Mikko Sipponen

DMVPN-ominaisuuden tutkiminen ja geneerisen ratkaisun kehittäminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

22.4.2016

Metropolia

Tekijä Otsikko Sivumäärä Aika	Mikko Sipponen DMVPN-ominaisuuden tutkiminen ja geneerisen ratkaisun kehittäminen 30 sivua + 2 liitettä 22.4.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Osaamisaluepäällikkö Janne Salonen

Insinöörityön tavoitteena oli tutustua Ciscon DMVPN-ominaisuuteen ja luoda hyvin räätälöidyn TeliaSoneran pilottiasiakaskonfiguraation pohjalta geneerisempi konfiguraatio, jota voitaisiin käyttää huomattavasti laajemmalla yritysasiakaspohjalla.

Työssä käsitellään DMVPN:n kehitystaustaa ja yleistä teoriaa sen toiminnasta, jonka jälkeen esitellään tuloksena ollut geneerinen konfiguraatio vaihe vaiheelta. Hieman erikoisemmat konfiguraatiokomennot avataan myös tarkemmin, miksi ne valittiin ja mitä ne tekevät.

Opinnäytetyön tuloksena oli geneerinen ja skaalautuva konfiguraatio muutamalla vaihtoehdolla reitityksen osalta. Viimeisenä esitellään työn konfiguraation testitulokset, konfiguroinnissa huomioitavat seikat ja vaikutukset asiakastoimitukseen.

Avainsanat	DMVPN, Geneerinen konfiguraatio

Author Title Number of Pages Date	Mikko Sipponen Exploring DMVPN technology and developing a generic configuration 30 pages + 2 appendices 22 April 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructor	Janne Salonen, Director of Engineering and Technology

The aim of the Thesis was to explore Cisco's DMVPN technology and create a generic configuration, applicable to a wide business customer base, based on a pilot customer's very specific configuration.

The thesis starts with the reasons for developing DMVPN and the general theory behind the technology, and moves on to present the resulted generic configuration step-by-step. The more exotic configuration commands are explained in detail, what they do and why they're used.

The result of the thesis was a generic and scalable configuration with a few alternatives regarding routing options. The test results of the configuration, things to consider in the configuration process and the general impact on the customer delivery process are discussed last.

Keywords	DMVPN, Generic configuration

Sisällys

Lyhenteet

DMVPN	Dynamic Multipoint Virtual Private Network. Ciscon kehittämä dynaaminen VPN-reititystekniikka.
NHRP	Next Hop Resolution Protocol. DMVPN:ssä käytetty, aiemmin kehitetty protokolla reitin selvittämiseksi.
CPE	Customer-premises equipment. Asiakkaan tiloissa sijaitsevat, toisen yrityksen omistamat laitteet.
OSI	Open Systems Interconnection Reference Model. Tiedonsiirrossa käytettävät protokollat eritasoissa kuvaava malli.
NBMA	Non-Broadcast, Multi-Access. Verkko, jossa on monta laitetta, mutta ei broadcast-liikennettä.
ATM	Asynchronous Transfer Mode. Protokolla, jossa data siirretään pienissä, vakiomittaisissa paketeissa.
NHS	Next-Hop Server. NHC-tietoja ylläpitävä laite NHRP-protokollassa.
NHC	Next-Hop Client. Laite, joka ei ylläpidä tietoja NHC-laitteista vaan rekisteröi itsensä NHS:lle NHRP-protokollassa.
PVC	Permanent virtual circuit. Kiinteä pakettikytkentäisten protokollien kytkentä.
SVC	Switched virtual circuit. Väliaikainen pakettikytkentäisten protokollien kytkentä.
CEF	Cisco Express Forwarding. Ciscon kehittämä rautapohjainen reititysratkaisu softwarepohjaisen sijasta. Vähentää reititykseen vaadittavaa prosessointitehoa ja vapauttaa resursseja muille toiminnoille.
WAN	Wide area network. Laajalle maantieteelliselle alueelle ulottuva verkko.

VRF	Virtual routing and forwarding. Tekniikka, joka mahdollistaa useamman reititystaulun samanaikaisen olemassaolon yhdellä reitittimellä. Mahdollistaa samojen IP-osoitteiden käytön eri interfaceilla ja eri verkkojen reititysten erottamisen toisistaan.
GRE	Generic Routing Encapsulation. Ciscon kehittämä tunnelointitekniikka, jolla voidaan salata monta verkkokerroksen protokollaa virtuaalisten point-to-point-linkkien sisään.
mGRE	Multipoint GRE. GRE-tunneli, jolla on yksi lähtöpiste ja monta vastapäätä.
IPsec	Internet Protocol Security. Kokoelma protokollia, joiden avulla viestintätapahtuma voidaan salata ja autentikoida.
Cisco IOS	Cisco Internetwork Operating System. Ciscon laitteiden käyttöohjelmisto.
ESP	Encapsulating Security Payload. IPseciin kuuluva protokolla, jolla varmistetaan paketin alkuperäisyys, eheys sekä luottamuksellisuus.
AH	Authentication Header. IPseciin kuuluva protokolla, jolla varmistetaan paketin alkuperäisyys sekä eheys.
IKE	Internet Key Exchange. IPseciin kuuluva protokolla avainten vaihtoon SA:n muodostamiseksi.
SA	Security association. Todennus siitä, että kaksi verkkolaitetta jakavat samat tietoturva-attribuutit.
NAT	Network address translation. Tekniikka, jolla käännetään yksi osoiteavaruus toiseksi.
CA	Certificate authority. Digitaalisia varmenteita myöntävä taho.
TCP	Transmission Control Protocol. Yksi IP-maailman ydinprotokollista, joka kontrolloi tietovirran siirtoa.

RA	Registration Authority. Taho, joka todentaa digitaalisten varmenteiden pyynnöt ja ohjeistaa CA:n myöntämään varmenteen.
DNS	Domain Name System. Nimijärjestelmä, joka yhdistää IP-osoitteen helpommin muistettavaan nimeen.
CRL	Certificate Revocation List. CA:n jakama lista perutuista varmenteista.
QoS	Quality of Service. Pakettien priorisoiminen niiden tärkeyden ja kiireellisyyden mukaan.
AES	Advanced Encryption Standard. Vuonna 2001 julkaistu salausalgoritmi.
MTU	Maximum transmission unit. Suurin yksikkökoko, joka voidaan lähettää.
MPLS	Multiprotocol Label Switching. Tekniikka, jossa dataa lähetetään solmujen kautta lyhyiden leimojen perusteella pitkien osoitteiden reitityksen sijaan.
ICMP	Internet Control Message Protocol. Yksi IP-maailman ydinprotokollista, jolla välitetään laitteiden tilannetietoja.
IGP	Interior Gateway Protocol. Reititysprotokolla, jolla välitetään tietoa samassa AS:ssa sijaitsevien laitteiden kanssa.
BGP	Border Gateway Protocol. Reititysprotokolla, jolla välitetään tietoa samassa AS:ssa sijaitsevien laitteiden kanssa ja eri AS:ien välillä.
EIGRP	Enhanced Interior Gateway Routing Protocol. Ciscon kehittämä, Ciscon laitteilla toimiva reititysprotokolla.
OSPF	Open Shortest Path First. Kenties laajimmin käytetty IGP-protokolla.
AS	Autonomous system. Yhden tai useamman, yhden tahon ylläpidossa olevan verkon reitityksen yksikkö.

1 Johdanto

DMVPN-ominaisuus Ciscon laitteilla on huomattavan laajojen VPN-verkkojen kevyen luonnin mahdollistava tekniikka, joka otettiin TeliaSoneran pilottiasiakkaalla käyttöön vuoden 2015 aikana. Tekniikka itsessään ei ole kovinkaan uusi, mutta moni asiakas on pitäytynyt omissa VPN-ratkaisuissaan, eikä ole vaatinut erillistä salausta operaattorin laitteen lähiverkkojen ja runkoverkon välillä. Tästä syystä VPN-konfiguraatiot CPE-laitteilla ovat lähes aina olleet asiakaskohtaisia, ja toteutustapa on täysin konfiguroivasta työntekijästä kiinni.

Julkisuudessa olleet suuret tietomurrot ja yleinen digitalisaatio ovat kuitenkin viime vuosina kannustaneet yrityksiä panostamaan tietoturvaan yhä enemmän, jopa taloudellisen taantumankin keskellä. Kasvanut panostus tarkoittaa TeliaSoneran kohdalla kysyntää toimitettujen yhteyksien turvaamiselle yhä useammalla tavalla. Kasvaneen kysynnän johdosta laajojen verkkojen VPN-toteutuksien standardoinnista on tullut perusteltua.

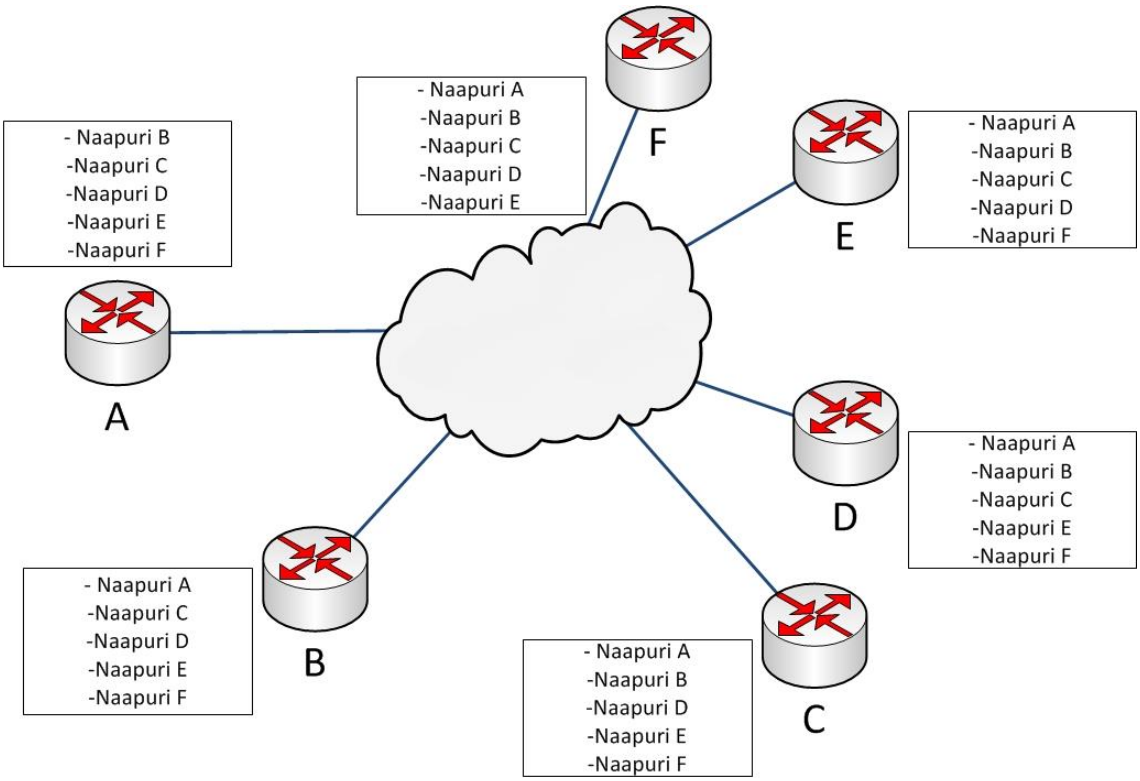
Työssä lähdettiin tutkimaan pilottiasiakkaan varsin monimutkaista DMVPN-verkkokonfiguraatiota tavoitteena puristaa se kasaan mahdollisimman geneeriseksi, jotta työn tulokseksi saatua konfiguraatiota voisi käyttää vähintäänkin pohjana mahdollisimman monelle asiakkaalle (asiakkaalla tarkoitetaan koko insinöörityössä yritysasiakasta). Asiakaskunnan laajuus asetti omat haasteensa konfiguraation geneerisyydelle ja pakotti lopulta tekemään reitityksen osalta kaksi eri vaihtoehtoa.

Tuloksena oleva konfiguraatio toimii tavoitteiden mukaisesti ja on skaalautuva, mutta testiympäristön rajallisuuden ja toimitusprosessin tämänhetkisten valmiuksien vuoksi päädyttiin antamaan kokemukseen ja pohdintaan perustuvia suosituksia jatkokehityksen suhteen.

2 DMVPN-tekniikan esittely

2.1 Kehitystarve

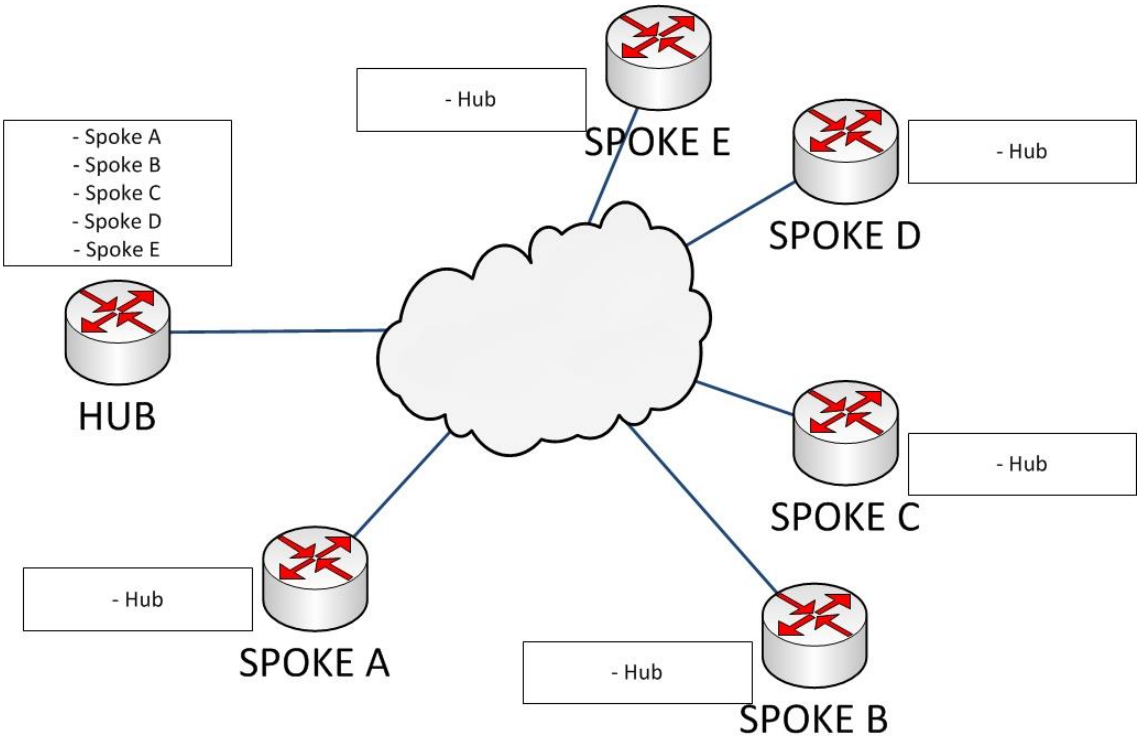
Dynamic Multipoint Virtual Private Network (DMVPN) on dynaaminen, Ciscon verkkolaitteiden tukema VPN-ratkaisu. DMVPN on tekniikkana kehitetty salausta vaativia, suuria ja usein voimakkaassa muutoksessa olevia verkkoja varten. Näiden verkkojen VPN-yhteyksien luonti ja ylläpitäminen perinteisillä menetelmillä on erittäin raskasta ja aikaa vievää. Asia voidaan havainnollistaa esimerkillä.



Kuva 1. Full mesh -topologialla toteutettu point-to-point VPN-verkko. Laitteiden yhteydessä vaadittavat tunnelinaapuruudet.

Perinteisillä point-to-point-VPN-tunneleilla toteutetussa full mesh -verkossa (kuva 1) tulisi jokaiselle laitteelle konfiguroida VPN-yhteys kaikkiin muihin verkon laitteisiin. Verkon kasvaessa tai pienentyessä yhdelläkin laitteella tulisi jokaisen laitteen konfiguraatioon tehdä manuaalisesti muutoksia. Ilmeisenä vaarana näissä muutoksissa verkon toimivuuden ja turvallisuuden kannalta on inhimillinen erehdys tai unohdus yhden tai useamman laitteen konfiguraation päivityksessä.

Reititinmäärän kasvaessa satoihin tai tuhansiin viankorjaus tai -rajaus on myös huomattavasti vaikeampaa, sillä jokaisella laitteella on tällöin satoja rivejä VPN-konfiguraatiota. Tunneleihin kuluvien IP-osoitteiden määrä point-to-point-tunneleilla toteutetussa full mesh -verkossa on myös valtava, vaikka privaattiosoitteita voidaankin käyttää. Vaikka aliverkotuksessa käytettäisiin maskia /30, puolet tunneleihin varatuista IP-osoitteista menisi hukkaan. Käytännössä asetelma toimii vain verkoissa, joissa point-to-point VPN-yhteys konfiguroidaan ainoastaan muutaman laitteen välille.



Kuva 2. Hub & spoke -topologialla toteutettu point-to-point-VPN-verkko. Laitteiden yhteydessä vaadittavat tunnelinaapuruudet.

Full mesh -topologian ylläpidollisesti raskasta ja IP-osoitteita valtavasti syövää asetelmaa pystytään keventämään huomattavasti vaihtamalla verkon topologia full mesh -tyyppisestä hub & spoke -ratkaisuksi (kuva 2). Kyseisessä ratkaisussa yksi laite valitaan toimimaan hubina, jonka kautta kaikki VPN-liikenne kulkee, jolloin verkon muille laitteille, spokeille riittää konfiguraatiossa vain yksi VPN-tunneli hubille. Hubille tulee toisaalta tällöin konfiguroida yhteys kaikkiin muihin laitteisiin. Ratkaisu on muutoksenhallinnan näkökulmasta full meshiä kevyempi, sillä verkkomuutokset vaikuttavat konfiguraatioon vain hubissa ja muutoksen kohteena olevassa laitteessa.

Tässäkin ratkaisussa on toki ongelmansa, sillä muutostoimenpiteiden kohdistuessa pääasiassa johonkin spokeen on konfiguraatiomuutosten unohtamisen riski hubin osalta edelleen olemassa. Jokaista tunnelia varten tarvitaan edelleenkin aliverkko, jolloin IP-osoitteita menee edelleen hukkaan, joskin huomattavasti vähemmän kuin full mesh -verkossa. Kaiken VPN-liikenteen kierrättäminen yhden pisteen kautta myös rasittaa hubia kuluttamalla kaistanopeutta sekä prosessointitehoa. Hubin konfiguraatiosta tulee niinikään myös hyvin raskas, sillä jo sadan reitittimen verkko tarkoittaa 700 riviä konfiguraatiota. DMVPN:llä vastaava ratkaisu saadaan toteutettua 15 konfiguraatiorivillä [1].

2.2 Ratkaisuna DMVPN

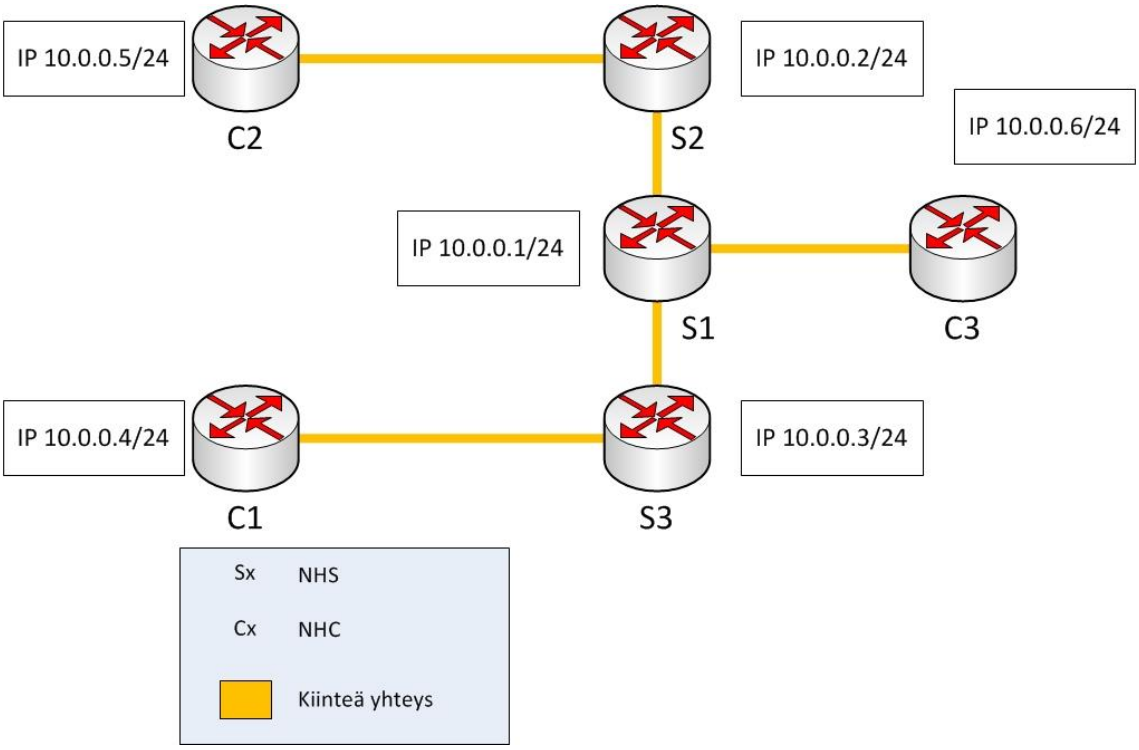
DMVPN on useiden tekniikoiden yhdistelmä, jossa pohjimmaisin komponentti on multipoint GRE -tunneli. Kuten aiemmin todettiin, point-to-point-yhteyksillä toimivassa VPN-verkossa jokainen tunneli vaatii oman aliverkkonsa. Point-to-point GRE -tunnelissa aliverkotettu tunnelin osoite sidotaan manuaalisesti muun verkon löydettävissä olevaan porttiin ja sen osoitteeseen, useimmiten laitteen ulkoverkon porttiin tai loopback-interfaceen. Multipoint GRE -tunnelissa tehdään laitteen omalta osalta vastaava sidonta kuin point-to-point-tunnelissa. Tunnelin toinen pää jää kuitenkin "auki". Toinen pää jätetään määrittelemättä, koska mGRE-tunnelit toimivat samassa aliverkossa, ja siten tunnelin toisia päitä on nimen mukaisesti useita. Tarkalleen ottaen mahdollisia tunnelin kohteita on niin monta kuin käytetyssä aliverkossa on muita host-osoitteita. Jos jokaisen tunnelinaapurin osoitesidonta tehtäisiin manuaalisesti, olisi mGRE-tunneleista hyötyä ainoastaan IP-osoitteiden säästämisen osalta. Työmäärä olisi edelleen valtava alkutoteutuksen ja muutoksenhallinnan osalta. Naapureiden osoitesidonnan dynaamisesti hoitava työkalu on selkeästi tarpeellinen, ja siinä vaiheessa kuvaan astuu NHRP.

2.3 NHRP

DMVPN-toteutuksessa liikennöinti verkossa voidaan toteuttaa joko hub-to-spoke- tai spoke-to-spoke-liikenteellä NHRP-protokollaa käyttäen. NHRP kehitettiin 1990-luvun lopulla OSI-mallin toisen tason NBMA-verkkojen reitityksen optimointiin [2]. Tällaisia verkkotekniikoita ovat esimerkiksi ATM ja Frame-Relay. Optimoinnin taustaideana oli luoda ”oikopolkuja” eli väliaikaisia yhteyksiä osittaisella mesh-topologialla muodostettuun

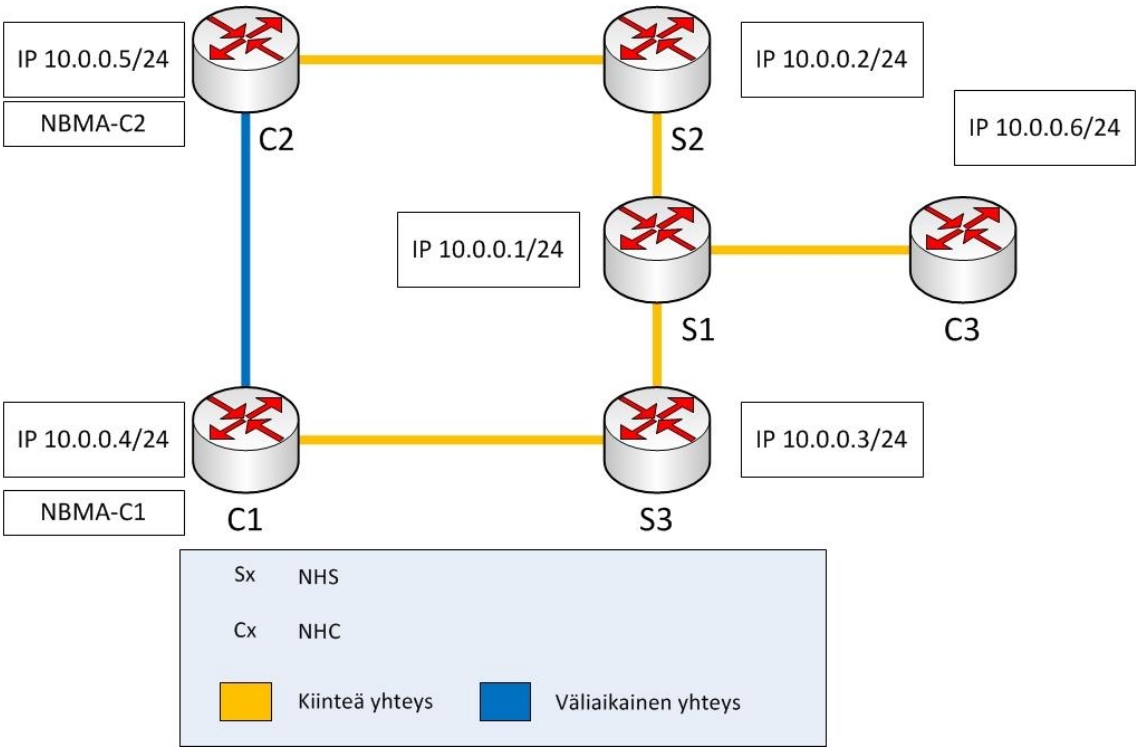
NBMA-verkkoon tarpeen mukaan ja vähentää siten turhaa liikennettä välikäsinä toimivilla laitteilla. Joitain vuosia protokollan määrittelyn jälkeen sitä päädyttiin hyödyntämään DMVPN:ssä.

NHRP-protokolla on elementti, joka tekee DMVPN:stä dynaamisen. Sen alkuperäisenä geneerisenä tehtävänä oli kytkeä IP-osoitteet ”oikeisiin” osoitteisiin, eli vanhojen verkkotekniikoiden normaalilla reitityksellä löydettävissä oleviin L2-osoitteisiin. Protokollan kaksi roolia reitittimille ovat NHS ja NHC. NHC (Next-Hop Client) on osapuoli, joka rekisteröi oman IP-osoitteensa ja L2-NBMA-osoitteensa määritellylle NHS:lle (Next-Hop Server). NHS pitää kirjaa sille rekisteröityneiden NHC-laitteiden IP-osoitteista sekä NBMA-osoitteista. Huomioitavaa on se, että laite voi samanaikaisesti olla sekä NHS, että NHC. Yhteys NHC:n ja NHS:n välillä on aina erikseen ja manuaalisesti määritelty, joten sitä voidaan pitää kiinteänä yhteytenä. [3.] Otetaan esimerkki (kuva 3).



Kuva 3. Lähtöasetelma NHRP:lle NBMA-verkossa.

Kuvan 3 mukaisessa asetelmassa NBMA-verkossa on useita server- ja client-laitteita. NHS-määrittelyt, eli kiinteät yhteydet on esitetty laitteiden välillä. Kiinteät yhteydet vanhoilla tekniikoilla ovat käytännössä PVC-kytköksiä (permanent virtual circuit). Tilanteessa, jossa C1 haluaisi lähettää paketin osoitteeseen 10.0.0.5, kulkisi se reittiä C1-S3-S1-S2-C2. C1 ei tietäisi mitään muista laitteista, joten se lähettäisi paketin määritellylle NHS:lleen, joka tässä tapauksessa on S3. S3 puolestaan katsoisi sille rekisteröityneiden NHC-laitteiden tiedot, ja huomattuaan, ettei osoitetta 10.0.0.5 löydy sen tiedoista, laittaisi se paketin eteenpäin ainoalle tuntemalleen NHS:lle, S1:lle. Kyselyn vastaanotettuaan S1 huomaisi, ettei senkään tiedossa ole kohdeosoitetta, joten se laittaisi paketin edelleen eteenpäin S2:lle. Vasta S2:lla olisi tieto kohdeosoitteesta, jonne paketti lopulta päätyisi. Liikenne olisi huomattavasti taloudellisempaa, jos C1 pystyisi liikennöimään suoraan C2:lle. Kyseinen liikennöinti onnistuu NHRP:n ja NBMA-osoitteiden avulla.



Kuva 4. NHRP:n toiminta NBMA-verkossa.

NBMA-osoitteet ovat NHRP:n keino löytää kohdelaite mistä päin verkkoa tahansa ja liikennöidä sille suoraan. Sen sijaan, että C1 lähettäisi kaikki paketit määriteltyjä PVC-kytkentöjä pitkin, lähettää se kyselypaketin kohdeosoitteen 10.0.0.5 tiedoista. Paketti

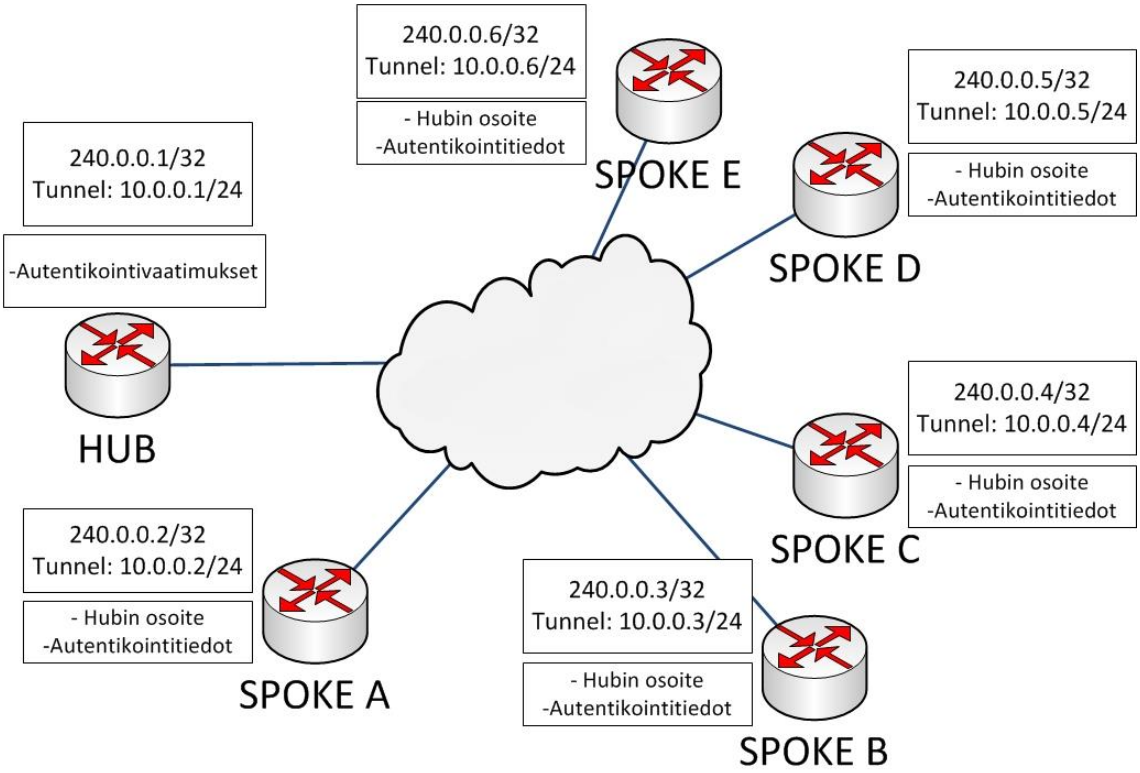
päätyy samalla tavalla samaa reittiä noudattaen S2:lle, jolta kohdeosoitteen NBMA-osoitetieto lopulta löytyy. Huomattuaan tietävänsä tiedustellun osoitteen rekisteröitymisen kautta, vastaa S2 lähettäjälle viestillä, jossa kertoo C2:n NBMA-osoitteen.

Opitun L2-tason NBMA-osoitteen avulla C1 löytää C2:n mistä tahansa topologian taustalla olevasta L2-verkosta ja pystyy muodostamaan sille suoran, väliaikaisen yhteyden liikennöintiä varten (kuva 4). Verkoissa, joille NHRP suunniteltiin, tällaiset väliaikaiset yhteydet ovat käytännössä SVC-kytköksiä (switched virtual circuit).

DMVPN-tekniikassa NHRP:tä ei kuitenkaan käytetä alkuperäisessä tarkoituksessaan, jossa se sitoi koko verkon löydettävissä olevan L2-NBMA-osoitteen vaikeammin paikallistettavaan IP-osoitteeseen. Syy tähän on yksinkertaisesti se, että aika on suurelta osin ajanut ohi niistä teknologioista, joille NHRP alun perin kehitettiin. Tekniikkaa voi kuitenkin soveltaa nykyäänkin vaihtamalla aikaisempi taustalla ollut L2-NBMA-verkko taustalla olevaksi L3-verkoksi. Alkuperäisessä NHRP:ssä looginen IP-verkko oli erillään fyysisestä NBMA-verkosta, ja sama erottelu on IP-maailmassa olemassa ”normaalin” verkon ja salattujen tunneleiden välillä. NHRP sitoo mGRE-tunnelin vaikeasti paikallistettavan IP-osoitteen koko verkon helposti löydettävissä olevaan IP-osoitteeseen. Useimmissa tapauksissa koko verkon löydettävissä oleva IP-osoite tarkoittaa julkista osoitetta.

2.4 DMVPN-tekniikan toiminta

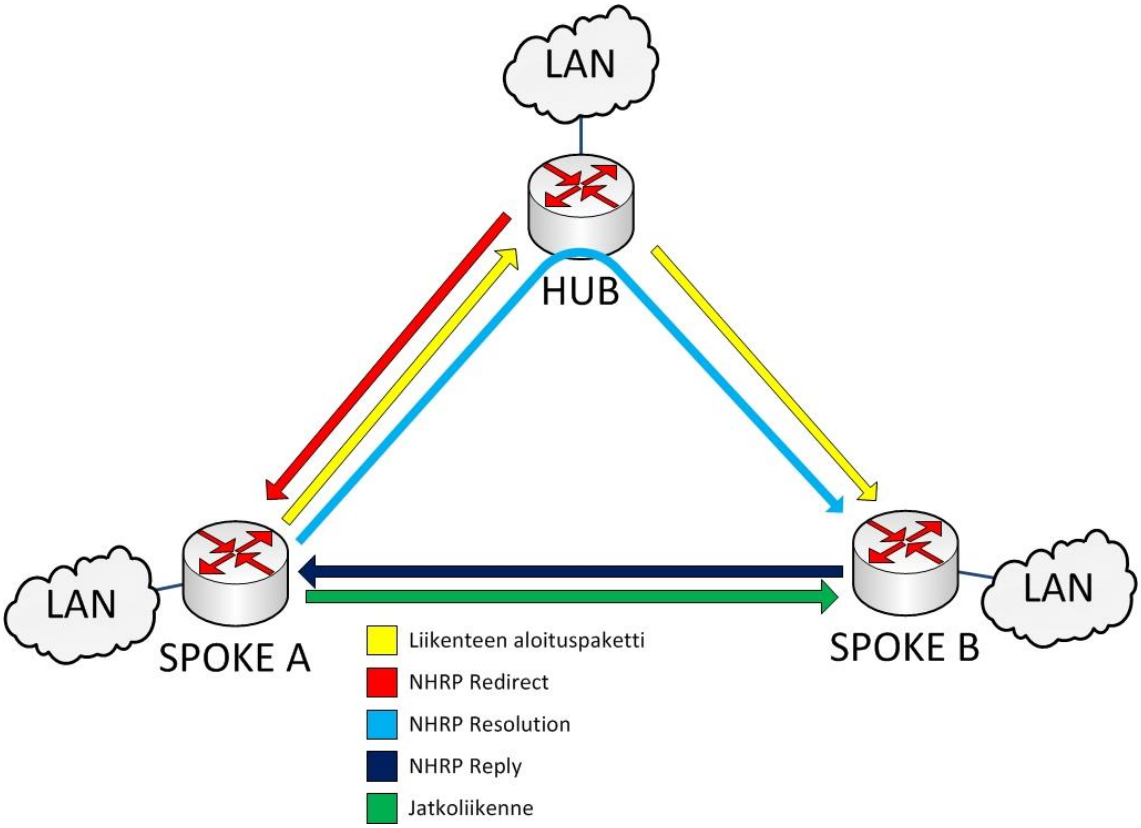
DMVPN:ssä jokaiselle uudelle spokelle konfiguroidaan hubin osoite (kuva 5) NHS-palvelimeksi ja autentikointitiedot rekisteröintiä varten. Näiden avulla spoke rekisteröi itsensä dynaamisesti osaksi verkkoa NHRP-protokollaa käyttäen. Hubille konfiguroidaan puolestaan autentikointivaatimukset, jotka rekisteröinnissä vaaditaan.



Kuva 5. DMVPN-tekniikalla toteutettu VPN-verkko. Laitteiden yhteydessä julkiset osoitteet (NBMA-osoitteet), tunnelien käyttämät privaattiosoitteet sekä konfiguroitavat tiedot.

Ratkaisu keventää verkon konfiguraatiota huomattavasti kumpaankin eri point-to-point-topologialla toteutettuun verkkoon verrattuna, sillä verkon kasvu ei vaadi muille laitteille lisärivejä konfiguraatioon eikä pienentyminen vastaavasti rivien poistoja. Resursseja vapautuu myös IP-osoitteiden puolelta, sillä mGRE-tunnelit voivat olla samassa aliverkossa. Kun aliverkon koko valitaan kattamaan tarvittava laitemäärä ja ennakoidaan tuleva laajeneminen ei juuri yhtään osoitetta mene hukkaan. Keventävä vaikutus ei kuitenkaan vielä hub-to-spoke-liikennetoteutuksessa ulotu liikenteeseen, joka kiertää edelleen täysin hubin kautta. Tekniikasta tulee liikennekuormankin osalta dynaaminen vasta spoke-to-spoke-liikenteen mahdollistamisen myötä.

Spoke-to-spoke-liikenteessä spoket avaavat dynaamisia tunneleita toisilleen tarpeen mukaan. Nämä tunnelit keventävät hubin liikennetaakkaa merkittävästi, koska valtaosa liikenteestä ei tällöin enää kierrä sen kautta.



Kuva 6. DMVPN spoke-to-spoke -liikenteen aloitus vaiheittain.

Dynaamisen tunnelin ensimmäinen avaus (kuva 6) spokelta toiselle alkaa paketin lähettämisellä hubille kuten hub-to-spoke-ratkaisussa. Tunnelin avaamistarve syntyy esimerkiksi tilanteessa, jossa spoke saa paketin omasta sisäverkostaan kohteena laite toisen spoken sisäverkossa. Spoke havaitsee, ettei kohdeosoite ole muualla sen omassa sisäverkossa ja lähettää tällöin paketin hubille, koska on saanut siltä käytössä olevalla reititysprotokollalla mainostuksen joko kohdeosoitteesta, yhteenvetoreitin kohteen verkosta tai yksinkertaisimmillaan oletusreitin. Mainostettavat reitit riippuvat hubin konfiguraatiosta ja verkon suunnittelussa tehdyistä reititysratkaisuista. Jos paketin kohteen spoke on rekisteröitynyt hubille, on kohdeverkko ja kohteen spoken tunneli- sekä NBMA-osoite hubin tiedossa ja paketti lähetetään normaalin reitityksen mukaisesti loppukohteeseen.

Paketin välittämisen jälkeen hub kuitenkin vastaa liikenteen aloittaneelle spokelle NHRP redirect -viestillä, joka sisältää kohteen spoken tunneliosoitteen ja kertoo kohteen olevan saavutettavissa optimaalisempaakin reittiä. Heräte redirect-viestin lähettämiselle syntyy paketin välittämisestä ulos samasta interfacesta, josta se on alun perin tullut laitteelle. DMVPN:n tapauksessa kyseessä on hubin mGRE-tunneli-interface. Tästä voi huomata,

kuinka vähän DMVPN-liikennettä kulkee oletuksena hubin kautta spoke-to-spoke-toteutuksissa. Hub ei periaatteessa voi toimia viestinvälittäjänä, koska jokainen välitetty paketti lähtee ulos samasta mGRE-tunnelista, josta se on hubille tullutkin, aiheuttaen redirect-paketin lähettämisen. Tämä ei kuitenkaan tarkoita, etteikö liikennettä voisi kulkea hubin kautta suuriakin määriä.

Viestin saatuaan liikenteen aloittanut spoke lähettää NHRP resolution -pyynnön kohteen spokelle tiedossa olevaa reititystietä pitkin, eli hubin kautta. Pyyntö sisältää kohdeosoitteen sekä lähettäjäspoken NBMA IP-osoitteen, johon kohteen spoke voi lähettää vastauksensa suoraan. Suoraan vastaaminen on mahdollista, koska kohteen spokella on tällöin normaalilla reitityksellä löydettävissä oleva IP-osoite, joka toimii muodostettavan dynaamisen tunnelin toisena päänä.

Pyynnön vastaanottanut spoke katsoo pyydetyn osoitteen verkon omasta reititystaulustaan, avaa dynaamisen tunnelin liikenteen aloittaneen spoken NBMA IP-osoitteeseen ja lähettää NHRP reply -viestin tunnelia pitkin. Reply-viestin lähteenä on kohteen spoken oma NBMA IP-osoite. Vastausviestin saatuaan liikenteen aloittanut spoke tekee omaan NHRP-tauluunsa kirjauksen, joka yhdistää kohdeverkon kyseisen spoken NBMA-osoitteeseen. Aloittajaspoke tekee konfiguraatiostaan riippuen myös CEF-kirjauksen tai -korjauksen ja jatkossa liikennöinti kohdeosoitteeseen tapahtuu dynaamista tunnelia pitkin suoraan kohteen spokelle. [4; 5]

Muodostettavat dynaamiset tunnelit jättävät loogisella tasolla hubin välistä, mutta hubin läpi voi kuitenkin kulkea liikennettä, jos se on taustalla olevan IP-verkon mukainen nopein reitti kohteeseen. Tällöin hub käsittelee salattua pakettia kuin mitä tahansa muuta liikennettä eikä NHRP-protokollaa käytetä. Loppujen lopuksi hubin läpi kulkevan liikenteen määrään vaikuttaa spoke-to-spoke-toteutuksissa kaikkein eniten hubin sijoittuminen loogisella verkkokartalla. Keskeisellä paikalla sijaitseva hub käsittelee pakostikin enemmän liikennettä kuin reunalla toimiva, mikä tarkoittaa, että verkon suunnittelijalla on mahdollisuus vaikuttaa hubin liikenteeseen myös hubin sijoituksella.

3 Konfiguraatio

Soneran liittymien päätelaitteisiin määritellään tilatuista palveluista riippuvainen konfiguraatio, jota ei tässä työssä erikseen käsitellä. DMVPN on oletusarvoisesti lisäpalvelu, jolloin loogisessa järjestyksessä laite konfiguroidaan aluksi perustasolle, jolla yhteys toimii LAN:in ja WAN:in välillä. Vasta perusyhteyden ollessa kunnossa ryhdytään konfiguroimaan lisäpalveluita. Esitettävässä konfiguraatiossa oletetaan laitteen ja sen lähtökonfiguraation olevan jo kunnossa ja yhteyden toimivan.

Työn konfiguraatio kehitettiin pilottiasiakkaan ratkaisun pohjalta, mutta kehityspohjana ollutta konfiguraatiota ei voida asiakkaan tietosuojasyistä esittää. Sitä voidaan kuitenkin kuvailla hyvin asiakaskohtaiseksi kahdennetun hub-yhteyden, lähes kymmenen tunnelin, viiden VRF:n sekä hyvin suodatetun ja kontrolloidun BGP-reitityksen vuoksi.

Tuloksena ollut konfiguraatio esitetään vaihe vaiheelta ja erot hubin sekä spoken konfiguraation välillä tuodaan esiin kohdissa, joissa eroavaisuuksia esiintyy. Esitettävästä konfiguraatiosta on sensuroitu TeliaSoneraan yhdistettävät IP-osoitteet, domainnimet, salasanat sekä muut tiedot, joita voi mahdollisesti käyttää haitallisesti TeliaSoneraa tai sen asiakkaita kohtaan.

DMVPN:stä saadaan liittymän lisäpalveluna mahdollisimman monipuolinen liittämällä se osaksi VRF:ää. Tällöin salaus saadaan kattamaan liikenne halutuista porteista, ja tämän salatun liikenteen reititys saadaan täysin erilleen muusta liikenteestä ja reitityksestä. Tarvittaessa VRF voidaan asettaa kattamaan laitteen kaikki reititys, mutta siinä tilanteessa erillinen VRF-määrittely voidaan yhtä hyvin jättää poiskin.

```
ip vrf dmvpn
rd 4:5
```

VRF:n nimi ja rd-arvo ovat laitekohtaisia, mutta liittymäkonfiguraatioiden yhdenmukaisuuden vuoksi niiden on silti syytä löytyä konfiguraatiopohjasta. Nimi dmvpn kertoo itsestäänselvästi, mihin kyseinen VRF liittyy, kun taas tarpeeksi suuri rd-arvo varmistaa ongelmattoman lisäyksen valtaosalle asiakasliittymistä. Osalla asiakkaista on muita VRF:iä käytössä, mutta niissä rd-arvo on lähtökohtaisesti pienempi.

Täydellinen DMVPN-konfiguraatio koostuu viidestä osatekijästä, jotka ovat

- multipoint GRE (mGRE)
- Next-Hop Resolution protokolla (NHRP)
- dynaaminen reititysprotokolla (EIGRP, RIP, OSPF, BGP)
- dynaaminen Ipsec-salaus
- Cisco Express Forwarding (CEF).

Koska tunnelin määrittelyssä viitataan salausprofiiliin, tulee konfiguraatio aloittaa ylläolevan listan osalta salauksen määrittelystä. Jos näin ei tehdä, palauttaa Ciscon IOS virheilmoituksen rivistä, jossa olemattomaan profiiliin viitataan. Rivin voi toki lisätä tunnelille myöhemminkin, mutta konfiguroinnin johdonmukaisuuden kannalta se ei ole mielekästä.

3.1 Salauskonfiguraatio

IPsec käsittää kaksi asiaa: pakettien salauksen sekä salausavainten vaihdon. Salauksen osalta valitaaan kattavampi ESP, koska vaihtoehtoisesta AH-protokollasta puuttuu pakettien luottamuksellisuuden todentaminen [6]. Avaintenvaihtoprotokollan osalta suositellaan käytettäväksi IKE-protokollaa ja siitä valitaan IKEv2-versio. Oletusversio DMVPN:ssä on IKEv1, ja IKEv2:n valitseminen vie konfiguraatiota FlexVPN:n suuntaan [7]. IKEv2 on kuitenkin yksinkertaisempi ja kehittyneempi versio, jossa TeliaSoneran tarpeiden kannalta merkittävin etu on NAT-tuki [8].

Salauksessa käytettävän IKEv2-protokollan SA-autentikointi voidaan toteuttaa eri tavoilla, joista järkevin vaihtoehto on CA-tahon myöntämä varmenne yhdistettynä digitaaliseen allekirjoitukseen. Kahden ratkaisun vertailussa pre-shared key -metodin ja varmenneautentikoinnin välillä varmenne valittiin sen turvallisuuden, helpon skaalautuvuuden, vähäisen ylläpidon tarpeen sekä vähäisen inhimillisen virheen riskin vuoksi. TeliaSonera myös myöntää ja käyttää omia varmenteitaan, joten infrastruktuuri ratkaisulle on jo olemassa.

```
crypto key generate rsa label ###<<LAITENIMI>>.##########.fi
modulus ####

ip tcp synwait-time 5

ip host ##########.com xxx.xxx.xxx.xxx
ip host ##########com xxx.xxx.xxx.xxx
ip host ##########.com xxx.xxx.xxx.xxx
```

Varmennetta varten luodaan rsa-avain, joka nimetään mm. laitetunnuksen mukaan yksilöllisen avaimen luomiseksi. Avainta käytetään varmenteen hakemiseksi ja sille määritellään myös moduulikoko. Samalla määritellään myös TCP-protokollan yhteyksille sallittu odotusaika sekä varmenteen myöntämiseen liittyvät palvelimet.

```
crypto pki certificate map OU 10
 subject-name = ##########

crypto pki trustpoint ##########.fi
 enrollment retry count 100
 enrollment retry period 10
 enrollment mode ra
 enrollment url ##########
 serial-number
 fqdn <<LAITENIMI>>.##########
 ip-address <<WAN-OSOITE>>
 password ##########
 fingerprint ##########
 subject-name ##########
 revocation-check crl none
 rsakeypair ###<<LAITENIMI>>.##########.fi
 match certificate OU
 auto-enroll 99

crypto pki authenticate ##########.fi
crypto pki enroll ##########.fi
```

Seuraavana tulee konfiguroida varmenteen myöntävä CA lisätietoineen. CA:n tarkastusta varten määritellään varmennekartta **OU**, jonka vastaavuus asetetaan vaatimukseksi varmenteen myöntäjälle myöhemmällä komennolla **match certificate OU**. Rekisteröimisprosessissa käytetään RA-tahoa, minkä vuoksi se määritelläänkin hakumuodoksi. Jos varmennepyyntöön ei määritellystä url-osoitteesta vastata, pyyntöä yritetään uudelleen kymmenen minuutin välein yhteensä sata kertaa. Pyyntöön liitetään laitteen sarjanumero, DNS-tiedot, salasana, varmennejälki, määritelty nimi, sekä aiemmin määritelty rsa-avain, johon varmenne yhdistetään. CRL-tarkastus jätetään pois, koska lista saadaan CA:lta vasta varmenteen myöntämisen jälkeen.

Varmenteilla on voimassaoloaika ja niitä tulee hakea säännöllisesti uudestaan, viimeistään käytössä olevan varmenteen vanhettua. Jotta liikenne ei katkeaisi tai häiriintyisi uuden varmenteen haun vuoksi, konfiguroidaan uuden varmenteen haku alkamaan automaattisesti, kun vanha varmenne on yhden prosentin päässä voimassaolonsa loppumisesta. Tämä tapahtuu komennolla **auto-enroll 99**. Viimeisenä vaiheena käynnistetään oman laitteen sekä CA:n varmenteen haku komennoilla **crypto pki authenticate (CA-nimi)** ja **crypto pki enroll (CA-nimi)**. IKE voidaan konfiguroida, kun varmenne on myönnetty onnistuneesti.

```
crypto ikev2 proposal DMVPN_PROP
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy DMVPN_POL
 match fvrf any
 proposal DMVPN_PROP

crypto ikev2 profile DMVPN_PROF
 match certificate OU
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint ##########.fi
 dpd 10 2 periodic
```

```
crypto logging session
crypto ikev2 disconnect-revoked-peers
```

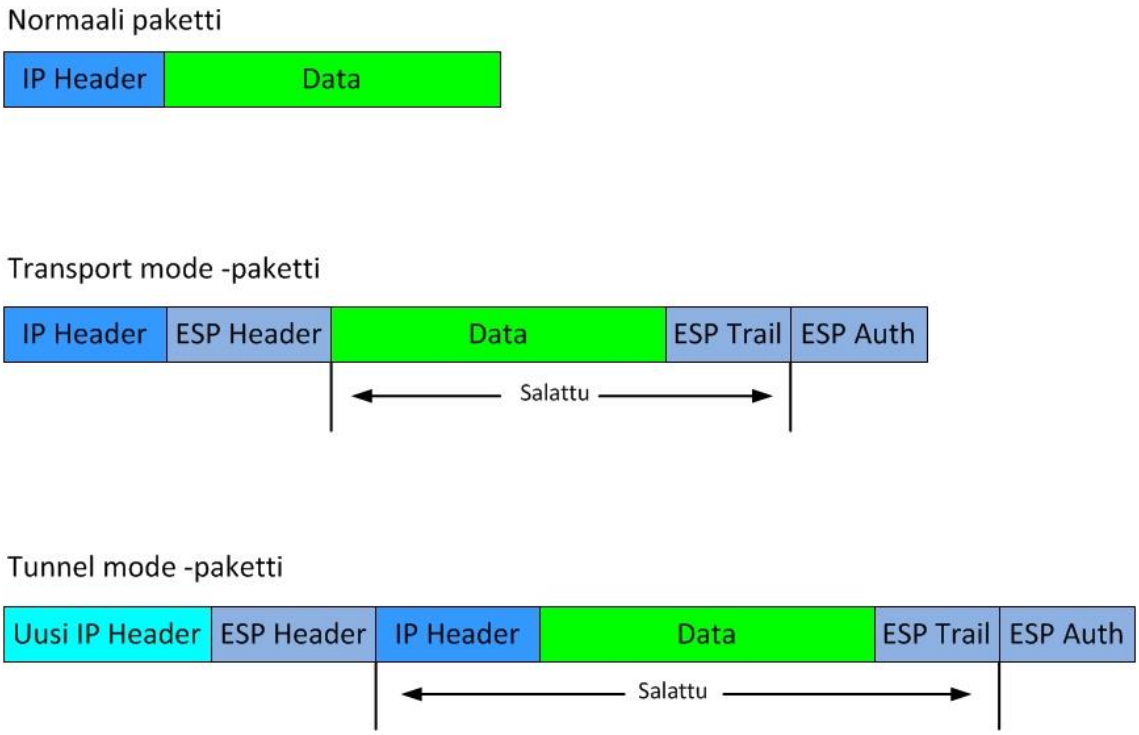
IKE:n osalta konfiguraatiossa määritellään käytettäväksi vahvinta **aes-cbc-256**-salausta ja yhtä pitkää **sha256** hash -algoritmia paketin eheyden takaamiseksi. Diffie-Hellman-ryhmän osalta valitaan suositusten mukainen 2048-bittinen ryhmä 14 [9]. Policyssa mahdollistetaan IKE:n toiminta VRF:ssä ja profiilissa puolestaan määritellään tunnelin toisen pään vaatimukseksi sama varmenne ja autentikointi tehdään rsa-allekirjoituksilla.

Komennolla **dpd 10 2 periodic** asetetaan keepalive-viestit säännöllisiksi 10 sekunnin väliajoin ja mahdollisen vastauksen puuttuessa uudelleenyritysviestien väliajaksi kaksi sekuntia. Tunneleiden yhteyksien katkeamiset tallennetaan logiin komennolla **crypto logging session** ja CRL-listalta löytyviin naapureihin katkaistaan yhteys komennolla **crypto ikev2 disconnect-revoked-peers**.

```
crypto ipsec security-association replay window-size 512

crypto ipsec transform-set DMVPN_TS esp-aes 256 esp-sha-hmac
 mode tunnel
```

Viimeinen osa konfiguraatiosta ennen tunnelin määrittelyä on IPsec-osuus. Pakettien kopiointihyökkäystä vastaan kehitetty anti-replay-suojaus asettaa jokaiselle salatulle paketille uniikin tunnistenumeron ja pitää kirjaa numeroista liikenteen mukana anti-replay window -muistissa. Tämän muisti-ikkunan oletuskoko on 64 pakettia, joka on riittävä useimmissa tapauksissa. Kuitenkin esimerkiksi QoS-määrittelyt saattavat asettaa liian monta priorisoitua pakettia muun liikenteen edelle, mikä johtaa aikaisempien pakettien pudotukseen muisti-ikkunan edettyä niiden tunnistenumeroiden ohitse. [10.] Muisti-ikkunan skaalan mahdollisesti aiheuttamiin ongelmiin puututaan ennaltaehkäisevästi asettamalla ikkunan koko 512 pakettiin komennolla **crypto IPsec security-association replay window-size 512**. Transform-set määrittelyssä ESP-protokollalle valitaaan 256-bittinen salaus AES-algoritmilla ja kattavammin salattu tunnel mode transform moden sijasta (kuva 7).



Kuva 7. Yksinkertaistettu esitys Tunnel moden ja transport moden eroista.

Tunnel mode on Ciscon laitteilla oletuksena, mutta rivistä ei ole haittaakaan, ja se näyttää joka tapauksessa konfiguraatiota tarkastelevalle henkilölle, että IPsecille on asetettu tunnel mode. Kaikki konfiguraatioiden tekemiseen tai tarkasteluun oikeutetut työntekijät eivät välttämättä muista tai tiedä oletusasetuksia, ja laitekohtaiset oletukset voivat periaatteessa muuttua ohjelmistovaihdoksen yhteydessä, joten rivin sisällyttäminen konfiguraatioon on perusteltua.

```
crypto ipsec df-bit clear

crypto ipsec profile DMVPN
 set transform-set DMVPN_TS
 set ikev2-profile DMVPN_PROF
 responder-only
```

IPsec-suojaus sekä liikenteen tunnelointi lisää pakettien pituutta. Pituuden lisäys tulee huomioida interfacejen MTU-arvoissa, jotta kasvaneet paketit mahtuvat läpi. MTU-arvojen kasvattaminen on kuitenkin tehokkaasti toteutettavissa vain TeliaSoneran omassa verkossa, jolloin konfiguraation geneerisyyttä ajatellen pakettien fragmentoinnin sallimisesta tulee mielekästä. Asiakasliittymä voi olla missä päin maailmaa tahansa, eivätkä

kumppanioperaattoreiden tai neljäntenä osapuolena toimivien paikallisoperaattoreiden laitteiston MTU-arvot useimmiten ole tiedossa saati kasvatettavissa TeliaSoneran toimesta. IPsec-pakettien fragmentointi sallitaan komennolla **crypto ipsec df-bit clear**.

IPsec-profiiliin liitetään aiemmin määritellyt transform-set sekä IKE-profiili. Hubille asetetaan profiiliin määrittely **responder-only**, joka nimensä mukaisesti tarkoittaa, että hub ei aloita naapuruuden muodostusta vaan ainoastaan vastaa spokejen aloitteisiin. Spokeilta rivi jätetään luonnollisesti pois.

3.2 Tunneli ja reititys

Tunneli tarvitsee ulkoverkkoa varten julkisivuna toimivan IP-osoitteen, jolla liikennöidään. Tätä varten luodaan Loopback 2, jolle annetaan asiakasverkosta riippuva IP-osoite, joka toimii laitteen NBMA IP -osoitteena. Yksinkertaisin ratkaisu on käyttää julkista IP-osoitetta, mutta jos liikenne esimerkiksi pysyy Suomen sisäisessä MPLS-yritysverkossa, on privaattiosoitteidenkin käyttö mahdollista.

```
interface Loopback2
 description Tunnel source
 ip address ###.###.###.### 255.255.255.255

interface Tunnel2
 ip vrf forwarding dmvpn
 description DMVPN-tunneli, <<LIITTYMÄTUNNUS>>
 ip address ###.###.###.### 255.255.255.###
 bandwidth <<TILATTU NOPEUS>>
 ip mtu 1500
 ip tcp adjust-mss 1460
 no ip redirects
 ip nhrp authentication <<SALASANA>>
 ip nhrp map multicast dynamic
 ip nhrp network-id ##########
 ip nhrp holdtime 360
 ip nhrp redirect
 ip nhrp shortcut
 load-interval 30
 qos pre-classify
```

```
tunnel source Loopback2
tunnel mode gre multipoint
tunnel key ##########
tunnel path-mtu-discovery
tunnel protection ipsec profile DMVPN shared
```

Tunneli itsessään asetetaan VRF:ään ja sille määritellään IP-osoite. Kyseinen osoite salataan IPsec-paketin sisään, joten privaatin IP-osoitteen asettaminen on tässä kohtaa järkevää ja erittäin suositeltavaa julkisten osoitteiden säästämiseksi. Tunnelille määritellään MTU-arvoksi 1500 tavua ja suurimmaksi TCP-segmenttikooksi asetetaan 1460 tavua. Yleiset ICMP-redirect-viestit ovat turvallisuusriski asiakastiloissa sijaitsevissa laitteissa, joten ne poistetaan käytöstä komennolla **no ip redirects**.

NHRP:n osalta asetetaan vaatimuksiksi autentikointisalasana sekä network-id, joiden tulee olla samat kaikilla DMVPN-verkon naapureilla. Koska dynaamiset IGP-reititysprotokollat käyttävät multicast-paketteja, tulee niiden toiminta mGRE-tunnelissa mahdollistaa komennolla **ip nhrp map multicast dynamic**. Holdtimeksi protokollalle asetetaan 360 sekuntia, mikä tarkoittaa, että spoke lähettää NHRP-rekisteröitymispyynnön joka 120. sekunti, ja hub odottaa rekisteröitymispyyntöä spokelta 360 sekuntia. Tällä varmistetaan verkon ajantasaisuus ja vältetään oletusarvoa huomattavasti paremmin virheelliset reittitiedot hubilla, sillä oletusarvo holdtimella on kaksi tuntia [11]. **Ip nhrp redirect** määrittelee hubin lähettämään spokeille redirect-paketteja eli tekee liikenteestä spoke-to-spoke-ratkaisun ja **ip nhrp shortcut** puolestaan tekee reitittimen CEF-tauluun korjauksen/kirjauksen opitusta nopeimmasta reitistä kohdeverkkoihin. Komennot pois jättämällä saadaan luonnollisesti hub-to-spoke-liikenneratkaisu, jos asiakas sellaista toivoo. On huomionarvoista, ettei redirect-komennosta ole mitään haittaa spokellakaan, sillä jos spoke saa paketin ja lähettää sen seurauksena redirect-viestin, on jokin mennyt reitityksessä pieleen ja asia tulee ilmi.

Ciscon IOS kerää jatkuvasti tilastotietoa interfacejen toiminnasta määritellyin väliajoin. Oletusväliaika on viisi minuuttia, mikä riittää hyvin ison kokonaiskuvan tarkasteluun, mutta purskeinen liikenne peittyy helposti niin suureen otantaan. Siksi otannan väliaika säädetään pienimmäksi mahdolliseksi, 30 sekunniksi, komennolla **load-interval 30**. Paketin salaaminen estää myös sisällön QoS-tarkastelun ja siten pakettien oikean priorisoinnin, minkä takia paketit priorisoidaan ennen salausta tai tunnelointia komennnolla **qos pre-classify**.

Tunnelin lähdeportiksi asetetaan aiemmin määritelty Loopback 2 ja vastaavasti aiemmin määritelty IPsec-profiili liitetään tunneliin. Sana komennon **tunnel protection ipsec profile DMVPN shared** perässä mahdollistaa saman profiilin käyttämisen useassa reititysinstanssissa, mikä tämän konfiguraation kannalta tarkoittaa käyttöä VRF:ssä tai useassa VRF:ssä. Tunnelista tehdään mGRE-tunneli komennolla **tunnel mode gre multipoint** ja tunnelin vastapäädyille asetetaan vaatimukseksi sama avaintunniste. Avaintunniste toimii yksilöivänä tekijänä tilanteessa, jossa käytössä on useampia mGRE-tunneleita samalla lähde-interfacella. Jos tunnistetta ei käytettäisi, yhteen verkkoon kuuluvaa liikennettä voisi hyvin päätyä toiseen tunneliin. Tunnisteen käytöllä tuetaan konfiguraation skaalautuvuutta mahdollistamalla useamman tunnelin käyttö jo oletusarvoisesti. Viimeisenä määrittelynä tunnelin toimintaa helpotetaan komennolla **tunnel path-mtu-discovery**, jolloin reititin selvittää dynaamisesti paketin reitin alhaisimman MTU-arvon ja asettaa pakettikoon sen mukaiseksi. Tunnelin konfiguraatiossa on kuitenkin eroa hubin ja spoken osalta siten, että spokella on muutama lisärivi omassa konfiguraatiossaan.

```
ip nhrp map <<HUB-TUNNEL2>> <<HUB-LOOP2>>
ip nhrp nhs <<HUB-TUNNEL2>>
```

Ylläolevat kaksi riviä tekevät laitteesta spoken. Ylempi rivi sitoo hubin tunneliosoitteen sen loopback 2 -osoitteeseen. Loopback-osoite tulisi olla spoken saavutettavissa normaalilla reitityksellä, joten sitomalla hubin tunneli löydettävissä olevaan IP-osoitteeseen, spoke osaa lähettää rekisteröintipyyntönsä oikeaan paikkaan. Komennolla **ip nhrp nhs <<HUB-TUNNEL2>>** määritellystä tunneliosoitteesta tehdään NHS, eli DMVPN:ssä hub kyseiselle spokelle. Viimeisenä osana konfiguraatiosta käydään läpi reititys.

Valtaosalla TeliaSoneran yritysasiakkaista on reititysratkaisuna Soneran oma BGP-reititys MPLS-yritysverkossa, jolloin ainoina erikseen konfiguroitavina reitteinä ovat MPLS-edgellä staattinen asiakkaan lähiverkon mainostus BGP:lle ja asiakastiloissa sijaitsevaan CPE-reitittimeen oletusreitti MPLS-edgelle päin. Tämä reititysratkaisu toimii oikein hyvin paketin siirtämiseen tunnettujen osoitteiden välillä, jolloin tunneloitu paketti saadaan kohdeosoitteeseen eikä muutoksia MPLS:n osalta tarvita. Tunneleiden itsensä osoitteet ja niiden VRF:n sidotut lähiverkot sen sijaan eivät mainostu eikä reititys niihin onnistu ilman dynaamista reititysprotokollaa. Kyseiset reititysviestit ja mainostukset kulkevat tunneloituna MPLS-verkon läpi, eikä siellä ajettava BGP vaikuta valittavaan protokollaan, joten sen osalta reititys on vapaasti valittavissa.

Reititysliikenteen kulkiessa tunneloituna ja reitittyen olemassa olevan infrastruktuurin reititysratkaisujen mukaisesti, saadaan DMVPN-verkosta yksi suljettu AS. Tämä mahdollistaa helpommin konfiguroitavissa olevien IGP-protokollien käytön. Monilla asiakkailla on eri valmistajien laitteita verkoissaan, joten Ciscon oma, vain Ciscon laitteilla toimiva EIGRP-protokolla ei ole mielekäs ratkaisu. Käytännössä jäljelle jää valittavaksi OSPF.

```
####Tunnel-interface(i)lle:
ip ospf network broadcast
ip ospf hello-interval 30
ip ospf priority 255

router ospf 150 vrf dmvpn
 default-information originate
 log-adjacency-changes
 redistribute connected
 passive-interface default
 no passive-interface Tunnel2
 network ###.###.###.### 0.0.0.### area 2 (TUNNEL2)
 network ###.###.###.### 0.0.0.### area 2 (LAN)
```

DMVPN-verkko on mitä ilmeisimmin broadcast-verkko, koska mikään interface ei ole point-to-point-konfiguroitu, ja siksi broadcast konfiguroidaan OSPF-verkon tyypiksi. DMVPN-ominaisuuden käyttöönottavan asiakkaan verkko voi olla hyvin laaja, jopa maailmanlaajuinen, ja usein nimenomaan ulkomailla sijaitsevat liittymät halutaan suojata operaattorin yhteyksiä myöten. Maailmanlaajuisten yhteyksen välissä voi olla monta kolmannen osapuolen nonbroadcast-verkkoa, joten broadcast-tyyppisestä OSPF:stä huolimatta hello-viestin väliajaksi valitaan nonbroadcast-verkkojen mukainen 30 sekuntia [12]. Hubilla prioriteetiksi asetetaan korkein arvo 255, jolla varmistetaan, että siitä tulee OSPF-verkon nimetty reititin ja hallitsee reititystä. Spokeilta rivi jätetään pois, jolloin niiden prioriteettiarvona on oletusasetuksena 1.

OSPF-prosessi sidotaan samaan VRF:n kuin tunneli aiemmin. Oletusreitin mainostus konfiguroidaan ainoastaan hubille, kun taas naapuruussuhteiden muutokset tallennetaan logiin kaikilla. Komento **redistribute connected** mainostaa kaikki samassa VRF:ssä kiinni olevat interfacet OSPF-prosessissa. Jotta mainostus ei sotke muita interfaceja tai MPLS-yritysverkkoa, asetetaan kaikki interfacet lähtökohtaisesti passiivisiksi ja

sallitaan mainostus vain halutusta tunnel-interfacesta. Viimeisenä asetetaan halutut verkot mainostettavaksi DMVPN-verkkoon.

Osalla asiakkaista on kuitenkin BGP käytössä asiakastilojen CPE-laitteissakin. Nämä tapaukset ovat asiakkaan tahdosta lähtöisin ja nimetyn suunnittelijan hyväksymiä ratkaisuja. Esimerkiksi monen valtion kattavan yritysverkon reititys on usein päätetty hoitaa BGP:llä, jolloin reitit mainostuvat asiakas-VRF:ssä AS:stä toiseen eri operaattoreiden ja asiakkaan välillä. Näillä asiakkailla ei ole mielekästä ajaa OSPF-prosessia BGP:n rinnalla, vaan asiakkaan BGP-konfiguraatioon lisätään uusi VRF, jossa DMVPN-reititys kulkee.

```
router bgp <<AS-NUMERO>>
 bgp listen range ###.###.###.###/## peer-group SPOKE
 network <<LOOPBACK2>> mask 255.255.255.255

 address-family ipv4 vrf dmvpn
  network 0.0.0.0
  network <<LAN>>
  redistribute connected
  neighbor SPOKE peer-group
  neighbor SPOKE remote-as <<AS-NUMERO>>
  neighbor SPOKE send-community
 exit-address-family
```

BGP-konfiguraatio aloitetaan hubin osalta lisäämällä tunneli-interfacejen verkko kuuntelualueeksi, joka nimetään ymmärrettävästi spokeksi. Spokella kuuntelualuetta ei tarvitse määritellä. Kummallakin laitetyypillä loopback-interface asetetaan globaalin prosessin mainostukseen, koska tunneloitu VRF-sidottu liikenne kulkee globaalissa BGP-prosessissa.

Varsinainen DMVPN-mainostus asetetaan VRF:n address-familyyn. Hubilla mainostettavaksi asetetaan oletusreitti ja lähiverkko, kun taas spokeilla ainoastaan lähiverkko. VRF:ään sidotut interfacet mainostetaan komennolla **redistribute connected**, aivan kuten OSPF:ssä. Hubilla naapuriksi asetetaan aiemmin määritelty kuunteluryhmä, jolla oletettavasti on sama AS-numero kuin hubilla. Hub luo dynaamisesti naapuruuden määritellyn kuunteluverkon spokeihin rekisteröitymisen yhteydessä. Jos jokin DMVPN-verkon

spoke on eri AS:ssä, tulee se naapuruussuhde luoda erikseen samalla tavalla kuin naapuruus hubiin konfiguroidaan spokelle.

```
neighbor <<HUB-TUNNEL2>> remote-as <<AS-NUMERO>>
  neighbor <<HUB-TUNNEL2>> activate
  neighbor <<HUB-TUNNEL2>> send-community
```

Spokelle konfiguroidaan kiinteästi vain yksi reititysnaapuruus hubille ja naapuruuden aktivointi tehdään spoken toimesta, koska hub ei aloita kommunikointia tai naapuruussuhteen muodostamista. Kummallakin laitetyypillä lähetetään communitytiedot, koska BGP:tä käyttävillä asiakkailla on useimmiten erillisiä reittikarttoja käytössä. Komennosta ei ole haittaakaan, jos reittikarttoja ei ole, joten sen sisällyttäminen konfiguraatioon on perusteltua.

3.3 Konfiguraation testaus

Konfiguraatio testattiin TeliaSoneran laboratorioverkossa viiden Cisco 892F -reitittimen (ohjelmisto 154-3.M) ja simuloidun runkoverkon avulla. Testauksessa ei havaittu ongelmia konfiguraation toimivuudessa, mutta korostetaan silti, ettei laboratorioverkko kuvaa täysin kattavasti kaikkia tuotantoverkon rungon ominaisuuksia tai mahdollisia ongelmia, liittymäkohtaisista ongelmista puhumattakaan. Konfiguraatiota suositellaan pilotoitavaksi muutamalla mahdollisimman erilaisista lähtökohdista toimivalla asiakasverkolla ennen laajempaa käyttöä.

Konfiguraation toimivuutta voi tarkkailla kaikilla normaaleilla salaukseen liittyvillä show-komennoilla, kuten esimerkiksi **show crypto ipsec sa**, **show crypto ikev2 proposal** ja **show crypto ikev2 profile**. Itse DMVPN:n toiminnan varmistamiseksi löytyy useita komentoja, joista hyödyllisin lienee yksinkertainen komento **show ip nhrp**, joka tarkastaa laitteilta NHRP-reittitaulun.

```
show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel2 created 00:23:32, never expire
  Type: static, Flags: used
  NBMA address: 1.1.1.1
192.168.0.0/24 via 10.0.0.2, Tunnel2 created 00:43:12, expire 00:00:30
  Type: dynamic, Flags: router
 NBMA address: 2.2.2.2
```

Komento paljastaa paljon tietoa NHRP-prosessin toiminnasta laitteella, jopa tässä lyhyessä muodossaan (laajemman tuloksen saa komennolla **show ip nhrp detail**). Tämä show-komento on annettu todennäköisesti spokelle, sillä ylempi NHRP-kartoitus osoitteen 10.0.0.1 ja NBMA-osoitteen 1.1.1.1 välillä on staattinen eikä vanhene koskaan. Ainoa vanhenematon NHRP-reitti on manuaalisesti määritelty. Useimmat manuaaliset reittisidonnat ovat spokejen konfiguraatioissa kohdassa, jossa hubin tunneliosoite sidotaan sen NBMA-osoitteeseen. Rivi voi kuitenkin löytyä myös hubin konfiguraatiosta, jos verkossa käytetään kahta hubia. Tällöin kumpikin hub sitoo manuaalisesti toisen NHS:ksi. Merkintä used kertoo kyseistä reittiä käytettävän pakettien siirtoon.

Alempi reitti on puolestaan dynaamisesti muodostettu reilut 43 minuuttia aikaisemmin ja vanhenee 30 sekunnin kuluessa, jos viestejä ei laitteiden kesken vaihdeta sinä aikana. Merkintä router kertoo kohteen olevan joko reititin tai sen takana sijaitseva verkko.

Flag-merkinnät kertovat reitistä hyvin paljon. **Show ip nhrp** -komennon tulosteessa voi löytyä jokaiselta reitiltä yksi tai useampi seuraavista merkinnöistä [4]:

- Authoritative kertoo, että reitti on saatu NHS:ltä tai reitittimeltä, joka ylläpitää kyseistä NBMA-osoitteen ja IP-osoitteen sidontaa.
- Implicit-merkintä kertoo, että laite ei ole oppinut kyseistä reittiä omasta aloitteestaan eli oman selvityspyynnön kautta, vaan välittämällä kolmannen osapuolen NHRP resolution -pyyntöä.
- Negative. Lähettäessään NHRP resolution -pyynnön laite asettaa reitille negatiivisen merkinnän. Merkintä kertoo, että reitti ei ole vielä valmis. Tämä estää uusien selvityspyyntöjen lähettämisen tilanteessa, jossa edelliseen pyyntöön ei vielä ole vastattu.
- Unique. Tämä oletuksena oleva merkintä estää reitin ylikirjoittamisen toisella reitillä, missä on sama IP-osoite, mutta eri NBMA-osoite. Merkintä estää reittitaulun sekaantumisen tilanteessa, jossa toiselle laitteelle on vahingossa konfiguroitu sama IP-osoite. Jos jollain spokella on vaihtuva NBMA-

osoite, tulee merkintä poistaa kyseis.ellä laitteella käytöstä komennolla **ip nhrp registration no-unique**.

- Registered-merkintä löytyy vain NHS:ltä. Reitti on opittu NHC:n lähettämästä NHRP-rekisteröintipyynnöstä. Vaikka reittimerkintä onkin NHC:llä pysyvä, vanhenee se NHS:llä, jollei NHC lähetä uutta rekisteröintipyyntöä holdtime-ajan puitteissa.

- Used. Kun paketti lähetetään reittitaulun osoitteeseen, kyseinen osoite merkitään termillä used. Merkintä tarkastetaan aina 60 sekunnin välein ja jos tarkastettaessa reitin vanhenemisaika on yli 120 sekuntia, merkintä poistetaan. Jos vanhenemisaika on tarkastellessa puolestaan vähemmän kuin 120 sekuntia, reitti päivitetään lähettämällä uusi NHRP resolution –pyyntö.

- Router-merkinnällä vaustettu kiraus on reittitieto, joka on joko toinen reititin tai sen takana sijaitseva verkko.

- Local-merkintä kertoo kohdeverkko olevan paikallinen, laitteessa kiinni oleva verkko. Laite pitää kirjaa NHRP-verkon toisista laitteista, joille on lähettänyt tiedon paikallisesta verkosta vastaamalla NHRP resolution pyyntöön. Jos laite syystä tai toisesta menettää yhteyden paikalliseen verkkoon, lähettää se NHRP purge -puhdistusviestin kaikille laitteille, joille on verkkoa mainostanut.

- (No socket) on väliaikainen merkintä, joka ilmaisee tarpeettomuuden tunnelin muodostamiseen tälle kohteelle. Esimerkiksi local- ja implicit-merkinnät ovat aina aluksi (no socket) -merkittyjä.

- Nat-merkintä löytyy sellaisista reiteistä, joissa NHC on NHRP-rekisteröintipyynnössä ilmaissut tukevansa NHRP NAT -laajennusta. Merkintä ei siis tarkoita, että kohdeosoite olisi NAT:in takana

Tilastoista kiinnostunut verkon ylläpitäjä voi puolestaan seurata NHRP-viestien määrää helposti komennolla **show ip nhrp traffic**.

```
show ip nhrp traffic
Tunnel2
  request packets sent: 8
  request packets received: 16
  reply packets sent: 6
  reply packets received: 2
  register packets sent: 2
  register packets received: 0
  error packets sent: 0
  error packets received: 0
```

Varsinaisen verkon ylläpidon kannalta NHRP-protokollan normaalitoiminnan yleiset pakettimäärät eivät ole niinkään merkityksellisiä, mutta komento ei missään nimessä ole turha. Tulosteesta näkee helposti protokollan mahdolliset virhetilanteet ja niiden määrän, ja on siksi varsin hyödyllinen vianselvityksessä varsinkin alkuvaiheissa. Jos verkon toiminnasta haluaa komentoa **show ip nhrp traffic** tarkemman kokonaiskuvan myös vikatilanteissa, antaa **show ip nhrp traffic interface tunnelX** kattavamman vastauksen.

```
show ip nhrp traffic interface tunnel2
Tunnel2: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 94
27 Resolution Request 14 Resolution Reply 48 Registration Request
0 Registration Reply 2 Purge Request 4 Purge Reply
0 Error Indication 0 Traffic Indication
Rcvd: Total 72
17 Resolution Request 23 Resolution Reply 0 Registration Request
31 Registration Reply 6 Purge Request 2 Purge Reply
0 Error Indication 0 Traffic Indication
```

Tuloste-esimerkki tuo hyvin esiin komennon hyödyllisyyden. Vaikka yleiskomennolla **show ip nhrp traffic** pystyikin katsomaan nopeasti mahdolliset virhepaketit, ei se tuonut esiin purge-paketteja lainkaan. Purge-paketit kertovat laitteen hallinnoiman verkon yhteyden katkeamisesta laitteelle, ja siten auttaa kokonaiskuvan selvittämisessä. Verkon kadottaminen laitteelta, jonka sitä pitäisi hallinnoida on yleensä tapahtuma, josta tehdään monta vikailmoitusta. Jos vikailmoituksissa kerrotaan, että DMVPN-verkko ei toimi, suunnataan tutkimisresurssit luonnollisesti DMVPN-verkkoon. Tarkempi traffic-komento antamalla huomataan heti purge-viestit, jotka viittaavat enemmänkin laite- tai sisäverkkovikaan. Yhden komennon käyttämisellä voidaan säästää huomattavasti aikaa ja rahaa turhaa tutkimista vähentämällä.

4 Loppuajatukset

4.1 Huomioitavaa konfiguraatiossa

Konfiguraatiossa tulee huomioida muutama asia, joita geneeriseen pohjaan ei mielekkäästi voi sisällyttää. Ensimmäinen liittyy tunnelin toimimiseen käytetyn WAN-tekniikan oletuksena oleviin MTU-arvoihin, joissa lähtökohtaisesti ei odoteta asiakkaan käyttävän tunnelointia. GRE-tunnelointi lisää pakettien pituutta 24:llä tavulla. Jotta asiakasliikenteessä voidaan käyttää 1500 tavun paketteja, pitää MTU:ta kasvattaa sekä edgellä että CPE-reitittimellä. Esimerkiksi ethernet-tekniikalla toteutetulla liittymällä kummallakin laitteella fyysisen interfacen MTU-arvoksi tulee määritellä 1548 tavua ja loogisen ali-interfacen **ip mtu** -arvoksi 1524 tavua.

Toisena huomioitavana asiana asiakkaan lähiverkkointerfacet tulee halutussa määrin liittää osaksi DMVPN-VRF:ää. Osalla asiakkaista on CPE-reitittimen takana oma kytkin, ja lähiverkkointerfacet ovat joko fyysisiä interfaceja tai loogisia subinterfaceja. Suurin osa asiakkaista käyttää kuitenkin erinäisiä vlan-interfaceja, jolloin fyysiset portit asetetaan vain trunkeiksi lähiverkon suuntaan. Tästä vaihtoehtojen kirjosta johtuen konfiguraatiopohjan käyttäjän tulee tarkastaa CPE-laitteen konfiguraatio sekä asiakkaan toiveet, ja vasta sen jälkeen tehdä päätös VRF:ään liitettävistä LAN-interfaceista. Useamman liitetyn lähiverkon tapauksessa tilanne tulee huomioida myös reitityksessä määrittelemällä uusia mainostusrivejä tarpeen mukaan.

Kolmantena huomioitavana seikkana CPE-laitetta konfiguroivan henkilön tulee tarkastaa, ettei asiakaskohtaisissa konfiguraatioissa ole päällekkäisyyttä tunneli- tai loopback-interfacen numeroinnin eikä myöskään VRF:n rd-arvon osalta. Tämä on erityisen tärkeää toteutettaessa palvelua olemassaolevaan liittymään, koska tällöin voidaan tehdä suurta vahinkoa käytössä oleville yhteyksille. Ciscon IOS toteuttaa komennot heti, joten Juniperin tyylistä tarkastelumahdollisuutta ei vahinkojen välttämiseksi ole. Samalla konfiguroivan henkilön kannattaa tarkastaa, onko jotain konfiguraation kohtia laitteella valmiiksi jostain toisesta lisäpalvelusta johtuen. Laitteelta voi esimerkiksi löytyä varmenne jo ennestään.

Viimeisenä tulee huomioida, että konfiguraatio itsessään on täysin skaalautuva niin laitemäärän kuin VRF:ien osalta. Ainoina rajoituksina ovat laitteiden oma tuki ja suorituskyky VRF-määrien suhteen sekä resurssit IP-suunnittelun ja yritysasiakastoimituksen osalta. Osa tuotantoverkossa olevasta Ciscon laitekannasta ei tue multi-VRF-ratkaisua lainkaan. Näitä laitteita ovat esim. Cisco 827, 828, 837 ja 1720. Cisco 3750ME:n suorituskyky ei puolestaan ole tarpeeksi hyvä GRE tunnelointia varten.

4.2 Vaikutukset toimitusprosessiin

Toimitusprosessissa DMVPN olisi mitä todennäkoisimmin tuotteistettu maksulliseksi lisäpalveluksi. Tuotteistusvaiheessa tulee päättää, saako asiakas vaikuttaa asiakaskohtaisiin NHRP-parametreihin, kuten esimerkiksi network-id:hen, vai päättääkö nämä asiat TeliaSoneran IP-suunnittelija. Kuka taho päätöksen tekeekään, niin kyseisten arvojen tulisi pysyä yhtenäisenä läpi verkon uusia liittymiä konfiguroitaessa. Palvelu vaatinee joka tapauksessa IP-suunnittelijaa, joka tutkii asiakasverkon, tekee päätöksen tarvittavista julkisista tai privaateista IP-osoitteista ja päivittää asiakkaan verkkodokumentin ajantasaiseksi. Verkkodokumentista tulee yhteyksien testaamisen ja konfiguroinnin helpottamiseksi löytyä tieto asiakkaan liittymistä, joilla DMVPN-lisäpalvelu on, sekä seuraavat tiedot:

- DMVPN-tunneleiden osoitteet liittymittäin.
- NBMA-osoitteet liittymittäin.
- NBMA-osoitteen interface (loopback vai WAN?)
- Interfacejen numerointi tulee olla selvillä. Tällä tavalla pyritään varmistamaan etukäteen, ettei asiakkaalla ole jo liittymällä vastaavasti numeroituja interfaceja.
- Hubin tunneliosoite ja NBMA IP-osoite tulee olla tiedossa. Muussa tapauksessa spokejen konfiguroiminen tulee kestämään pidempään verkonhallinnan selvittäessä hubin tietoja.
- NHRP authentication -salasana.
- NHRP network-id.
- Tunnel key.

- Tunnelin nopeus tulee ilmoittaa, ellei asiakas halua dynaamista kaistanjakoa WAN-linkille.
- Reititystapa tulee olla tiedossa. Jos tapaa ei ilmoiteta, tehdään oletuksena OSPF:llä.
- AS-numero, jos asiakkaalla on käytössä BGP-reititys.

Palvelusta tulee luonnollisesti tehdä palvelukuvaus sekä hinnoittelupäätös ja kouluttaa ne myyjille, jotta he osaisivat kuvailla palvelun hyödyt asiakkaille ja onnistuvat myymään palvelua. Palvelun toiminta ja rajoitteet on hyvä myöskin kouluttaa myyjille ja erityisesti toimitusprosessia koordinoiville toimitusvastaaville asiakaskokemuksen laadun säilyttämisen vuoksi. Esimerkiksi palvelun rajoittuminen Ciscon laitteille ja niilläkin vain tietyille malleille tulee olla tiedossa. Myöskin asiakkaan liittymän olemassaolevat ja muut tilatut palvelut pitää ottaa huomioon mm. VRF-määrien rajoitteiden ja johtopituuden asettaman fyysisen nopeusrajoitteen vuoksi.

Vaikka rajoitteet ilmaistaisiin palvelukuvauksessa, jonka asiakas vahvistaa lukeneensa sopimuksen allekirjoituksen yhteydessä, kärsii asiakaskokemus huomattavasti, jos tilaus viivästyy ja asiakkaan toimipisteen yhteyksissä on katko konfigurointivaiheessa esimerkiksi väärän laitetyypin aiheuttaman laitevaihdon vuoksi. Heti alun myyntivaiheessa tai toimitusvastaavan käsittelyssä havaitusta laitevaihdon tarpeesta ja suunnitellusti toteutetusta laitevaihdosta jää puolestaan paljon positiivisempi asiakaskokemus, vaikka koko prosessissa kestäisi yhteensä yhtä kauan kuin viime hetkellä konfigurointivaiheessa havaitussa laitevaihdossa. Asiakkaan suhtautuminen on aina positiivisempi ja toiminnasta jää parempi kuva, jos viivästykset ovat etukäteen tiedossa.

Prosessissa tulee myös huomioida varmenteiden myöntämiseen liittyvät oikeudet, joita kaikilla työntekijöillä, esimerkiksi kesätyöntekijöillä, ei ole. Ongelma voidaan osittain kiertää sillä, että oikeudeton työntekijä konfiguroi CPE-laitteen hakemaan varmennetta ja toinen, oikeudet omaava työntekijä myöntää varmenteen palvelimelta. Järjestely vaatii toki yhteisymmärryksen toimintatavasta ja hiukan koordinointia työntekijöiden välillä, mutta on silti toteutettavissa. Joka tapauksessa kyse on erikoiskonfiguroitavasta lisäpalvelusta, joiden asentaminen ei useimmiten ole yhtä kiireellistä kuin pääyhteyksien, joten viivästys prosessissa myöntämisoikeuksien vuoksi lienee hyväksyttävissä.

Konfiguraatio tulee myöskin dokumentoida Soneran verkonhallinnan wikisivuille, jotta palvelu voidaan toteuttaa yhtenäisesti läpi asiakaskunnan eri verkonhallintatiimeissä. Tuotantoverkossa olevan konfiguraation yhdenmukaisuus on erittäin tärkeää, koska monella eri tavalla toteutettuun verkkoon ei esimerkiksi saa toimivia skriptejä, joilla muutoksia voidaan toteuttaa massa-ajona. Eri tavalla toteutetut konfiguraatiot aiheuttavat myös lisätyötä viankorjauksen ja -selvityksen muodossa, kun jonkin alkuperäisen konfiguroinnin ja muutoksen tehneen henkilön konfiguroinnin eroavaisuuden takia toisen työntekijän tekemä muutos esimerkiksi kaataakin koko tunnelin.

Lähteet

1 Cisco IOS DMVPN Overview. 2008. Verkkodokumentti. <http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multi-point-vpn-dmvpn/DMVPN_Overview.pdf>. Luettu 11.4.2016.

2 Luciani, Katz, Piscitello, Cole, Doraswamy. 1998. NBMA Next Hop Resolution Protocol (NHRP). Verkkodokumentti. <https://tools.ietf.org/html/rfc2332>. Luettu 11.4.2016.

3 Petr Lapukhov. 2008. DMVPN Explained. Verkkodokumentti. <http://blog.ine.com/2008/08/02/dmvpn-explained/>. Luettu 11.4.2016.

4 NHRP. 2005. Verkkodokumentti. <http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html>. Luettu 16.4.2016.

5 Petr Lapukhov. 2008. DMVPN Phase 3. Verkkodokumentti. <http://blog.ine.com/2008/12/23/dmvpn-phase-3/>. Luettu 16.4.2016.

6 McGrew, Hoffman. 2014. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH). Verkkodokumentti. <https://tools.ietf.org/html/rfc7321#section-3>. Luettu 16.4.2016.

7 Latosiewicz. 2013. FlexVPN Migration: Hard Move from DMVPN to FlexVPN on Same Devices. Verkkodokumentti. <http://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/115726-flexvpn-hardmove-same-00.html>. Luettu 16.4.2016.

8 Kaufman. 2005. Internet Key Exchange (IKEv2) Protocol. Verkkodokumentti. <https://tools.ietf.org/html/rfc4306#page-96>. Luettu 16.4.2016.

9 Configuring Internet Key Exchange Version 2 (IKEv2). 2011. Verkkodokumentti. <http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-1mt/Configuring_Internet_Key_Exchange_Version_2.html>. Luettu 17.4.2016.

10 Chapter: IPsec Anti-Replay Window Expanding and Disabling. 2012. Verkkodokumentti. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/15-mt/sec-ipsec-data-plane-15-mt-book/sec-ipsec-antireplay.html>. Luettu 17.4.2016.

11 Cisco IOS IP Addressing Services Command Reference. 2014. Verkkodokumentti. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book/ipaddr-i4.html#wp7868593100>. Luettu 18.4.2016.

12 Chapter: OSPF commands. 2007. Verkkodokumentti. <http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfospf.html#wp1018239>. Luettu 18.4.2016.

Hub-konfiguraatio

```
ip vrf dmvpn
rd 4:5

crypto key generate rsa label ###<<LAITENIMI>>.##########.fi modulus
####

ip tcp synwait-time 5

ip host ##########.com xxx.xxx.xxx.xxx
ip host ##########com xxx.xxx.xxx.xxx
ip host ##########.com xxx.xxx.xxx.xxx

crypto pki certificate map OU 10
 subject-name = ##########

crypto pki trustpoint ##########.fi
 enrollment retry count 100
 enrollment retry period 10
 enrollment mode ra
 enrollment url ##########
 serial-number
 fqdn <<LAITENIMI>>.##########
 ip-address <<WAN-OSOITE>>
 password ##########
 fingerprint ##########
 subject-name ##########
 revocation-check crl none
 rsakeypair ###_<<LAITENIMI>>.##########.fi
 match certificate OU
 auto-enroll 99

crypto pki authenticate ##########.fi
crypto pki enroll ##########.fi

crypto ikev2 proposal DMVPN_PROP
 encryption aes-cbc-256
```

```
 integrity sha256
 group 14

crypto ikev2 policy DMVPN_POL
 match fvrf any
 proposal DMVPN_PROP

crypto ikev2 profile DMVPN_PROF
 match certificate OU
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint ##########.fi
 dpd 10 2 periodic

crypto logging session
crypto ikev2 disconnect-revoked-peers
crypto ipsec security-association replay window-size 512

crypto ipsec transform-set DMVPN_TS esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec df-bit clear

crypto ipsec profile DMVPN
 set transform-set DMVPN_TS
 set ikev2-profile DMVPN_PROF
 responder-only

interface Loopback2
 description Tunnel source
 ip address ###.###.###.### 255.255.255.255


interface Tunnel2
 ip vrf forwarding dmvpn
 description DMVPN-tunneli, <<LIITTYMÄTUNNUS>>
 ip address ###.###.###.### 255.255.255.###
 bandwidth <<TILATTU NOPEUS>>
 ip mtu 1500
```

```
 ip tcp adjust-mss 1460
 no ip redirects
 ip nhrp authentication <<SALASANA>>
 ip nhrp map multicast dynamic
 ip nhrp network-id ##########
 ip nhrp holdtime 360
 ip nhrp redirect
 ip nhrp shortcut
 load-interval 30
 qos pre-classify
 tunnel source Loopback2
 tunnel mode gre multipoint
 tunnel key ##########
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN shared


####REITITYS

####Tunnel-interface(i)lle:
ip ospf network broadcast
ip ospf hello-interval 30
ip ospf priority 255

router ospf 150 vrf dmvpn
 default-information originate
 log-adjacency-changes
 redistribute connected
 passive-interface default
 no passive-interface Tunnel2
 network ###.###.###.### 0.0.0.### area 2 (TUNNEL2)
 network ###.###.###.### 0.0.0.### area 2 (LAN)

###BGP-KONFIGURAATIO, JOS ASIAKKAALLA BGP-REITITYS KÄYTÖSSÄ

router bgp <<AS-NUMERO>>
 bgp listen range ###.###.###.###/## peer-group SPOKE
 network <<LOOPBACK2>> mask 255.255.255.255
```

```
address-family ipv4 vrf dmvpn
 network 0.0.0.0
 network <<LAN>>
 redistribute connected
 neighbor SPOKE peer-group
 neighbor SPOKE remote-as <<AS-NUMERO>>
 neighbor SPOKE send-community
exit-address-family
```

Spoke-konfiguraatio

```
ip vrf dmvpn
rd 4:5

crypto key generate rsa label ###<<LAITENIMI>>.##########.fi modulus
####

ip tcp synwait-time 5

ip host ##########.com xxx.xxx.xxx.xxx
ip host ##########.com xxx.xxx.xxx.xxx
ip host ##########.com xxx.xxx.xxx.xxx

crypto pki certificate map OU 10
 subject-name = ##########

crypto pki trustpoint ##########.fi
 enrollment retry count 100
 enrollment retry period 10
 enrollment mode ra
 enrollment url ##########
 serial-number
 fqdn <<LAITENIMI>>.##########.fi
 ip-address <<WAN-OSOITE>>
 password ##########
 fingerprint ##########
 subject-name ##########
 revocation-check crl none
 rsakeypair ###<<LAITENIMI>>.##########.fi
 match certificate OU
 auto-enroll 99

crypto pki authenticate ##########.fi
crypto pki enroll ##########.fi

crypto ikev2 proposal DMVPN_PROP
 encryption aes-cbc-256
```

```
 integrity sha256
 group 14

crypto ikev2 policy DMVPN_POL
 match fvrf any
 proposal DMVPN_PROP

crypto ikev2 profile DMVPN_PROF
 match certificate OU
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint ##########.fi
 dpd 10 2 periodic

crypto logging session
crypto ikev2 disconnect-revoked-peers
crypto ipsec security-association replay window-size 512

crypto ipsec transform-set DMVPN_TS esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec df-bit clear

crypto ipsec profile DMVPN
 set transform-set DMVPN_TS
 set ikev2-profile DMVPN_PROF

interface Loopback2
 description DMVPN Tunnel source
 ip address ###.###.###.### 255.255.255.255

interface Tunnel2
 ip vrf forwarding dmvpn
 description DMVPN-tunneli, <<LIITTYMÄTUNNUS>>
 ip address ###.###.###.### 255.255.255.###
 bandwidth <<TILATTU NOPEUS>>
 ip mtu 1500
 ip tcp adjust-mss 1460
 no ip redirects
```

```
 ip nhrp authentication <<SALASANA>>
 ip nhrp map <<HUB-TUNNEL2>> <<HUB-LOOP2>>
 ip nhrp map multicast dynamic
 ip nhrp network-id ##########
 ip nhrp holdtime 360
 ip nhrp nhs <<HUB-TUNNEL2>>
 ip nhrp redirect
 ip nhrp shortcut
 load-interval 30
 qos pre-classify
 tunnel source Loopback2
 tunnel mode gre multipoint
 tunnel key ##########
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN shared

####REITITYS

####Tunnel-interface(i)lle:
ip ospf network broadcast
ip ospf hello-interval 30

router ospf 150 vrf dmvpn
 log-adjacency-changes
 redistribute connected
 passive-interface default
 no passive-interface Tunnel2
 network ###.###.###.### 0.0.0.### area 2 (TUNNEL2)
 network ###.###.###.### 0.0.0.### area 2 (LAN)

###BGP-KONFIGURAATIO, JOS ASIAKKAALLA BGP-REITITYS KÄYTÖSSÄ

router bgp <<AS-NUMERO>>
 network <<LOOPBACK2>> mask 255.255.255.255

 address-family ipv4 vrf dmvpn
  network <<LAN>>
  redistribute connected
  neighbor <<HUB-TUNNEL2>> remote-as <<AS-NUMERO>>
```

```
 neighbor <<HUB-TUNNEL2>> activate
 neighbor <<HUB-TUNNEL2>> send-community
exit-address-family
```