20/0] via 10.10.10.1, 01:09:35
     10.0.0.0/30 is subnetted, 3 subnets
C       10.10.10.0 is directly connected, FastEthernet1/0/1
B       10.10.11.0 [200/0] via 10.10.100.2, 06:34:13
C       10.10.100.0 is directly connected, FastEthernet1/0/24
B    192.168.100.0/24 [20/0] via 10.10.10.1, 01:09:35

mariedger02#sh ip rou
Codes: C -connected, S -static, I -IGRP, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
       E1 -OSPF external type 1, E2 -OSPF external type 2, E -EGP
       i -IS-IS, L1 -IS-IS level-1, L2 -IS-IS level-2, * -candidate default
       U -per-user static route, o -ODR

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 3 subnets
B       10.10.10.0 [200/0] via 10.10.100.1, 06:33:25
C       10.10.11.0 is directly connected, Ethernet0/0
C       10.10.100.0 is directly connected, Ethernet0/1
B    192.168.100.0/24 [200/0] via 10.10.10.1, 01:08:48
     172.16.0.0/32 is subnetted, 4 subnets
B       172.16.1.1 [200/0] via 10.10.100.1, 06:33:26
B       172.16.1.3 [200/0] via 10.10.10.1, 00:13:25
B       172.16.1.2 [200/0] via 10.10.10.1, 01:08:48
C       172.16.2.1 is directly connected, Loopback0
```

Konfiguraatiot edge-laitteilla pysyivät kaikissa testeissä samoina. Laitteiden täydelliset konfiguraatiot on esitetty liitteissä 1 ja 2. Myös maricper01:n ja maricper02:n konfiguraatiot eBGP:n osalta säilyivät kaikissa testeissä muuttumattomina.

4.2. BGP ja HSRP/VRRP

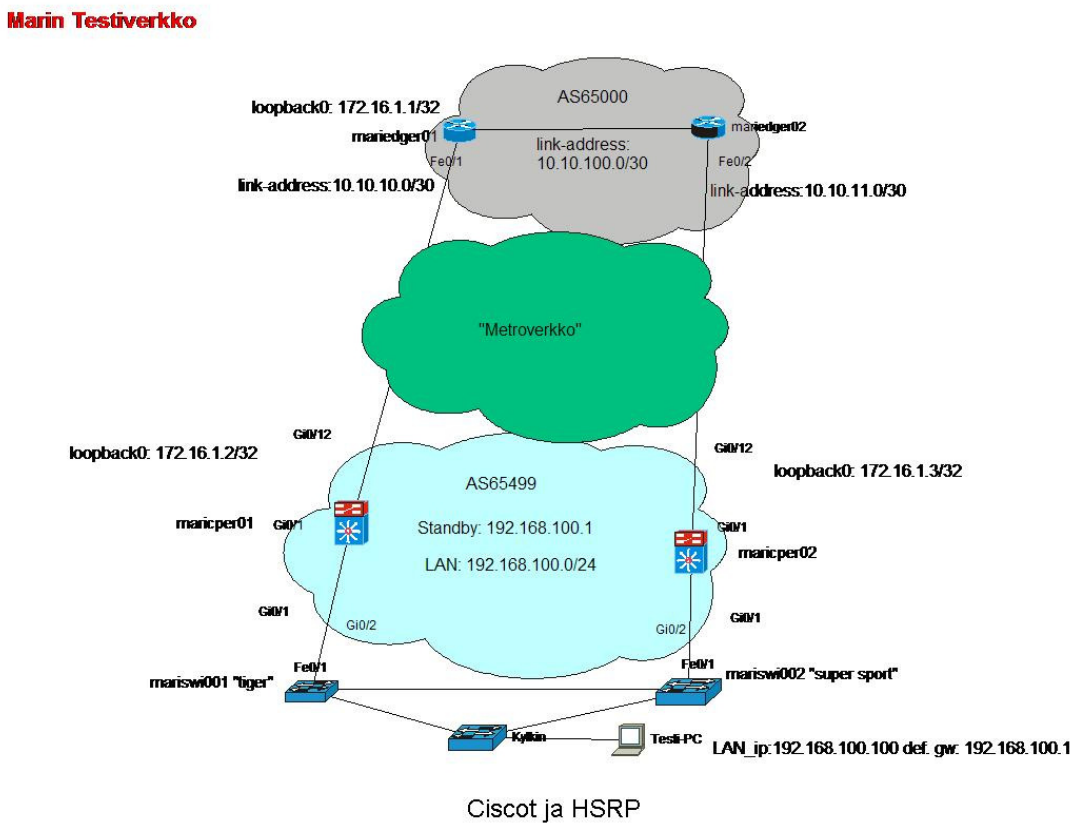
Ensimmäinen testaus suoritettiin kuvion 10 mukaisessa verkossa. Mittausten tulokset herättivät sen verran epäilyksiä, että päätettiin muuttaa verkon fyysistä rakennetta.



KUVIO 10. Ensimmäinen verkkotopologia.

Muutaman tehdyn mittauksen jälkeen havaittiin, että liikenne kääntyi liian nopeasti varayhteydelle eikä BGP:n ajastimien vaikutusta voinut havaita. Syynä tähän käyttäytymiseen oli suora linkki edgen ja cpe:n välillä. Linkin katkeaminen vaikutti siten, että BGP muutti tilaansa heti. Todellisuudessa tällainen tilanne tulee hyvin harvoin vastaan, koska yleensä CPE:n ja edgen välissä on operaattorin runkoverkon laitteita.

Verkkoon lisättiin toinen edge-laite ja cpe-laitteet kytkettiin edge-laitteisiin metroverkkoa simuloivan kytkimen kautta. Näin verkon topologiasta saatiin todenmukaisempi. Muutettu topologia nähdään kuviosta 11.



KUVIO 11. Muutettu verkkotopologia.

Laitteet nimeltä mariedger01 ja –r02 simuloivat operaattorin PE-laitetta. Laitteet maricper01 ja maricper02 ovat tässä tutkittavia asiakaslaitteita. EGP- ja IGP-protokollana käytetään BGP:tä. CPE-laitteet varmentavat toisiaan ja varmennusprotokollana on tässä testissä HSRP Ciscon reititinparilla ja VRRP Juniper-Cisco-parilla.

Kytkimissä on pelkkä oletuskonfiguraatio, jossa on automaattisesti PVST (Per Vlan Spanning Tree) päällä. Spanning Tree protokollaa käytetään kytkinverkoissa silmukoiden estoon. Tässä työssä ei ole tarkoitus perehtyä kytkinverkkoihin ja niissä käytettyihin tekniikoihin.

Maricper01:n (WS-C3550) konfiguraatio liitteessä 3 ja maricper02:n (WS-C3550) konfiguraatio liitteessä 4. Maricper01:n (Juniper SRX210-LM) konfiguraatio liitteessä 5 ja maricper02:n (c1812) liitteessä 6.

4.2.1 BGP naapuruus alas

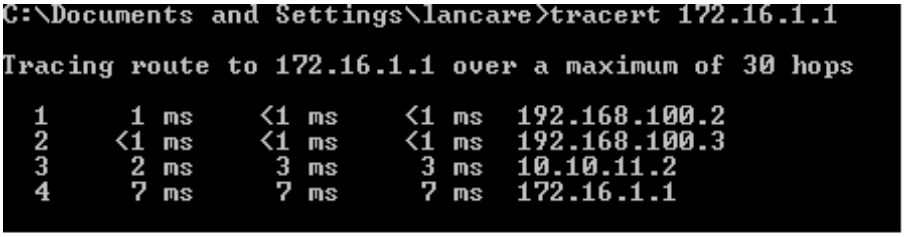
Ensimmäisenä testinä suljettiin laitteelta mariedger01 BGP-naapuruus laitteelle maricper01. Tällä testillä simuloidaan operaattorin PE-laitteen hajoamista. Tässä testissä ei HSRP:n (Ciscon reitittimet) ja VRRP:n (Juniper – Cisco-pari) pitäisi muuttaa lainkaan tilaansa, koska kumpikaan redundantti-protokollista ei reagoi reititysprotokollan muutoksiin. Liikenteen kääntyessä ei pitäisi katkoksen olla kovin pitkä, koska BGP:n mariedger01:llä ei tarvitse reagoida ajastimiin, vaan muutos BGP:n tilassa tapahtuu likimain heti. Ainoastaan reititystaulujen päivitys cpe- ja edge-laitteilla tulee aiheuttamaan hetkellisen katkoksen. Reititystaulun päivitysnopeus riippuu laitteen suorituskyvystä. Normaalissa verkossa katkos voisi olla pidempi, kuin mikä testissä saadaan mitattua, koska yleensä reititystaulut laitteilla ovat pidemmät kuin tällaisessa

CISCO

Kun naapuruus suljettiin mariedger01:ltä, se lähetti Notification-viestin maricper01:lle ja BGP-sessio välillä marierdger01-maricper01 siirtyy Init-tilan kautta Active-tilaan. Maricper01 poistaa BGP-taulustaan mariedger01:ltä oppimansa reitit ja ilmoittaa iBGP naapurilleen (maricper02), että ei enää mainosta ko. reittejä. Samoin mariedger01:nen poistaa BGP-taulustaan maricper01:lta oppimansa reitit ja asentaa BGP-taulusta varayhteyden kautta näkyvät reitit reititystauluunsa. BGP käyttäytyi samoin sekä Ciscon että Juniperin reitittimillä.

Tässä testissä liikenteen kääntyminen tapahtui nopeasti, kuten oli tarkoituskin. Testi-PC:ltä huomattiin ainoastaan yhden ping-paketin katoaminen. Wiresharkin tulosteesta voitiin havaita katkoksen olevan noin 5,2 sekuntia. Kaikissa kolmessa

mittauksessa saatiin likimain sama tulos. Tässä tapauksessa asiakas ei välttämättä edes huomaa liikenteen kääntymistä, ainoastaan kaikkein viive-herkimmät sovellukset saattavat reagoida katkokseen. Kuviossa 12 on tuloste testi-PC:ltä otetusta traceroutesta kohti mariedger01:n loopback0:n IP-osoitetta (172.16.1.1). Tulosteesta voidaan havaita, että liikenne kulkee AS:stä ulos varayhteyden kautta. Ensimmäinen hyppy on pääliittymän lan-interfacen osoite, seuraava hyppy on taas varaliittymän lan-interfacen osoite. Osoite 10.10.11.2 on mariedger02:n ja maricper02:n välisen linkin edgen osoite.



KUVIO 12. Traceroute testi-PC:ltä.

Seuraavassa tulosteessa on BGP-taulu ja reititystaulu tarkisteltuna mariedger01:ltä:

```
mariedger01#sh ip bgp
BGP table version is 163, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal,
              r RIB-failure, S Stale
Origin codes: i -IGP, e -EGP, ? -incomplete

   Network          Next Hop    Metric  LocPrf  Weight  Path
*> 10.0.0.0         10.10.11.1  0                       65499 65499 65499 65499
?
*> 10.10.10.0/30    0.0.0.0     0               32768   ?
*  10.10.11.0/30    10.10.11.1  0       0               65499 65499 65499 65499 ?
*>                  0.0.0.0     0               32768   ?
*> 172.16.0.0       10.10.11.1  0                       65499 65499 65499 65499 ?
*> 172.16.1.1/32    0.0.0.0     0               32768   ?
*> 172.16.1.3/32    10.10.11.1  0       0               65499 65499 65499 65499
?
*> 192.168.100.0    10.10.11.1  0       0               65499 65499 65499 65499 ?
```

BGP-taulun tulosteesta voidaan havaita, että verkko 192.168.100.0/24 mainostuu ainoastaan varayhteyden kautta, koska AS-polku on prependattu (jatkettu) kolme

kertaa. Seuraavasta tulosteesta nähdään, että reititystauluun on asennettu maricper02:n kautta kulkeva reitti.

```
mariedger01#sh ip rou
Codes: C -connected, S -static, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
       E1 -OSPF external type 1, E2 -OSPF external type 2, E -EGP
       i -IS-IS, su -IS-IS summary, L1 -IS-IS level-1, L2 -IS-IS level-2
       ia -IS-IS inter area, * -candidate default, U -per-user static route
       o -ODR, P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.1/32 is directly connected, Loopback0
B       172.16.0.0/16 [20/0] via 10.10.11.1, 00:02:14
B       172.16.1.3/32 [20/0] via 10.10.11.1, 00:02:14
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/30 is directly connected, FastEthernet1/0/1
B       10.0.0.0/8 [20/0] via 10.10.11.1, 00:02:14
C       10.10.11.0/30 is directly connected, FastEthernet1/0/2
B    192.168.100.0/24 [20/0] via 10.10.11.1, 00:02:14
mariedger01#
```

HSRP ei muuta tilaansa, vaan pääliittymä pysyy aktiivisena, kuten alla olevista show-käskyistä voidaan havaita:

```
maricper01#sh stan
Vlan1 -Group 1
  Local state is Active, priority 120, may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 1.022
  Virtual IP address is 192.168.100.1 configured
  Active router is local
  Standby router is 192.168.100.3 expires in 7.076
  Virtual mac address is 0000.0c07.ac01
  Authentication text "mari"
  3 state changes, last state change 18:20:17
  IP redundancy name is "hsrp-Vl1-1" (default)
  Priority tracking 1 interface or object, 1 up:
    Interface or object        Decrement  State
    GigabitEthernet0/12           10      Up
maricper02#sh stand
Vlan1 -Group 1
  State is Standby
```

```
  13 state changes, last state change 18:19:50
Virtual IP address is 192.168.100.1
Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.972 secs
Authentication text "mari"
Preemption enabled
Active router is 192.168.100.2, priority 120 (expires in 9.340 sec)
Standby router is local
Priority 115 (configured 115)
  Track interface GigabitEthernet0/12 state Up decrement 10
IP redundancy name is "hsrp-Vl1-1" (default)
```

Käskyjen tulosteesta voidaan huomata, että hello-viestien intervalli on 3 sekuntia ja pitoaika 10 sekuntia.

Kun liikenne palautettiin pääliittymälle eli BGP-naapuruus nostettiin ylös maried-ger01:ltä, yhtään ping-pakettia ei hävinnyt, ainoastaan yhden paketin viive kasvoi huomattavasti.

JUNIPER

Myös Juniperin tapauksessa liikenne kääntyi varayhteydelle todella nopeasti, yksi ping-paketti hävisi ja Wiresharkin tulosteita tutkimalla saatiin keskimääräiseksi katkosajaksi noin 5 sekuntia. Kun liikenne palautettiin pääyhteydelle, yhtään pakettia ei kadonnut, yhdessä paketissa huomattiin normaali suurempi viive.

Tällä reititin-yhdistelmällä redundantti-protokollana oli käytössä VRRP. Myöskään VRRP ei muuttanut tilaansa tätä testiä tehdessä. Alla tulosteet molempien cpe-laitteiden VRRP:n tilasta:

```
root@maricper01> show vrrp detail
Physical interface: fe-0/0/5, Unit: 0, Address: 192.168.100.2/24
  Index: 73, SNMP ifIndex: 123, VRRP-Traps: disabled
  Interface state: up, Group: 1, State: master, VRRP Mode: Active
  Priority: 110, Advertisement interval: 1, Authentication type: none
  Delay threshold: 100, Computed send rate: 0
  Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 192.168.100.1
  Advertisement Timer: 0.480s, Master router: 192.168.100.2
  Virtual router uptime: 1d 01:32, Master router uptime: 1d 01:32
  Virtual Mac: 00:00:5e:00:01:01
  Tracking: enabled
    Current priority: 110, Configured priority: 110
    Priority hold time: disabled
    Interface tracking: enabled, Interface count: 1
      Interface     Int state   Int speed   Incurred priority cost
      ge-0/0/0.0    up              1g                  0
    Route tracking: disabled
```

```
maricper02#sh vrrp
Vlan1 -Group 1
  State is Backup
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
    Track object 1 state Up decrement 1
  Master Router is 192.168.100.2, priority is 110
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec (expires in 3.273 sec)
```

4.2.2 Maricper02 virrattomaksi

Tämä testi simuloi sähkökatkoa tai laitteen vikaantumista. Tässä testissä molempien redundantti-protokollien pitäisi muuttaa tilaansa ja liikenteen pitäisi siirtyä varayhteydelle. Redundantti-protokollien kääntymisen ei pitäisi vaikuttaa katkoksen pituuteen, koska niiden timerit ovat huomattavasti pienemmät kuin BGP:n, joten niiden pitäisi reagoida noin kolmessa sekunnissa pääliittymän sammumiseen. Reitityksen pitäisi kääntyä 20 - 40 sekunnissa, johtuen BGP:n ajastimista.

CISCO

Seuraavaksi sammutettiin pääliittymä, jolloin sekä BGP-mainostus että HSRP kääntyivät varayhteydelle. Tässä tapauksessa havaittiin selkeä katkos liikenteelle, ping-paketteja hävisi maksimissaan kahdeksan. Kolmen mittauksen perusteella keskimääräinen katkosaika liikenteessä oli noin 32,8 sekuntia. Tämä katkos johtuu siitä, että BGP:n timerit oli asetettu 10 ja 30 sekuntiin, eli 10 sekunnin välein reitittimet lähettävät toisilleen keepalive-viestejä, mikäli toinen osapuoli ei saa keepalive-viestiä 30 sekuntiin, se poistaa naapurilta opitut reitit BGP-taulusta ja sulkee BGP-istunnon kyseiseen naapuriin.
Kuviossa 13 olevasta Wiresharkin tulosteesta voidaan havaita, että tässä mittauksessa ping-paketteja katosi kahdeksan (rivit 177 - 223).

171 50.330409	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
172 50.885666	192.168.100.2	224.0.0.2	HSRP	Hello (state Active)
173 51.134221	192.168.100.3	224.0.0.2	HSRP	Advertise (state Passive)
174 51.329565	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
175 51.330411	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
177 52.329618	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
178 52.890049	192.168.100.3	224.0.0.2	HSRP	Hello (state Standby)
181 55.890074	192.168.100.3	224.0.0.2	HSRP	Hello (state Standby)
183 57.657758	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
185 58.890111	192.168.100.3	224.0.0.2	HSRP	Hello (state Standby)
187 60.886383	192.168.100.3	224.0.0.2	HSRP	Advertise (state Active)
188 60.886395	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
192 63.157844	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
193 63.886181	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
199 66.886212	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
203 68.657895	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
204 68.658253	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
205 69.886503	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
208 72.014401	192.168.100.3	192.168.100.2	BGP	KEEPALIVE Message, KEEPALIVE Message
209 72.886307	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
210 73.402468	192.168.100.3	192.168.100.2	BGP	KEEPALIVE Message
212 74.157966	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
213 74.158331	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
217 75.886341	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
219 76.474889	192.168.100.3	192.168.100.2	BGP	NOTIFICATION Message
220 76.475709	192.168.100.3	192.168.100.2	TCP	bgp > irisa [FIN, PSH, ACK] Seq=79 Ack=1 Win=15263 Len=0
222 78.886371	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
223 79.658052	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
225 81.710640	192.168.100.3	192.168.100.2	BGP	[TCP Retransmission] KEEPALIVE Message, KEEPALIVE Message, KEEPALIVE Message, NOTIFICATION Message
226 81.886407	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
229 84.886454	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
230 85.158099	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
231 85.167321	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply

KUVIO 13. Maricper01:n sammutus.

Alla olevasta show-käskyn tulosteesta nähdään, että varaliittymä on HSRP:n kannalta muuttunut pääliittymäksi (Active router is local), vastaavasti varaliittymä on tuntematon (Standby router is unknown), koska tässä tapauksessa on vain kaksi toisiaan varmistavaa liittymää ja toinen liittymä on virrattomana:

```
maricper02#sh stand
Vlan1 -Group 1
  State is Active
    14 state changes, last state change 00:02:31
  Virtual IP address is 192.168.100.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.320 secs
  Authentication text "mari"
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 115 (configured 115)
    Track interface GigabitEthernet0/12 state Up decrement 10
  IP redundancy name is "hsrp-Vl1-1" (default)
```

Kun liikenne kääntyi takaisin pääliittymälle, ainoastaan yksi ping-paketti katosi. Katkos liikenteelle oli noin 5,5 sekunnin luokkaa. Kuviosta 14 nähdään HSRP:n käyttämät viestit ja tilat, kun pääliittymä käynnistyy. Tulosteesta voidaan päätellä, että pääreitittimen käynnistyessä se lähettää Coup-viestin, jossa se ilmoittaa olevansa Listen-tilassa. Seuraavassa hello-viestissä maricper01 ilmoittaa olevansa active-tilassa ja näin ollen roolit ovat vaihtuneet.

1202 393.208848	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1203 393.212328	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1204 393.891101	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
1205 393.891632	192.168.100.2	224.0.0.2	HSRP	Coup (state Listen)
1206 393.891638	192.168.100.2	224.0.0.2	HSRP	Hello (state Active)
1210 393.894626	192.168.100.3	224.0.0.2	HSRP	Advertise (state Passive)
1211 393.895766	192.168.100.3	224.0.0.2	HSRP	Hello (state Speak)
1213 394.208859	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1218 396.879839	192.168.100.2	224.0.0.2	HSRP	Hello (state Active)
1221 396.894567	192.168.100.3	224.0.0.2	HSRP	Hello (state Speak)
1223 399.662051	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1224 399.662908	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1225 399.736404	192.168.100.2	224.0.0.2	HSRP	Hello (state Active)
1228 399.894611	192.168.100.3	224.0.0.2	HSRP	Hello (state Speak)
1230 400.662063	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1231 400.662926	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1232 401.336749	192.168.100.2	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x1e52
1233 401.662071	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1234 401.662931	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1236 402.662079	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1237 402.662953	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1238 402.663875	192.168.100.2	224.0.0.2	HSRP	Hello (state Active)
1239 402.894700	192.168.100.3	224.0.0.2	HSRP	Hello (state Speak)
1240 403.662101	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1241 403.662969	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1242 403.891384	192.168.100.3	224.0.0.2	HSRP	Hello (state Standby)
1244 404.662136	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
1245 404.662985	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
1248 405.656480	192.168.100.2	224.0.0.2	HSRP	Hello (state Active)

KUVIO 14. Maricper01 käynnistyy.

BGP:n osalta reititys kääntyy kulkemaan pääyhteyden kautta, kun pääliittymän ja edgen välinen naapuruus nousee ylös ja reititystaulut päivittyvät tilanteen mukaisiksi.

JUNIPER

Kun Juniperista sammutettiin virrat, huomattiin ainoastaan yhden tai kahden ping-paketin häviävän. Sama voitiin havaita tutkittaessa Wiresharkin tulosteita, joista katkosajaksi saatiin noin 5,5 sekuntia. Ote Wiresharkin tulosteesta kuviossa 15. Tulosteesta voidaan havaita, että maricper02 muuttuu master-reitittimeksi noin 3,5 sekunnin kuluttua viimeisestä maricper01:n lähettämästä mainostusviestistä. Näissä testeissä ei muokattu VRRP:n oletuslaskureita, joten niiden arvot olivat yksi ja kolme sekuntia. Eli master-reititin lähettää mainostuksia sekunnin välein ja mikäli uutta mainostusta ei vastaanoteta kolmen sekunnin sisällä, ottaa backup-reititin liikenteenvälityksen hoitaakseen.

189 49.370519	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
190 49.635082	192.168.100.2	224.0.0.18	VRRP	Announcement (v2)
192 50.369252	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
193 50.370534	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
194 51.369275	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
195 51.370723	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
197 52.369299	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
200 53.226608	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
204 54.225675	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
207 55.225694	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
209 56.225812	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
210 57.225789	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
211 57.838104	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
212 57.844975	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
215 58.225820	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
216 58.838120	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
217 58.843486	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply
218 59.225811	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
219 59.838140	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request

KUVIO 15. Maricper01:n sammutus virtakytkimestä.

Alla olevasta tulosteesta voidaan havaita reitittimen rooli, ajastin-laskureiden arvot, priority-arvot sekä virtuaaliset osoitteet.

```
maricper02#sh vrrp
Vlan1 -Group 1
  State is Master
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
    Track object 1 state Up decrement 10
  Master Router is 192.168.100.3 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec
```

Koska tulos poikkesi melko paljon vastaavasta testistä Ciscon reitittimellä, tehtiin tämä testi neljä kertaa. Neljännellä kerralla debugattiin liikennettä sekä maried-ger01:llä että maricper02:lla. Debug-tulosteesta voitiin havaita, että Juniperin reititin lähettää BGP-naapureilleen ilmoituksen sammumisestaan. Eli virtakatkaisimesta sammuttaminen vei yhteyden alas hallitusti. Testi tehtiin vielä kerran siten, että irrotettiin Juniperin virtajohto, jolloin tilanne saatiin simuloitua todenmukaisempana esim. sähkökatkoksen tai äkillisen laitteen vikaantumisen osalta. Tällöin ping-paketteja katosi seitsemän kappaletta ja tulosteesta saatiin katkosajaksi laskettua noin 33 sekuntia, joka aiheutuu BGP:n timereista.

Maricper01:n käynnistyessä huomattiin yhden ping-paketin katoavan ja liikenteen kääntymisen aiheuttavan 5,5 sekunnin katkoksen.

4.2.3 Maricper01:n wan-linkki irti

Tässä testissä irrotettiin wan-linkin piuha maricper01:stä, jolloin simuloitiin fyysistä vikaa, kuten kuidun tai kaapelin katkeamista. Wan-linkin katkeamisen seurauksena verkon reitityksen pitäisi muuttua. Kun linkki katkaistaan, pitäisi tapahtua seuraavaa:

- Maricper01 poistaa edgen kautta opitut reitit BGP-taulustaan. Samalla se lähettää iBGP-naapurilleen ilmoituksen, ettei enää tunne reittiä em. verkkoihin, jolloin maricper02 poistaa maricper01:n kautta oppimansa reitit ja asentaa reititystauluun mariedger02:n kautta tulevat reitit.

- Mariedger01 on saanut keepalive-viestin maricper01:ltä ennen linkin katkeamista, se on asettanut hold time-laskurin arvoksi 0. Laskurin arvo kasvaa, kunnes se saavuttaa hold time:ksi asetetun arvon, joka on tässä tapauksessa 30. Koska mariedger01 ei saa uutta keepalive viestiä maricper01:ltä hold time:n aikana, se toteaa naapurin ”kuolleeksi” ja sulkee peering-session, samalla se poistaa maricper01:ltä oppimansa reitit BGP-taulusta ja asentaa BGP-taulusta mariedger02:n kautta mainostuvat verkot reititystauluunsa.

Tässäkin tapauksessa katkoksen keston pitäisi olla 20 - 40 sekunnin välillä. Tämän jälkeen liikenne testi-PC:ltä mariedger01:n loopback0:n osoitteeseen pitäisi toimia.

Myös redundantti-protokollien pitäisi vaihtaa tilaansa, koska molemmissa on konfiguroituna nimenomaan wan-liitynnän seuranta.

Verkon konvergoituminen BGP:n osalta tapahtui tässä testissä samalla tavalla sekä Ciscon että Juniperin reitittimellä.

CISCO

HSRP on konfiguroitu niin, että se seuraa wan-interfacen tilaa ja mikäli interface menee jostain syystä alas, vähentää HSRP priority-arvoaan 10 ja lähettää sen Hello-viestissä. Kun maricper02 saa Hello-viestin, jossa priority-arvo on pienempi, kuin sillä itsellään, se lähettää Coup-viestin ja muuttaa tilansa aktiiviseksi, jonka seurauksena maricper01:stä tulee standby-reititin. Tämä muutos tapahtuu hyvin nopeasti, suuremman katkoksen liikenteeseen aiheuttaa BGP:n reittien kääntyminen. Alla tulosteet HSRP:n tilasta:

maricper01#sh stand

```
Vlan1 -Group 1
  Local state is Standby, priority 110 (confgd 120), may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.186
  Virtual IP address is 192.168.100.1 configured
  Active router is 192.168.100.3, priority 115 expires in 7.764
  Standby router is local
  Authentication text "mari"
  6 state changes, last state change 00:01:22
  IP redundancy name is "hsrp-Vl1-1" (default)
  Priority tracking 1 interface or object, 0 up:
    Interface or object        Decrement  State
    GigabitEthernet0/12            10      Down  (line protocol down)


 maricper02#sh stand
Vlan1 -Group 1
  State is Active
    53 state changes, last state change 00:00:09
  Virtual IP address is 192.168.100.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.616 secs
  Authentication text "mari"
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 115 (configured 115)
    Track interface GigabitEthernet0/12 state Up decrement 10
  IP redundancy name is "hsrp-Vl1-1" (default)
```

Kuten tulosteesta voidaan havaita, on pääliittymän priority-arvo laskenut 110, vaikka arvoksi on konfiguroitu 120 ja maricper02-reititin on muuttunut aktiiviseksi.

Ciscon reitittimellä katkosajaksi tuli tässä testissä keskimäärin 31 sekunnin katkosaika, mikä johtuu BGP:n ajastimien arvosta.

JUNIPER

Tässä testissä ping-paketteja katosi keskimäärin kuusi kappaletta. Wiresharkin-tulosteesta lasketuksi keskimääräiseksi katkosajaksi saatiin 28,8 sekuntia. Myös VRRP muutti tilaansa tässä testissä, koska VRRP oli konfiguroitu siten, että se reagoi wan-interfacen muutokseen. Alla olevassa tulosteessa näkyy VRRP:n tila sekä maricper01:llä että maricper02:lla:

```
root@maricper01> show vrrp detail
Physical interface: fe-0/0/5, Unit: 0, Address: 192.168.100.2/24
  Index: 69, SNMP ifIndex: 123, VRRP-Traps: disabled
  Interface state: up, Group: 1, State: backup, VRRP Mode: Active
  Priority: 100, Advertisement interval: 1, Authentication type: none
  Delay threshold: 100, Computed send rate: 0
  Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 192.168.100.1
  Dead timer: 3.250s, Master priority: 105, Master router: 192.168.100.3
  Virtual router uptime: 00:06:46
  Tracking: enabled
    Current priority: 100, Configured priority: 110
    Priority hold time: disabled
    Interface tracking: enabled, Interface count: 1
      Interface     Int state   Int speed   Incurred priority cost
      ge-0/0/0.0    down              0                   10
    Route tracking: disabled
```

```
maricper02#sh vrrp
Vlan1 -Group 1
  State is Master
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
    Track object 1 state Up decrement 10
  Master Router is 192.168.100.3 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec
```

Tulosteesta nähdään, että VRRP:n mainostusväli on sekunnin ja aika, jonka jälkeen master-reititin julistetaan “kuolleeksi”, on 3,59 sekuntia. Nämä ovat VRRP:n oletusarvot, joiden muuttamista ei nähty tarpeelliseksi, koska suurimman viiveen liikenteen kääntymiselle aiheuttaa BGP:n ajastimet.

Kun wan-linkki kytkettiin takaisin, katosi yksi ping-paketti liikenteen kääntyessä maricper01:lle, tällöin katkosaika oli keskimäärin 5,5 sekuntia.

4.2.4 Maricper01:n lan-linkki poikki

Seuraavassa testissä irrotettiin maricper01:ltä lan-portin kytkentä, tämä testi simuloi lan:ssa olevan kaapelin/kuidun katkeamista tai kytkimen hajoamista. Yhteyden katketessa pitäisi tapahtua seuraavaa:

- Kun maricper01 huomaa, että sen lan-interface menee alas, se poistaa kyseessä olevan verkon BGP-taulustaan ja lähettää update-ilmoituksen kadonneesta reitistä mariedger01:lle. Mariedger01 asentaa reititystauluunsa BGP-taulusta löytyvän vaihtoehtoisen reitin ko. verkkoon. Tähän menee aikaa muutama sekunti linkin tilan muutoksesta.

- Maricper02 odottaa 30 sekuntia keepalive-ilmoituksia maricper01:ltä, kun 30 sekuntia edellisestä keepalive-viestistä on kulunut, se sulkee peering-session maricper01:lle ja poistaa sitä kautta oppimansa reitit BGP-taulusta. Tämän jälkeen maricper02 asentaa reititystauluun mariedger02:n kautta oppimansa reitit ja liikenne palautuu.

HSRP:n ja VRRP:n tiloissa pitäisi myös tapahtua muutoksia.

Tässäkin mittauksessa katkosajan pitäisi olla riippuvainen ainoastaan BGP:n timereista ja näin ollen asettua 20 - 40 sekunnin välille.

CISCO

Ciscon reitittimillä mitattu liikenteen katkos oli noin 33 sekuntia, joka johtuu jälleen BGP:n timereista.

Alla tuloste HSRP:n tilasta maricper01:ltä:

```
maricper01#sh stand
Vlan1 -Group 1
  Local state is Init (interface down), priority 120, may preempt
  Hellotime 3 sec, holdtime 10 sec
  Virtual IP address is 192.168.100.1 configured
  Active router is unknown
  Standby router is unknown
  Authentication text "mari"
  14 state changes, last state change 00:01:33
  IP redundancy name is "hsrp-Vl1-1" (default)
  Priority tracking 1 interface or object, 1 up:
    Interface or object       Decrement  State
    GigabitEthernet0/12           10     Up
```

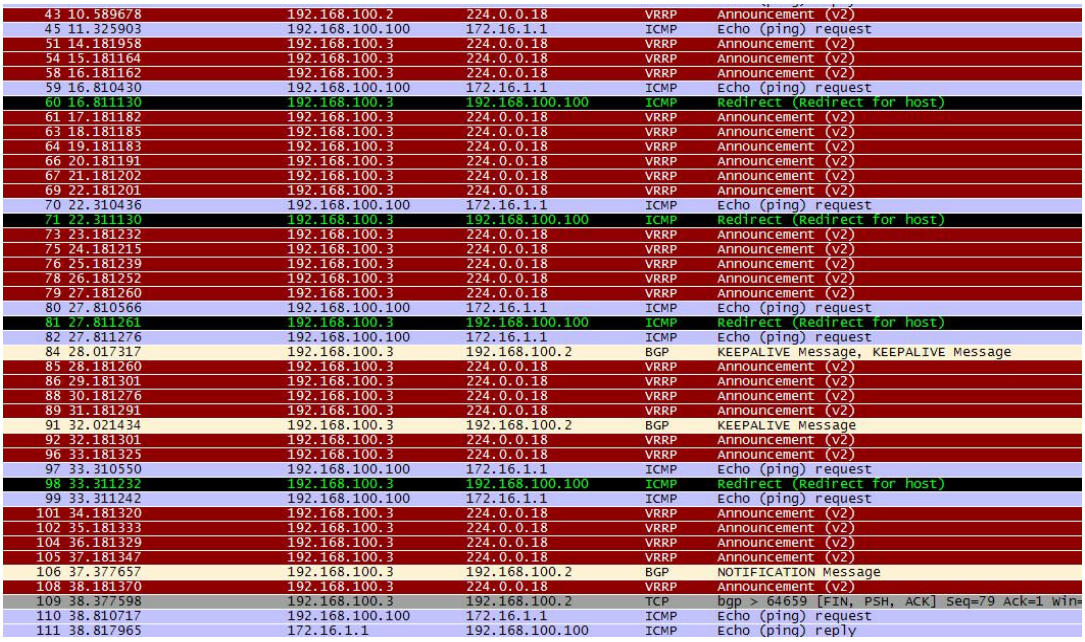
HSRP on muuttanut tilansa Init:iin, koska liityntä, johon HSRP on konfiguroitu, on alhaalla. Ja koska maricper01:llä ei ole yhteyttä lan:n kautta maricper02:lle, se ei myöskään tiedä sillä hetkellä aktiivisena olevaa reititintä (Active router is unknown). HSRP ehtii kääntää liikenteen varareitittimelle hieman yli sekunnissa, mutta BGP:n mainostusten kääntyminen kestää noin puoli minuuttia.

Kun lan-kaapeli kytkettiin takaisin maricper01:een, liikenne palautui nopeasti ja vain yksi ping-paketti katosi kääntymisen aikana, liikenteeseen aiheutui näin ollen noin 5,5 sekunnin katkos.

JUNIPER

Sama testi suoritettiin myös Juniperin reitittimellä ja tässäkin testissä Juniper käyttäytyi BGP:n osalta samalla tavalla kuin Ciscon reititin. Katkosajaksi saatiin keskimäärin 29 sekuntia. Kuvion 16 Wiresharkin tulosteesta nähdään, kuinka

maricper02:sta on tullut master-reititin VRRP:n kannalta, mutta liikenne ei vielä siinä vaiheessa toimi, koska maricper02 ei ole vielä päivittänyt BGP- ja reititystauluaan:



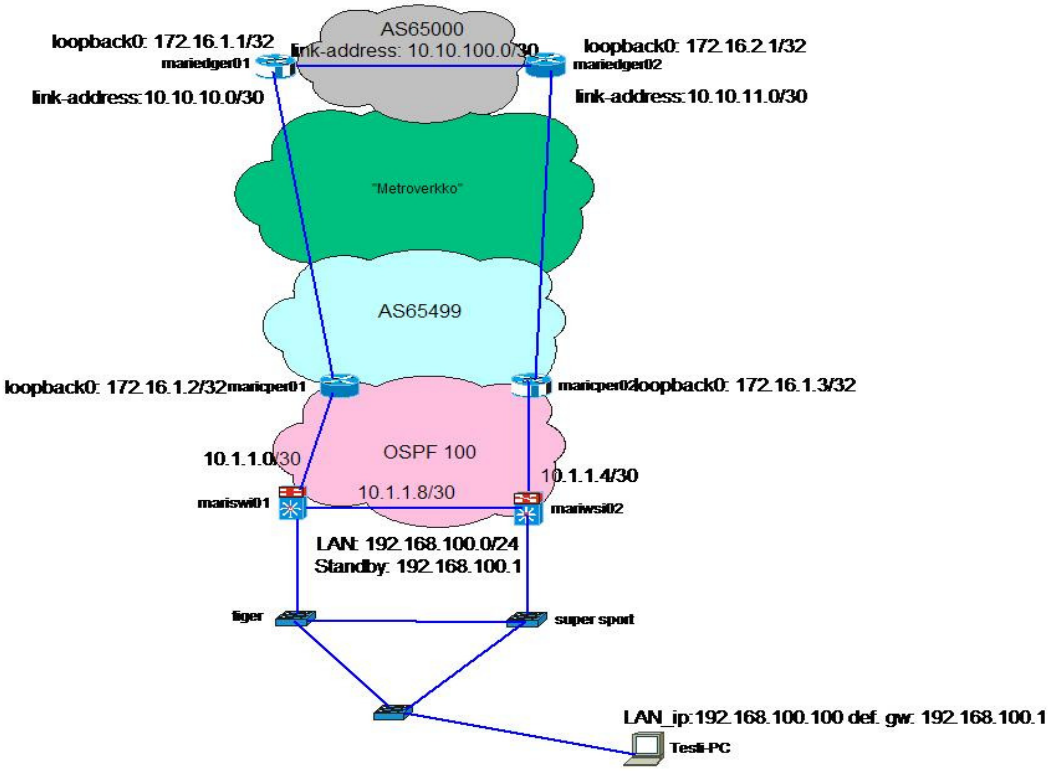
43 10.589678	192.168.100.2	224.0.0.18	VRRP	Announcement (v2)
45 11.325903	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
51 14.181958	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
54 15.181164	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
58 16.181162	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
59 16.810430	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
60 16.811130	192.168.100.3	192.168.100.100	ICMP	Redirect (Redirect for host)
61 17.181182	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
63 18.181185	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
64 19.181183	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
66 20.181191	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
67 21.181202	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
69 22.181201	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
70 22.310436	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
71 22.311130	192.168.100.3	192.168.100.100	ICMP	Redirect (Redirect for host)
73 23.181232	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
75 24.181215	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
76 25.181239	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
78 26.181252	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
79 27.181260	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
80 27.810566	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
81 27.811261	192.168.100.3	192.168.100.100	ICMP	Redirect (Redirect for host)
82 27.811276	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
84 28.017317	192.168.100.3	192.168.100.2	BGP	KEEPALIVE Message, KEEPALIVE Message
85 28.181260	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
86 29.181301	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
88 30.181276	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
89 31.181291	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
91 32.021434	192.168.100.3	192.168.100.2	BGP	KEEPALIVE Message
92 32.181301	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
96 33.181325	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
97 33.310550	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
98 33.311232	192.168.100.3	192.168.100.100	ICMP	Redirect (Redirect for host)
99 33.311242	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
101 34.181320	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
102 35.181333	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
104 36.181329	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
105 37.181347	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
106 37.377657	192.168.100.3	192.168.100.2	BGP	NOTIFICATION Message
108 38.181370	192.168.100.3	224.0.0.18	VRRP	Announcement (v2)
109 38.377598	192.168.100.3	192.168.100.2	TCP	bgp > 64659 [FIN, PSH, ACK] Seq=79 Ack=1 Win=
110 38.810717	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
111 38.817965	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply

KUVIO 16. Maricper01:n lan-linkki poikki.

Liikenteen palautuessa pääliittymälle tässäkin testissä katosi yksi ping-paketti ja katkosajaksi saatiin 5,5 sekuntia.

4.3 BGP ja OSPF

Seuraavaksi tutkittiin, kuinka saadaan toteutettua redundantti verkko käyttäen BGP:tä EGP-protokollana ja OSPF:ää IGP-protokollana. Lähiverkon varmistus vietiin reitittäville kytkimille, jolloin redundantti-protokollana oli HSRP. Reitittiminä käytettiin Juniperia (pääliittymä) ja Ciscoa (varaliittymä). Verkon topologiaa jouduttiin muuttamaan ja se on esitetty kuviossa 17. Maricper01:n konfiguraatio on esitetty liitteessä 7 ja maricper02:n konfiguraatio liitteessä 8. Mariswi01:n ja -02:n konfiguraatiot ovat liitteissä 9 ja 10.



KUVIO 17. BGP- ja OSPF-verkon topologia.

Lisäksi jouduttiin miettimään, kuinka saadaan estettyä reitityssilmukoiden muodostuminen, kun reittejä redistribuutataan (edelleen mainostetaan) reititysprotokollien välillä. Suodattaminen päätettiin tehdä route-map:n avulla siten, että OSPF-prosessiin redistribuutatuille BGP:n verkoille asetetaan tag (merkkaus) 555, kun OSPF-verkot redistribuutataan BGP-prosessiin, tarkistetaan reittien tag:t ja jos niistä löytyy 555, reitit hylätään. Alla olevasta tulosteesta voidaan havaita, että normaalitilanteessa verkko 192.168.100.0/24 mainostuu maricper01:n kautta:

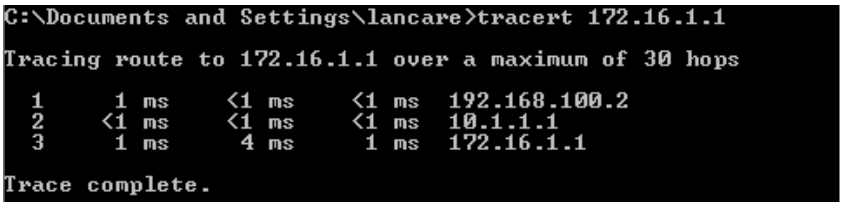
```
mariedger01#sh ip rou
Codes: C -connected, S -static, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
       E1 -OSPF external type 1, E2 -OSPF external type 2, E -EGP
       i -IS-IS, su -IS-IS summary, L1 -IS-IS level-1, L2 -IS-IS level-2
       ia -IS-IS inter area, * -candidate default, U -per-user static route
       o -ODR, P -periodic downloaded static route

Gateway of last resort is 88.194.144.1 to network 0.0.0.0
```

```
     172.16.0.0/32 is subnetted, 3 subnets
C       172.16.1.1 is directly connected, Loopback0
B       172.16.2.1 [200/0] via 10.10.100.2, 00:21:52
B       172.16.1.2 [20/0] via 10.10.10.1, 00:21:52
S    192.89.200.0/24 [1/0] via 88.194.144.1
     10.0.0.0/30 is subnetted, 6 subnets
B       10.1.1.8 [20/101] via 10.10.10.1, 00:21:52
C       10.10.10.0 is directly connected, FastEthernet1/0/1
B       10.1.1.0 [20/0] via 10.10.10.1, 00:21:52
B       10.10.11.0 [200/0] via 10.10.100.2, 00:21:52
B       10.1.1.4 [20/1002] via 10.10.10.1, 00:21:52
C       10.10.100.0 is directly connected, FastEthernet1/0/24
     88.0.0.0/20 is subnetted, 1 subnets
C       88.194.144.0 is directly connected, FastEthernet1/0/23
B    192.168.100.0/24 [20/2] via 10.10.10.1, 00:21:52
S*   0.0.0.0/0 [254/0] via 88.194.144.1
```

Alla maricper02:n reititystaulu, josta voidaan havaita, että mariedger01:n loopback0:n osoite (172.16.1.1/32), mainostuu maricper01:n kautta:

```
maricper02#sh ip rou
Codes: C -connected, S -static, R -RIP, M -mobile, B -BGP
       D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
       N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
       E1 -OSPF external type 1, E2 -OSPF external type 2
       i -IS-IS, su -IS-IS summary, L1 -IS-IS level-1, L2 -IS-IS level-2
       ia -IS-IS inter area, * -candidate default, U -per-user static route
       o -ODR, P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/32 is subnetted, 2 subnets
O E1    172.16.1.1 [110/1101] via 10.1.1.6, 00:21:20, Vlan1
B       172.16.2.1 [20/0] via 10.10.11.2, 00:32:09
O E1 192.89.200.0/24 [110/1101] via 10.1.1.6, 00:21:20, Vlan1
     10.0.0.0/30 is subnetted, 6 subnets
O       10.1.1.8 [110/1101] via 10.1.1.6, 00:25:24, Vlan1
B       10.10.10.0 [20/0] via 10.10.11.2, 00:21:19
O       10.1.1.0 [110/1101] via 10.1.1.6, 00:25:24, Vlan1
C       10.10.11.0 is directly connected, FastEthernet0
C       10.1.1.4 is directly connected, Vlan1
B       10.10.100.0 [20/0] via 10.10.11.2, 00:32:09
     88.0.0.0/20 is subnetted, 1 subnets
O E1    88.194.144.0 [110/1101] via 10.1.1.6, 00:21:20, Vlan1
O    192.168.100.0/24 [110/1001] via 10.1.1.6, 00:25:24, Vlan1
```

Kuviossa 18 on traceroute:n tuloste testi-PC:ltä, josta voidaan havaita, että liikenne kulkee maricper01:n kautta:



KUVIO 18. Traceroute testi-PC:ltä normaalitilanteessa.

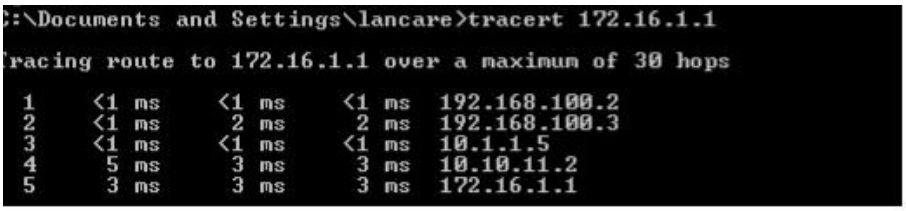
4.3.1 BGP-naapuruus edgeltä alas

Ensimmäisenä testinä oli tarkoitus sulkea BGP-naapuruus mariedger01:ltä. Tässä tapauksessa katkosajan pitäisi olla hieman pidempi, kuin kuvion 11 topologialla tehty vastaava testi, koska on otettava huomioon OSPF:n konvergoituminen. Verkossa tapahtuu seuraava, kun naapuruus suljetaan:

- Mariedger01 lähettää kyseiselle naapurille notification-viestin, jossa se ilmoittaa peering-session sulkemisesta. Maricper01 poistaa BGP-taulustaan edgeltä oppimansa verkot, jolloin niitä ei myöskään redistribuutata (edelleen mainosteta) OSPF-prosessiin.

- Maricper02 poistaa BGP-taulustaan verkot, mitkä se on oppinut maricper01:n kautta ja asentaa reititystauluunsa BGP-taulusta mariedger02:n kautta opitut verkot.

Kun BGP-naapuruus suljettiin, havaittiin kahden ping-paketin katoaminen. Wiresharkin tulosteista voitiin havaita, että katkosajaksi tuli keskimäärin 5,7 sekuntia, joka on aavistuksen enemmän, kuin kuviossa 11 esitetyllä topologialla. Alla tracerouten tuloste kohti mariedger01:n loopback0:n osoitetta testi-PC:ltä:



KUVIO 19. Traceroute testi-PC:ltä, kun BGP-naapuruus on suljettu.

Kuvion 19 tulosteesta voidaan havaita, että paketti kulkee ensin mariswi01:lle, josta se siirtyy mariwsi02:lle, seuraava hyppy on maricper02, josta seuraava hyppy on mariedger02 ja viimeinen hyppy on mariedger01:n loopback0.

Kun naapuruus nostetaan edgeltä ylös, palautuu liikenne nopeasti ja yhtään ping-pakettia ei katoa. Voidaan vain havaita yhden paketin osalta normaali pidempi viive.

4.3.2 Maricper01 virrattomaksi

Tässä testissä irrotettiin virtajohto maricper01:stä ja seurattiin liikenteen kääntymistä. Testin määräävin tekijä katkosajan määräytymisessä pitäisi olla BGP:n käyttäytyminen ja näin ollen odotettavissa olevan tuloksen pitäisi olla 20 - 40 sekunnin välillä. OSPF:n ja HSRP:n pitäisi konvergoitua nopeammin, kuin BGP:n.

Kun virtapiuha irrotettiin, meni noin kolme sekuntia, kun mariswi01 huomasi muutoksen ja päivitti linkkitila-tietokantansa ja reititystaulunsa. Tämän jälkeen maricper02:n reititystaulu päivittyi ja liikenne lähiverkon suunnasta siirtyi kulkemaan sen kautta. Mariedger01 sen sijaan odotti 30 sekuntia edellisen keepalive-viestin vastaanottamisesta, ennen kuin se sulki peering-session marcper01:lle ja päivitti BGP- ja reititystaulunsa, vasta tämän jälkeen liikenne testi-PC:ltä mariedger01:n loopback0:n palautui. Liikenteelle aiheutunut katkos oli tässä testissä keskimäärin 28 sekuntia ja se aiheutuu nimenomaan BGP:n ajastimista.

Kuvion 20 tulosteesta nähdään HSRP:n tilojen muuttuminen kytkimillä mariswi01 ja -02, sekä OSPF:n prosessin lähettämät linkkitila-tietokannan päivitys- ja hello-viestit.

339 96.030547	192.168.100.3	224.0.0.2	HSRP	Advertise (state Active)
340 96.030552	192.168.100.3	224.0.0.2	HSRP	Coup (state Standby)
341 96.031066	192.168.100.3	224.0.0.2	HSRP	Advertise (state Active)
342 96.031072	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
344 96.031862	192.168.100.2	224.0.0.2	HSRP	Hello (state Speak)
346 97.125387	192.168.100.2	224.0.0.5	OSPF	Hello Packet
347 97.141430	192.168.100.2	224.0.0.5	OSPF	LS Update
349 98.933410	192.168.100.2	224.0.0.2	HSRP	Hello (state Speak)
350 99.030660	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
355 99.638706	192.168.100.3	224.0.0.5	OSPF	LS Acknowledge
357 100.832949	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
358 101.913431	192.168.100.2	224.0.0.2	HSRP	Hello (state Speak)
360 102.030654	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
363 102.145741	192.168.100.3	224.0.0.5	OSPF	LS Update
364 103.638705	192.168.100.3	224.0.0.5	OSPF	Hello Packet
366 104.645470	192.168.100.2	224.0.0.5	OSPF	LS Acknowledge
367 104.850026	192.168.100.2	224.0.0.2	HSRP	Hello (state Speak)
368 105.030716	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
370 106.030054	192.168.100.2	224.0.0.2	HSRP	Hello (state Standby)
371 106.333020	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
372 107.125464	192.168.100.2	224.0.0.5	OSPF	Hello Packet
374 108.030774	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
375 108.953503	192.168.100.2	224.0.0.2	HSRP	Hello (state Standby)
378 111.030790	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
379 111.833088	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
380 111.941516	192.168.100.2	224.0.0.2	HSRP	Hello (state Standby)
382 113.638839	192.168.100.3	224.0.0.5	OSPF	Hello Packet
384 114.030816	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
385 114.897559	192.168.100.2	224.0.0.2	HSRP	Hello (state Standby)
387 117.030864	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
388 117.125554	192.168.100.2	224.0.0.5	OSPF	Hello Packet
389 117.333173	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
390 117.861591	192.168.100.2	224.0.0.2	HSRP	Hello (state Standby)
394 120.030897	192.168.100.3	224.0.0.2	HSRP	Hello (state Active)
395 120.741613	192.168.100.2	224.0.0.2	HSRP	Hello (state Standby)
397 122.833225	192.168.100.100	172.16.1.1	ICMP	Echo (ping) request
398 122.838364	172.16.1.1	192.168.100.100	ICMP	Echo (ping) reply

KUVIO 20. Maricper01 virtapiuha irti.

Kuvion 21 tracerouten tulosteesta voidaan havaita, että ensimmäinen hyppy on mariswi02, josta liikenne siirtyy maricper02:lle ja sieltä mariedger02:n kautta kohteeseen.

```
C:\Documents and Settings\lancare>tracert 172.16.1.1

Tracing route to 172.16.1.1 over a maximum of 30 hops

  1    <1 ms     2 ms     2 ms  192.168.100.3
  2    <1 ms    <1 ms    <1 ms  10.1.1.5
  3     3 ms     3 ms     3 ms  10.10.11.2
  4     5 ms     7 ms     3 ms  172.16.1.1

Trace complete.
```

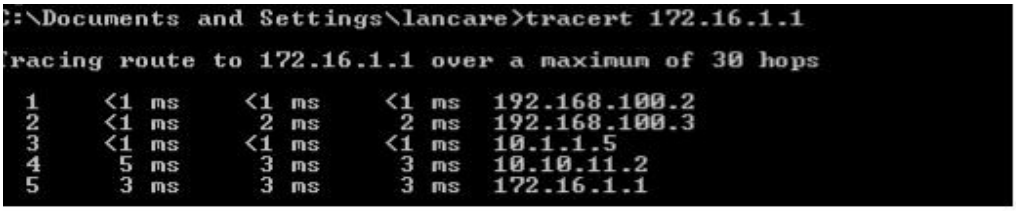
KUVIO 21. Traceroute testi-PC:ltä, kun maricper01 on virrattomana.

Liikenteen kääntyessä takaisin pääliittymälle yhtään ping-pakettia ei kadonnut.

4.3.3 Wan-linkki poikki

Tässä testissä irrotettiin pääliittymän wan-linkki, jolloin saadaan simuloitua kuidun/kaapelin katkeaminen tai operaattorin kytkentäpaikan vikaantuminen. Verkon konvergoitumisen pitäisi tapahtua samalla mekanismilla, kuin edellisessä testissä, joten odotettavissa oleva katkosaika olisi myös välillä 20 - 40 sekuntia.

Tässä testissä keskimääräiseksi katkosajaksi tulosteiden perusteella saatiin 29,1 sekuntia. Kuviossa 22 on traceroute-tuloste testi-PC:ltä, josta nähdään, että paketti kulkee reittiä mariswi01 –> mariwsi02 –> maricper02 –> mariedger02 –> mariedger01. Kytkimet eivät HSRP:n osalta muuta tilaansa ja siksi liikenne kulkee mariswi01:n kautta.



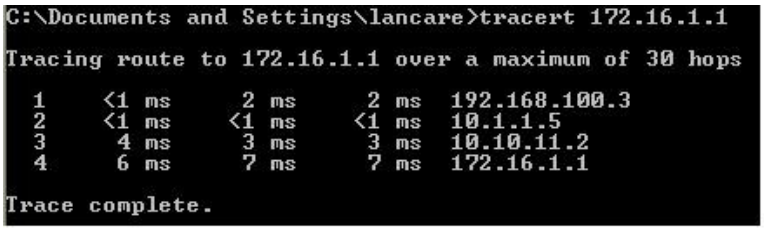
KUVIO 22. Traceroute testi-PC:ltä, kun wan-linkki on poikki.

Kun wan-linkki nousee ylös ja normaalitilanne saavutettiin, ei liikenteessä havaittu katkosta.

4.3.4 Lan-kaapeli irti

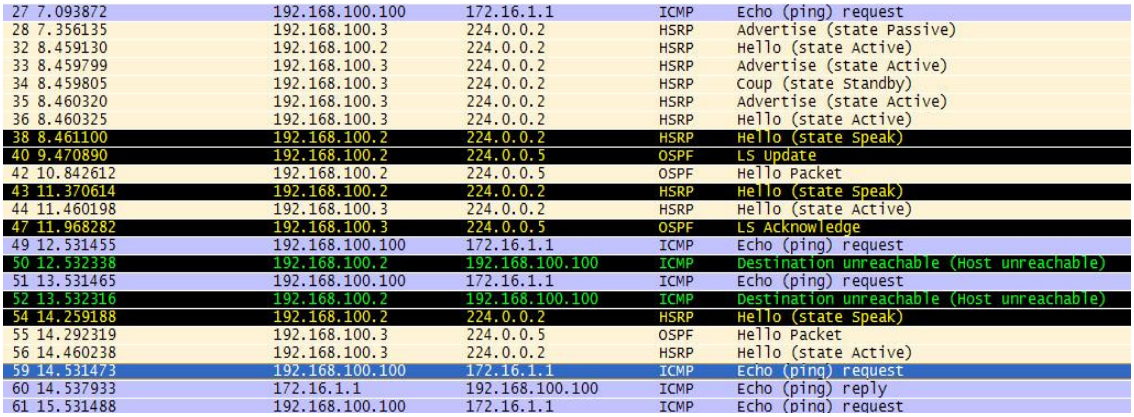
Tässä testissä irrotettiin lan-kaapeli maricper01:n lan-portista, sillä simuloitiin lan-kuidun/kaapelin katkeamista tai lan:ssa olevan kytkimen hajoamista. Verkon konvergoitumisajaksi pitäisi saada huomattavasti lyhyempi aika, kuin kahdessa edeltävässä testissä, koska BGP:n naapuruuksissa ei tapahdu muutoksia, ainoastaan BGP- ja reititystaulut muuttuvat. OSPF pitäisi konvergoitua verkossa tapahtuvasta muutoksesta nopeasti.

Kolmen mittauksen keskimääräinen katkosaika oli 7,7 sekuntia. Kun maricper01 huomaa interfacen menevän alas, se poistaa kyseisen verkon mainostuksen ja lähettää BGP update-viestin mariedger01:lle, joka päivittää reittitietonsa heti. HSRP muuttaa kytkimillä mariswi01 ja -02 tilaansa, samoin OSPF huomaa maricper01-mariswi01:n välisen linkin menevän alas, jolloin reititys kääntyy kulkemaan maricper02:n kautta, kuten kuviosta 23 voidaan havaita.



KUVIO 23. Traceroute testi-PC:ltä, kun maricper01:n lan-linkki on poikki.

Kuvion 24 tulosteessa näkyy HSRP:n tilan muuttuminen ja OSPF:n vaihtamat viestit liikenteen kääntyessä.



KUVIO 24. Maricper01:n lan-linkki alhaalla.

Kun linkki palautettiin ja liikenne kääntyi takaisin maricper01:lle, liikenteessä ei havaittu lainkaan katkosta.

5 YHTEENVETO

Testauksissa huomattiin, että tutkituilla kombinaatioilla merkittävin tekijä viiveessä, joka liikenteen kääntyessä ilmenee, on BGP:n ajastimien aiheuttama viive. Redundantti-protokollien oletusajastimet toimivat näissä tapauksissa hyvin eikä tarvetta niiden muuttamiselle nähty. BGP:n ajastimia pienentämällä voitaisiin saada nopeammin konvergoituva verkko, mutta se voisi tehdä verkosta epästabiilimman. Mikäli BGP:n ajastimet konfiguroidaan liian pieniksi, voi jokin räpsyvä reitti aiheuttaa jatkuvaa reititystaulun päivitystä ja suuremmissa verkoissa se vaikuttaa reitittimien suorituskykyyn ja verkon läpäisykykyyn. Sovellustasolla verkon katkoksien aiheuttamaa häiriötä ei pystytty mittauksissa todentamaan, koska testiympäristöön ei rakennettu palveluita, joten seuraavassa esitetyt vaikutukset sovelluksiin perustuvat lähinnä teoriatietoon ja kokemukseen. Työssä oli tarkoitus perehtyä lähinnä yritysliittymissä käytettäviin ratkaisuihin, joten sovelluksien tarkastelu on tehty siltä kannalta. Liikenteen katkeamisesta kääntymisen aikana eniten häiriintyvät reaaliaikaiset sovellukset, jotka toimivat pääsääntöisesti UDP:n ja RTP:n päällä, kuten esim. VoIP ja videoneuvottelu-sovellukset. Itse UDP ei reagoi verkkoyhteyden katkeamiseen, vaan reagointi jää sitä käyttävän sovellustason protokollan, kuten RTP:n, varaan. TCP-istunnot voivat katketa, riippuen TCP:n ajastimista, tällöin käyttäjän on avattava yhteys uudestaan. TCP:n ajastimet taas riippuvat monista tekijöistä, kuten verkon ruuhkaisuudesta ja käytettävissä olevasta kaistasta.

Laitteiden välillä ei huomattu toiminnassa eroja, vaan molempien tulokset vastaavat hyvin protokollien standardeja. Juniperin osalta huomattiin, että virtakytkimestä suoritettava katkaisu sammuttaa reitittimen hallitusti, jolloin myös BGP-prosessi ajetaan alas sammuvan reitittimen toimesta. Mikäli vastaavalla laitteella halutaan testata asiakasyhteyden varmennuksen toimivuutta, on syytä katkaista laitteen virta irrottamalla virtapiuha, jolloin tilanne vastaa paremmin oikeaa vikaa.

Ratkaisumalleista tietyissä tilanteissa nopeimmin konvergoituvaksi ratkaisuksi osoittautui verkko, jossa EGP-protokollana oli BGP ja IGP-protokollana OSPF. Etenkin lan-linkin katkeamisesta toipuminen tapahtui huomattavasti muita topologioita

nopeammin. Tähän vaikuttaa OSPF:n käyttäminen IGP-protokollana, koska se päivittää nopeasti linkkitilakantansa ja sitä kautta reittien edelleen mainostamisen BGP:hen.

LÄHTEET

Anttila, A. 2001. TCP/IP- tekniikka 2. uud. p. Helsinki: Helsinki Media 200.

BGP Best Path Selection Algorithm. 2006. Viitattu 25.4.2011. http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094431.shtml.

Cisco Hot Standby Router Protocol (HSRP). 1998. Viitattu 27.3.2011. http://www.faqs.org/rfcs/rfc2281.html.

Cisco Hot Standby Router Protocol RFC 2281. 1998. Viitattu 27.3.2011. http://tools.ietf.org/html/rfc2281.

Configuring BGP 2011a, n.d. Viitattu 25.4.2011. http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html#wp1001470.

Configuring BGP 2011b, n.d. Viitattu 25.4.2011. http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html#wp1002924.

Configuring BGP 2011c, n.d. Viitattu 23.4.2011. http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html#wp1040707.

Halabi, S. & McPherson D., 2001. Internet Routing Architectures, 2 p, Indianapolis, USA: Cisco Press.

How to Block One or More Networks From a BGP Peer. 2006. Viitattu 25.4.2011. http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00801310cb.shtml#acclists.

BGP Katsaus, 2010. Viitattu 6.4.2011. http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-interfaces-and-routing/section-bgp-overview.html#jd0e57856.

Kaario, K., 2002, TCP/IP-verkot. Porvoo: Docendo Finland Oy.

Luoma M. 2008 Verkkopalvelujen tuotanto. Viitattu 23.4.2011. http://www.netlab.tkk.fi/opetus/s383192/2006/kalvot/L6.pdf.

Niemi, P. 2008 Moniverkkoliityntä asiakkaan näkökulmasta. Viitattu 23.4.2011. www.netlab.tkk.fi/opetus/s383310/07-08/Niemi_25032008.ppt.

Stewart, B. & Gough, C. 2008 CCNP BSCI Official Exam Certification Guide, Indianapolis, USA: Cisco Press.

TeliaSonera Annual Report. 2010. Viitattu 3.12.2010.
http://www.teliasonera.com/2009/fi/YE/.

Tutoriaalit: Cisco IOS-pikaopas. 2009. Viitattu 27.3.2011.
http://sarajarvi.org/tutoriaalit-cisco-ios-pikaopas/#reititys.

Using HSRP for Fault-Tolerant IP Routing. 2009. Viitattu 3.4.2011.
http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Using_HSRP_for_Fault-Tolerant_IP_Routing#Understanding_How_HSRP_Works.

Virtual Router Redundancy Protocol RFC2338. 1998. Viitattu 5.5.2011.
http://datatracker.ietf.org/doc/rfc2338/?include_text=1.

White, R., McPherson, D. & Srihari, S., 2004, Practical BGP, Addison Wesley.

LIITTEET

Liite 1. Mariedger01:n konfiguraatio

```
mariedger01#sh run
Building configuration...

Current configuration : 2333 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mariedger01
!
logging buffered 65000 debugging
no logging console
enable password cisco
!
no aaa new-model
ip subnet-zero
ip routing
!
vtp mode transparent
!
no mpls traffic-eng auto-bw timers frequency 0
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy ascending
!
vlan 100
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
 no clns route-cache
!
interface FastEthernet1/0/1
 no switchport
 ip address 10.10.10.2 255.255.255.252
```

```
 no clns route-cache
!
interface FastEthernet1/0/2
 no switchport
 no ip address
 no clns route-cache
!
interface FastEthernet1/0/3
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
!
```

```
interface FastEthernet1/0/24
 no switchport
 ip address 10.10.100.1 255.255.255.252
 no clns route-cache
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/1/1
 switchport trunk allowed vlan 100
 switchport mode trunk
!
interface GigabitEthernet1/1/2
!
interface Vlan1
 no ip address
 no clns route-cache
!
interface Vlan100
 no ip address
 no clns route-cache
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute static
 neighbor 10.10.10.1 remote-as 65499
 neighbor 10.10.10.1 description maricper01
 neighbor 10.10.100.2 remote-as 65000
 neighbor 10.10.100.2 description mariedger02
 no auto-summary
!
ip classless
ip http server
!
!
control-plane
!
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 no login
end
```

Liite 2. Mariedger02:n konfiguraatio

```
mariedger02#sh run
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname mariedger02
!
enable password cisco
!
!
interface Loopback0
 ip address 172.16.2.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.10.11.2 255.255.255.252
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface Ethernet0/1
 ip address 10.10.100.2 255.255.255.252
!
interface Serial0/1
 no ip address
 shutdown
!
router bgp 65000
 no synchronization
 timers bgp 10 30
 redistribute connected
 redistribute static
 neighbor 10.10.11.1 remote-as 65499
 neighbor 10.10.11.1 description maricper02
 neighbor 10.10.100.1 remote-as 65000
 neighbor 10.10.100.1 description mariedger01
 no auto-summary
!
ip classless
```

```
logging buffered 65000 debugging
no logging console
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Liite 3. Maricper01:n konfiguraatio (c3550)

```
maricper01#sh run
Building configuration...

Current configuration : 2075 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maricper01
!
logging buffered 65000 debugging
no logging console
enable password cisco
!
ip subnet-zero
ip routing
!
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Loopback0
 ip address 172.16.1.2 255.255.255.255
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
```

```
interface GigabitEthernet0/3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/4
 switchport mode dynamic desirable
!
interface GigabitEthernet0/5
 switchport mode dynamic desirable
!
interface GigabitEthernet0/6
 switchport mode dynamic desirable
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
!
interface GigabitEthernet0/8
 switchport mode dynamic desirable
!
interface GigabitEthernet0/9
 switchport mode dynamic desirable
!
interface GigabitEthernet0/10
 switchport mode dynamic desirable
!
interface GigabitEthernet0/11
 switchport mode dynamic desirable
!
interface GigabitEthernet0/12
 no switchport
 ip address 10.10.10.1 255.255.255.252
!
interface Vlan1
 ip address 192.168.100.2 255.255.255.0
 no ip redirects
 standby 1 ip 192.168.100.1
 standby 1 priority 120
 standby 1 preempt
 standby 1 authentication mari
 standby 1 track GigabitEthernet0/12
!
router bgp 65499
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute static
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 description mariedger01
 neighbor 10.10.10.2 route-map LOCALPREFIN in
```

```
 neighbor 192.168.100.3 remote-as 65499
 neighbor 192.168.100.3 description maricper02
 no auto-summary
!
ip classless
ip http server
!
route-map LOCALPREFIN permit 10
 set local-preference 200
!!
line con 0
 password cisco
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Liite 4. Maricper02:n konfiguraatio (c3550)

```
maricper02#sh run
Building configuration...

Current configuration : 2163 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname maricper02
!
logging buffered 65000
no logging console
enable password cisco
!
no aaa new-model
!
ip subnet-zero
ip routing
!
vtp mode transparent
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Loopback0
 ip address 172.16.1.3 255.255.255.255
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface GigabitEthernet0/3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/4
 switchport mode dynamic desirable
!
interface GigabitEthernet0/5
 switchport mode dynamic desirable
!
interface GigabitEthernet0/6
 switchport mode dynamic desirable
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
!
interface GigabitEthernet0/8
 switchport mode dynamic desirable
!
interface GigabitEthernet0/9
 switchport mode dynamic desirable
!
interface GigabitEthernet0/10
 switchport mode dynamic desirable
!
interface GigabitEthernet0/11
 switchport mode dynamic desirable
!
interface GigabitEthernet0/12
 no switchport
 ip address 10.10.11.1 255.255.255.252
!
interface Vlan1
 ip address 192.168.100.3 255.255.255.0
 standby 1 ip 192.168.100.1
 standby 1 priority 115
```

```
 standby 1 preempt
 standby 1 authentication mari
 standby 1 track GigabitEthernet0/12
!
router bgp 65499
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute static
 neighbor 10.10.11.2 remote-as 65000
 neighbor 10.10.11.2 description mariedger01
 neighbor 10.10.11.2 route-map ASPREPEND out
 neighbor 192.168.100.2 remote-as 65499
 neighbor 192.168.100.2 description maricper01/primary
 no auto-summary
!
ip classless
ip http server
!
!
route-map ASPREPEND permit 10
 set as-path prepend 65499 65499 65499
!
!
control-plane
!
!
line con 0
 password cisco
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Liite 5. Maricper01:n konfiguraatio (Juniper

```
maricper01#
testi@maricper01# show
## Last changed: 2011-04-27 11:57:18 EEST
version 10.0R1.8;
system {
    host-name maricper01;
    time-zone Europe/Helsinki;
    internet-options {
        path-mtu-discovery;
        source-port {
            upper-limit 65535;
        }
        tcp-drop-synfin-set;
    }
    authentication-order password;
    root-authentication {
        encrypted-password "$1$15c1QEBD$2xchhYkROh2sX24/d8ddV0"; ## SECRET-
DATA
    }
    login {
        retry-options {
            tries-before-disconnect 3;
        }
        class admin {
            idle-timeout 10;
            login-alarms;
            permissions all;
        }
        class view-config {
            idle-timeout 10;
            permissions view;
        }
                encrypted-password "$1$Jqi3neaN$NwRLIwCBAYip12n9IkuID1"; ## SECRET-
DATA
            }
        }
        user remote-rw {
            uid 2004;
            class admin;
        }
        user testi {
            uid 2002;
            class admin;
            authentication {
                encrypted-password "$1$XCWyGxoh$76hRAcCTI0x5Ix2PJjFJX1"; ## SECRET-
DATA
```

```
        }
      }
    }
    services {
      telnet;
    }
    syslog {
      archive size 100k files 3;
      user * {
        any critical;
      }
      file messages {
        any any;
        authorization info;
      }
      file interactive-commands {
        any any;
        interactive-commands any;
      }
      file error-messages {
        any error;
        authorization error;
      }
      file auth-debug {
        authorization any;
        archive size 1m files 2;
      }
      time-format millisecond;
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 5;
    license {
      autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
      }
    }
}
chassis {
    config-button no-clear;
}
interfaces {
    ge-0/0/0 {
      unit 0 {
        family inet {
          address 10.10.10.1/30;
        }
      }
    }
     fe-0/0/5 {
```

```
        unit 0 {
            family inet {
                address 192.168.100.2/24 {
                    primary;
                    vrrp-group 1 {
                        virtual-address 192.168.100.1;
                        priority 110;
                        preempt;
                        accept-data;
                        track {
                            interface ge-0/0/0 {
                                priority-cost 10;
            }
        }
    }
    fe-0/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.2/32;
            }
        }
    }
}
routing-options {
    graceful-restart;
    autonomous-system 65499;
}
protocols {
    bgp {
        hold-time 30;
        group TO_EDGE {
            type external;
            description eBGP;
            neighbor 10.10.10.2 {
                import LOCALPREFIN;
                export PREFIXES_OUT;
                peer-as 65000;
            }
        }
        group LAN {
            type internal;
            description maricper02;
            neighbor 192.168.100.3 {
                export NEXTHOP_SELF;
                peer-as 65499;
            }
```

```
        }
    }
}
policy-options {
    policy-statement LOCALPREFIN {
        term LOCALPREF_PRIMARY {
            from {
                route-filter 0.0.0.0/0 upto /32;
            }
            then {
                local-preference 200;
                accept;
            }
        }
        term DEFAULT_ACTION {
            then reject;
        }
    }
    policy-statement NEXTHOP_SELF {
        term ONE {
            then {
                next-hop self;
                accept;
            }
        }
    }
    policy-statement PREFIXES_OUT {
        term PRIMARY_OUT {
            from protocol [ direct local static bgp ];
            then accept;
        }
        term DEFAULT_ACTION {
            then reject;
        }
    }
}
security {
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                all;
```

```
        }
      }
   }
   policies {
      default-policy {
         permit-all;
      }
   }
}

[edit]
testi@maricper01#
```

Liite 6. Maricper02:n konfiguraatio (c1812)

```
maricper02#sh run
Building configuration...

Current configuration : 1581 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname maricper02
!
boot-start-marker
boot-end-marker
!
no logging console
enable password tele
!
no aaa new-model
!
resource policy
!
ip cef
!
!
track 1 interface FastEthernet0 line-protocol
!
interface FastEthernet0
 ip address 10.10.11.1 255.255.255.252
 duplex auto
 speed auto
!
```

```
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 ip address 192.168.100.3 255.255.255.0
 vrrp 1 ip 192.168.100.1
 vrrp 1 priority 105
 vrrp 1 track 1
!
router bgp 65499
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute static
 neighbor 10.10.11.2 remote-as 65000
 neighbor 10.10.11.2 description mariedger01
 neighbor 10.10.11.2 route-map ASPREPEND out
 neighbor 192.168.100.2 remote-as 65499
 neighbor 192.168.100.2 description maricper01/primary
 no auto-summary
!
!
no ip http server
no ip http secure-server
route-map ASPREPEND permit 10
```

```
 set as-path prepend 65499 65499 65499
!
control-plane
!
!
line con 0
 password cisco
line aux 0
 password cisco
line vty 0 4
 password cisco
 login
!
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

Liite 7. Maricper01 konfiguraatio, BGP + OSPF (Juniper)

```
testi@maricper01> show configuration
## Last commit: 2011-04-27 15:38:48 EEST by chaffinch
version 10.0R1.8;
system {
    host-name maricper01;
    time-zone Europe/Helsinki;
    internet-options {
        path-mtu-discovery;
        source-port {
            upper-limit 65535;
        }
        tcp-drop-synfin-set;
    }
    authentication-order password;
    root-authentication {
        encrypted-password "$1$15c1QEBD$2xchhYkROh2sX24/d8ddV0"; ## SECRET-
DATA
    }
    login {
        retry-options {
            tries-before-disconnect 3;
        }
        class admin {
            idle-timeout 10;
```

```
        login-alarms;
        permissions all;
      }
      class view-config {
        idle-timeout 10;
        permissions view;
      }

      user remote-rw {
        uid 2004;
        class admin;
      }
      user testi {
        uid 2002;
        class admin;
        authentication {
          encrypted-password "$1$XCWyGxoh$76hRAcCTI0x5Ix2PJjFJX1"; ## SECRET-
DATA
        }
      }
    }
    services {
      telnet;
    }
    syslog {
      archive size 100k files 3;
      user * {
        any critical;
      }
      file messages {
        any any;
        authorization info;
      }
      file interactive-commands {
        any any;
        interactive-commands any;
      }
      file error-messages {
        any error;
        authorization error;
      }
      file auth-debug {
        authorization any;
        archive size 1m files 2;
      }
      time-format millisecond;
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 5;
```

```
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
chassis {
    config-button no-clear;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.10.10.1/30;
            }
        }
    }
    fe-0/0/5 {
        unit 0 {
            family inet {
                address 10.1.1.1/30;
            }
        }
    }
    fe-0/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.2/32;
            }
        }
    }
}
routing-options {
    graceful-restart;
    autonomous-system 65499;
}
protocols {
    bgp {
        hold-time 30;
        group TO_EDGE {
            type external;
            description eBGP;
            neighbor 10.10.10.2 {
                import LOCALPREFIN;
                export PREFIXES_OUT;
                peer-as 65000;
```

```
        }
      }
    }
    ospf {
      export BGP_TO_OSPF;
      import FROM_OSPF;
      area 0.0.0.0 {
        interface fe-0/0/5.0;
      }
    }
}
policy-options {
    policy-statement BGP_TO_OSPF {
      term ALL {
        from protocol bgp;
        then {
          tag 555;
          external {
            type 1;
          }
          accept;
        }
      }
    }
    policy-statement FROM_OSPF {
      term DENY_LOOPING {
        from tag 555;
        then reject;
      }
      term REST {
        from protocol ospf;
        then accept;
      }
    }
    policy-statement LOCALPREFIN {
      term LOCALPREF_PRIMARY {
        from {
          route-filter 0.0.0.0/0 upto /32;
        }
        then {
          local-preference 200;
          accept;
        }
      }
      term DEFAULT_ACTION {
        then reject;
      }
    }
    policy-statement NEXTHOP_SELF {
```

```
        term ONE {
            then {
                next-hop self;
                accept;
            }
        }
    }
    policy-statement PREFIXES_OUT {
        term PRIMARY_OUT {
            from protocol [ direct local static bgp ospf ];
            then accept;
        }
        term DEFAULT_ACTION {
            then reject;
        }
    }
}
security {
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                all;
            }
        }
    }
    policies {
        default-policy {
            permit-all;
        }
    }
}

testi@maricper01>
```

Liite 8. Maricper02:n konfiguraatio, BGP + OSPF (c1812)

```
maricper02#sh run
Building configuration...

Current configuration : 1793 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname maricper02
!
boot-start-marker
boot-end-marker
!
no logging console
enable password cisco
!
no aaa new-model
!
resource policy
!
ip cef
!
track 1 interface FastEthernet0 line-protocol
!
interface FastEthernet0
 ip address 10.10.11.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet2
!
interface FastEthernet3
!
```

```
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 ip address 10.1.1.5 255.255.255.252
 ip ospf cost 1000
 ip ospf priority 11
!
router ospf 100
 log-adjacency-changes
 redistribute bgp 65499 metric 200 subnets tag 555
 network 10.1.1.4 0.0.0.3 area 0
!
router bgp 65499
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute static
 redistribute ospf 100 match internal external 1 external 2 route-map LOOPIN_ESTO
 neighbor 10.10.11.2 remote-as 65000
 neighbor 10.10.11.2 description mariedger01
 neighbor 10.10.11.2 route-map ASPREPEND out
 no auto-summary
!
no ip http server
no ip http secure-server
!
route-map LOOPIN_ESTO deny 10
 description * Suodata reitit tagilla 555 *
 match tag 555
!
route-map LOOPIN_ESTO permit 15
!
route-map ASPREPEND permit 10
 set as-path prepend 65499 65499 65499
!
control-plane
!
!
```

```
line con 0
 password cisco
line aux 0
 password cisco
line vty 0 4
 password cisco
 login
!
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end

maricper02#
```

Liite 9. Mariswi01:n konfiguraatio

```
mariswi01#sh run
Building configuration...

Current configuration : 1958 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mariswi01
!
logging buffered 65000 debugging
no logging console
enable password cisco
!
ip subnet-zero
ip routing
!
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 100
!
```

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface GigabitEthernet0/3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/4
 no switchport
 ip address 10.1.1.9 255.255.255.252
 ip ospf cost 100
 ip ospf priority 11
!
interface GigabitEthernet0/5
 switchport mode dynamic desirable
!
interface GigabitEthernet0/6
 switchport mode dynamic desirable
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
!
interface GigabitEthernet0/8
 switchport mode dynamic desirable
!
interface GigabitEthernet0/9
 switchport mode dynamic desirable
!
interface GigabitEthernet0/10
 switchport mode dynamic desirable
! interface GigabitEthernet0/11
 switchport mode dynamic desirable
!
interface GigabitEthernet0/12
 no switchport
 ip address 10.1.1.2 255.255.255.252
 ip ospf cost 100
 ip ospf priority 11
!
interface Vlan1
 no ip address
 no ip redirects
!
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
```

```
 no ip redirects
 standby 1 ip 192.168.100.1
 standby 1 priority 120
 standby 1 preempt
 standby 1 authentication mari
 standby 1 track GigabitEthernet0/12
!
router ospf 100
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.8 0.0.0.3 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
ip classless
ip http server
!
access-list 77 permit any
snmp-server community tunturi RW 77
snmp-server packetsize 1024
!
line con 0
 password cisco
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

mariswi01#
```

Liite 10. Mariswi02:n konfiguraatio

```
mariswi02#sh run
Building configuration...

Current configuration : 2125 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mariswi02
```

```
logging buffered 65000
no logging console
enable password cisco
!
no aaa new-model
!
ip subnet-zero
ip routing
!
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 100
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface GigabitEthernet0/3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/4
 no switchport
 ip address 10.1.1.10 255.255.255.252
 ip ospf cost 1000
 ip ospf priority 100
!
interface GigabitEthernet0/5
 switchport mode dynamic desirable
!
interface GigabitEthernet0/6
 switchport mode dynamic desirable
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
!
interface GigabitEthernet0/8
 switchport mode dynamic desirable
!
interface GigabitEthernet0/9
 switchport mode dynamic desirable
```

```
interface GigabitEthernet0/10
 switchport mode dynamic desirable
!
interface GigabitEthernet0/11
 switchport mode dynamic desirable
interface GigabitEthernet0/12
 no switchport
 ip address 10.1.1.6 255.255.255.252
 ip ospf cost 1000
 ip ospf priority 100
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 192.168.100.3 255.255.255.0
 standby 1 ip 192.168.100.1
 standby 1 priority 115
 standby 1 preempt
 standby 1 authentication mari
 standby 1 track GigabitEthernet0/12
!
router ospf 100
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 network 10.1.1.4 0.0.0.3 area 0
 network 10.1.1.8 0.0.0.3 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
ip classless
ip http server
!
route-map ASPREPEND permit 10
 set as-path prepend 65499 65499 65499
!
control-plane
!
line con 0
 password cisco
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

mariswi02#
```