Tuukka Järvi

Hierarkkisen QoS:n implementointi yrityksen MPLS VPN -ympäristöön

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

28.5.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Tuukka Järvi Hierarkkisen QoS:n implementointi yrityksen MPLS VPN -ympäristöön 52 sivua + 4 liitettä 28.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	päällikkö, asiakaspalvelu ja ylläpito, Markus Säkäjärvi lehtori Marko Uusitalo

Tässä työssä rakennettiin QoS-ratkaisu asiakasyrityksen tietoverkkoon. Verkon käyttäjät käyttävät hyvin viivekriittisiä keskitettyjä tietojärjestelmiä sekä IP-puhelinjärjestelmää ja IP-puhelimia. Työn tärkein tavoite oli tuottaa ratkaisu, jonka avulla voidaan poistaa sekä puheluiden laadussa että kriittisiä järjestelmiä käytettäessä ilmenneet ongelmat, sillä ne ovat tulleet merkittävästi esiin mitattaessa asiakkaan käyttäjien tyytyväisyyttä yrityksen tarjoamiin palveluihin.

Työn alussa kuvataan taustalla oleva teoria, verkko- ja TCP/IP-teknologiat. Seuraavaksi käydään yksityiskohtaisesti läpi MPLS-verkkojen rakenne ja toiminta sekä QoS-ratkaisut. Käytännön osuus muodostuu verkon aktiivilaitteiden konfiguroinnista ja toiminnan testaamisesta.

Tuloksena saatiin toimiva tietoverkko, jonka välityskyky riittää mainiosti asiakkaan nykytarpeisiin ja jota voidaan helposti laajentaa tarpeiden kasvaessa.

Avainsanat	IP, MPLS, VPN, QoS, DiffServ

Author(s) Title Number of Pages Date	Tuukka Järvi Implementing hierarchical QoS to company's MPLS VPN network 52 pages + 4 appendices 28 May 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Markus Säkäjärvi, Manager, Customer service and operations Marko Uusitalo, Senior Lecturer

In this study we will implement a QoS solution to customer's network. The applications used in the network are time-critical, e.g. VoIP and real-time data transfer.

The aim was to create a solution with which the problems in the current network are solved and the customer satisfaction is increased.

In the beginning of the thesis the theoretical background, the TCP/IP protocol family, MPLS VPN networks and Quality of Service methods are gone through. The practical part of the study consist of configuring the network active devices ie. Cisco routers and layer 3 switches. After the configuration traffic in company network was monitored and analyzed.

As a result a fully functional network was aquired with a capacity that easily covers the customer's current needs and can be easily extended if the requirements increased.

Keywords	IP, MPLS, VPN, QoS, DiffServ

Sisällys

Lyhenteet

ARPA	Advanced Research Projects Agency; Yhdysvaltalainen tutkimuskeskus.
ARPANET	Advanced Research Projects Agency Network; ARPA:n rakentama ensimmäinen pakettikytkentäinen verkko.
AS	Autonomous System, Autonominen järjestelmä, reititysalue; TCP/IP-reititysprotokollissa käytettävän yksittäisen toimijan (esimerkiksi verkko-operaattorin) verkkokokonaisuus.
BGP	Border Gateway Protocol; reititysprotokolla, jota käytetään reitittämiseen autonomisten järjestelmien välillä.
bps	Bittiä sekunnissa, b/s; siirtonopeuden mitta. Kerrannaisyksiköt kbps (1000 bittiä sekunnissa), Mbps (miljoona bittiä sekunnissa) ja Gbps (miljardi bittiä sekunnissa).
Broadcast	Yleislähetys; levitysviesti, joka lähetetään kaikille tai osalle verkon solmuista.
CoS	Class of Service; Ethernet-kehyksessä oleva kolmen bitin ohjauskenttä.
CRC	Cyclic Redundancy Checking, CRC-varmistus; syklinen ylimäärävarmistus.
DARPA	Defense Advanced Research Projects Agency; Yhdysvaltain asevoimien tutkimusorganisaatio.
DSCP	Differentiated Services Code Point; IPv4-otsakkeessa sijaitseva 6-bittinen luokittelukenttä.
DiffServ	Differentiated Services; IETF:n määrittelemä palvelunlaatumekanismi liikenteen hallintaan.
Egress	Lähtö; egress router on leimakytkentäisen verkon laidalla sijaitseva lähtöreititin, joka voi olla toisen verkon tuloreititin, ingress router.
Ethernet	Lähiverkkotekniikka.
FEC	Forwarding Equivalence Class, välitysekvivalenssiluokka; joukko IP-paketteja, kuljetetaan samoilla tiedoilla.
FIFO	First In First Out; jonotussysteemi.
IANA	Internet Assigned Numbers Authority; valvoo maailmanlaajuisesti IP-osoitteiden jakoa.
IBGP	Internal BGP; autonomisen alueen sisäinen BGP-reititys.
ICMP	Internet Control Message Protocol; TCP/IP-hallintaprotokolla.
IEEE	Institute of Electrical and Electronics Engineers; kansainvälinen tekniikan alan järjestö.

IETF	Internet Engineering Task Force; kansainvälinen internetteknologioiden standardoinnista vastaava organisaatio.
IGP	Interior Gateway Protocol; reititysprotokolla, toimii itsenäisen alueen sisällä.
Ingress	Sisääntulo; ingress router on leimakytkentäisen verkon laidalla sijaitseva tuloreititin.
IntServ	Integrated Services; Arkkitehtuuri, joka määrittelee QoS-elementtejä verkossa.
IOS	Internetwork Operating System; Ciscon käyttöjärjestelmä.
IP	Internet Protocol; tietoliikenneprotokolla.
IPSec	Internet Protocol Security; joukko IP-protokollan laajennuksia, joilla lisätään IP-liikenteen turvallisuutta.
IPv4	Internet Protocol version 4; Internet-protokolla versio 4.
IPv6	Internet Protocol version 6; Internet-protokolla versio 6.
IS-IS	Intermediate System-to-Intermediate System; linkkitila-reititysprotokolla.
ISO	International Organization for Standardization; Kansainvälinen standardointijärjestö.
ISP	Internet Service Provider; internet-palveluntarjoaja.
Jitter	Värinä; tietoliikenteen jaksollisessa signaalissa yhden tai useamman ominaispiirteen ei-toivottu poikkeama.
Koodekki	Codec; muuttaa analogisen signaalin digitaaliseksi ja takaisin digitaalisesta analogiseksi.
Kytkin	Switch; laite, joka yhdistää pakettikytkentäisen lähiverkon osia, segmenttejä. Toimii OSI-mallin siirtoyhteyskerroksella.
Label	Lippu, leima.
Latency	Viive; paketilta matkaan lähettäjältä vastaanottajalle ja takaisin kuluva aika.
LAN	Local Area Network; lähiverkko.
Layer	OSI-mallin kerros, esimerkiksi siirtoyhteyskerros Layer 2, L2, sekä verkkokerros Layer 3, L3.
LDP	Label Distribution Protocol; protokolla lipputietojen vaihtoon MPLS-verkossa.
LER	Label Edge Router; MPLS-verkon reunalaite, joka välittää leimatonta liikennettä leimakytkettyyn verkkoon.
LIB	Label Information Base; MPLS-verkon laitteiden ylläpitämämä tietokanta lippumerkinnöistä.

LSP	Label Switched Path; polku, jota pitkin paketit kulkevat MPLS-verkossa.
LSR	Label Switch Router; MPLS-verkon runkolaite, joka käsittelee lippuja ja leimakytkettyä liikennettä.
MAC	Media Access Control; Ethernet-verkon laitteita yksilöivä Layer 2 -tason osoite.
MPLS	Multiprotocol Label Switching; leimakytkentä, lippumerkintöihin perustuva IETF:n standardoima pakettien kytkentätekniikka.
MP-BGP	Multiprotocol BGP; reititysprotokolla, BGP:n moniprotokollalaajennus.
MTU	Maxium Transmission Unit; suurin paketti, joka voidaan välittää eteenpäin kokonaisena.
NLRI	Network Layer Reachability Information; BGP:n käyttämä informaatio.
Oktetti	Kahdeksan bitin mittainen tiedonsiirtoyksikkö, vrt. tavu.
OSPF	Open Shortest Path First; Linkkitila-reititysprotokolla.
OSI-malli	Open Systems Interconnection Reference Model; tietoliikenteen viitemalli.
P	Provider; MPLS-palveluntarjoajan runkolaite.
Paketti	Packet, IP-paketti, IP-datagrammi; internet-liikennöinnin perussiirtoyksikkö.
P-laite	Provider Router; reititin, joka välittää liikennettä MPLS-verkossa.
PE-laite	Provider Edge; operaattoriverkon reunalaite, johon VPN-asiakkaat kytkeytyvät.
QoS	Quality of Service; palvelun laatu.
RD	Route Distinguisher, reittierotin; 64 bitin VPN-kohtainen IPv4-osoitteeseen liitettävä reittitunniste.
Reititin	Router; laite, joka ohjaa tietoverkossa kulkevat datapaketit oikeisiin verkkosegmentteihin paketeissa olevien osoitetietojen perusteella. Toimii OSI-mallin verkkokerroksella.
RID	Router-ID; reitittimen tunnus, tavallisesti suurin loopback-osoite.
RIR	Regional Internet Registry; valvoo IP-osoitteiden rekisteröintiä alueellisesti.
RSVP	Resource Reservation Protocol; Kuljetuskerroksen protokolla, jolla varataan verkkoresursseja priorisoidulle verkkoliikenteelle Integrated Services -arkkitehtuurissa.
RT	Route Target; väline reittien määritykseen VPN-yhteyksissä.
RTCP	Real-Time Transport Control Protocol; RTP-protokollan tukiprotokolla.
RTP	Real-Time Transport Protocol; UDP:n päällä toimiva reaaliaikaisen äänen kuljettamiseen tarkoitettu protokolla.

Shaping	Shape-tilassa jokaiselle jonolle annetaan prosentuaalinen osuus taattua kaistaa.
SIP	Session Initiation Protocol; VoIP:n ydinprotokolla.
Streaming	Striimaus, suoratoisto; tiedonsiirtotapa, jossa multimediatiedoston sisältöä aletaan esittää käyttäjälle heti kun tiedonsiirto on päässyt käyntiin.
Tavu	Byte, B; 8 bitin mittainen tiedonsiirtoyksikkö. Kerrannaisyksiköt kilotavu (kT, kB), megatavu (MT, MB) ja gigatavu (GT, GB).
TCP	Transmission Control Protocol; luotettava kuljetuskerroksen tiedonsiirtoprotokolla.
TTL	Time To Live; hyppyjen maksimimäärä siirtotiellä.
ToS	Type of Service; 8-bittinen ohjauskenttä IPv4-otsakkeessa.
UDP	User Datagram Protocol; yhteydetön kuljetuskerroksen tiedonsiirtoprotokolla.
VoIP	Voice over Internet Protocol; tekniikka, jonka avulla puhetta siirretään IP-verkoissa.
VPN	Virtual Private Network; näennäisverkko, jolla yhdistetään kaksi tai useampia verkkoja julkisen verkon yli.
VPN-IPv4	IP-osoitteen ja RD:n kombinaatio.
VRF	VPN Routing and Forwarding table; virtuaaliverkkokohtainen reititys- ja kytkentätaulu.
VRI	VPN forwarding instance; virtuaaliverkkokohtainen reititys- ja kytkentätoiminne PE-reitittimessä.

.

1 Johdanto

Tietoverkkojen ja internetin käyttö on muuttunut uusien palveluiden ja sovellusten käyttöönoton myötä täydellisesti. Uudet toiminnot, kuten videopuhelut ja Internet-protokollan päällä ajettu puhe (VoIP), nostavat verkon vaatimukset uudelle tasolle. Monilla uusilla ominaisuuksilla on aivan eri vaatimukset verkolle kuin mihin se alun perin rakennettiin. Alkuperäinen yhteydetön malli ei tarjoa resurssienhallintatyökaluja, jotka varmentaisivat pakettien esteettömän läpimenon.

Internet-puhelua tehdessä tai verkon resursseja käytettäessä voi tulla vastaan tilanne, että osa verkosta voi olla ruuhkautunut, jolloin datapaketit eivät yksinkertaisesti pääse kohteeseensa. Lähes kaikki reaaliaikaiset sovellukset, kuten videopuhelut vaativat myös tietyn vähimmäistason resursseja toimiakseen tehokkaasti.

Eri liikennetyypeillä on hyvin erilaisia vaatimuksia verkolle tietoturvan, tiedon eheyden. viiveen, viiveen vaihtelun ja kaistanvarauksen suhteen. Esimerkiksi ääni- ja videoliikenne eivät siedä pakettien häviämistä (packet loss) ja vaativat taatun kaistanleveyden ja alhaisen viiveen (latency) sekä vähäisen vaihtelun viiveessä (jitter) toimiakseen tyydyttävästi. Tiedonsiirtoliikenne puolestaan kuluttaa oletusarvoisesti linkin kaiken vapaan, käytettävissä olevan kapasiteetin. Tyydyttääkseen käyttäjiä puhelinliikenne ja keskitetyt palvelut tarvitsevat alhaisen viiveen ja vaihtelun lisäksi korkean tason luotettavuutta ja saatavuutta.

IP-liikenne kulkee tietoverkoissa reitittimien (router) kautta. Reititin selvittää IP-paketin otsakkeen osoitekenttien avulla, mihin paketti on menossa, ja reitittää sen sitten seuraavalle reitittimelle kohti kohdetta. Reititys tapahtuu reitittimessä sijaitsevan reititystaulun (routing table) avulla, joka kertoo seuraavan hypyn (hop), eli portin ja osoitteen, mihin paketti ohjataan. Reititin vertaa jokaisen välitettävän paketin kohdeosoitetta reititystaulun riveihin, kunnes oikea reitti löytyy. Reititys hidastaa liikennettä varsinkin suurissa verkoissa, joissa reititystaulut ovat suuria.

MPLS-tekniikan (Multiprotocol Label Switching, leimakytkentätekniikka) avulla voidaan toteuttaa monipalveluverkkoja, joissa virtuaaliverkot toimivat yhden hallinnollisen verkon (autonominen alue) sisällä. Siinä paketit kytketään eteenpäin IP-osoitteiden asemasta MPLS-lipuilla. MPLS mahdollistaa näin liikenteen nopean välittämisen

verkon läpi ilman, että paketit olisi reititettävä erikseen jokaisella hypyllä. Keskeinen MPLS-verkkojen ominaisuus on tunnelointi, jota käytettäessä vain verkon reunalaitteet käsittelevät liikennettä sen natiivimuodossa, ja verkon muut laitteet välittävät liikenteen puuttumatta sen rakenteeseen.

Tämä työ on tehty yritykselle, jonka käyttäjät käyttävät hyvin viivekriittisiä keskitettyjä tietojärjestelmiä sekä IP-puhelinjärjestelmää ja IP-puhelimia. Työn tärkein tavoite oli tuottaa ratkaisu, jonka avulla voidaan poistaa sekä puheluiden laadussa, että kriittisiä järjestelmiä käytettäessä ilmenneet ongelmat, sillä ne ovat tulleet merkittävästi esiin mitattaessa asiakkaan käyttäjien tyytyväisyyttä yrityksen tarjoamiin palveluihin.

Tällaisessa ympäristössä pelkkä kaistanleveyden kasvattaminen voi olla hyvin kallis ratkaisu, eikä se välttämättä edes yksinään riittäisi verkon toiminnan saattamiseksi tyydyttävälle tasolle. Eri liikennetyypeillä on siis eri vaatimukset verkolle. Verkon toimintaa voidaan tehostaa liikenteen jonotusjärjestelyin, joiden painopiste tässä työssä liittyy dataliikenteen priorisointiin hierarkkisesti määrätyin ehdoin.

Työssä keskityttiin tietoliikenteen sujuvuuden ja sovellusten toimivuuden kehittämiseen tietoliikennepriorisoinnin avulla. Termillä Quality of Service (QoS) tarkoitetaan tietoliikenteen luokittelua ja priorisointia. Priorisoinnin perusteella osaa liikenteestä voidaan hidastaa tai jopa pudottaa kokonaan pois, mikäli linjojen välityskyky ei riitä. Liikennettä voidaan priorisoida esimerkiksi sovellusten, käyttäjien tai käytettyjen tietokoneiden perusteella.

Vaikka työn pääpaino oli QoS-ratkaisuissa, teoriaosuudessä käydään läpi myös MPLS-tekniikkaa varsin yksityiskohtaisesti, koska kohdeverkot oli toteutettu MPLS-tekniikoilla.

Luvussa 2 esitetään työssä käytetty teoria, lähtötilanne ja työn rajaus. Luvussa 3 kuvataan MPLS-tekniikkaa ja luvussa 4 esitetään QoS-käytännöt. Luvussa 5 käydään läpi asiakasyrityksen verkkotopologia sekä tutustutaan käytännön toteutukseen näyttämällä verkon laitteisiin tehdyt konfiguraatiot vaihe vaiheelta. Työssä keskitytään kokonaan Layer 3 -tason IPv4-pohjaisiin VPN-ratkaisuihin. Luku 6 sisältää käytännön testauksen ja järjestelmän suorituskyvyn tarkastelun.

2 Internet-tekniikat

Tässä luvussa käydään lyhyesti läpi työssä tarvittu Internet-protokolliin liittyvä teoria. Tietoliikenneprotokollia voidaan tarkastella International Organization for Standardisation (ISO) -järjestön kehittämällä tietoliikenteen viitemallilla (Open Systems Interconnection Reference Model, OSI-malli). OSI-mallissa tietoliikenne ja -sovellukset jaetaan seitsemälle kerrokselle (layer). Malli on hierarkkinen. Alimpana on fyysinen kerros, joka määrittelee kaapeloinnin, liittimet ja signaalit ja ylimpänä sovelluskerros. Hierarkia kasvaa alhaalta ylöspäin. Kuvassa 1 on esitetty OSI-malli. Siirtoyhteyskerros sisältää mm. lähiverkon palvelut ml. Ethernet-protokollan. Internet-protokollat sijaitsevat verkkokerroksella. Kuljetuskerroksella ovat TCP- ja UDP-protokollat. Ylimpiä kolmea kerrosta kutsutaan yhdessä sovelluspalveluiksi. [1.]

Sovelluskerros
Esitystapakerros
Istuntokerros
Kuljetuskerros
Verkkokerros
Siirtoyhteyskerros
Fyysinen kerros

Kuva 1. OSI-malli. [1.]

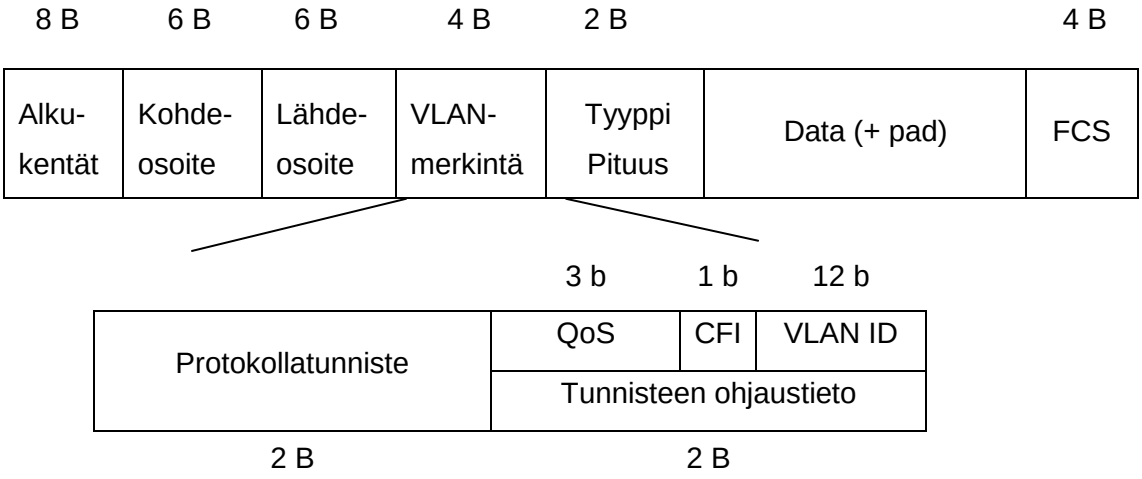
Toinen yleisesti käytetty viitemalli on TCP/IP-malli, jossa on neljä kerrosta. Sen alin kerros sisältää likimain OSI-mallin kerrokset 1 ja 2, toinen eli Internet-kerros vastaa OSI-mallin verkkokerrosta, kolmas eli kuljetuskerros vastaa OSI-mallin kuljetuskerrosta ja ylimpänä oleva sovelluskerros sisältää OSI-mallin kerrokset 5, 6 ja 7. [2.]

Tiedonvälityksessä sovelluskerroksen päällä olevassa sovelluksessa syntynyt data kulkee mallin kerrosten läpi alaspäin. Jokaisen kerroksen palvelut rakentavat uuden kehyksen, joka sisään ylemmältä kerrokselta tullut kehys sijoitetaan. Alimman kerroksen tehtävänä on ohjata syntynyt kokonaisuus siirtotielle. Vastaanotossa operaatiot tapahtuvat päinvastaisessa järjestyksessä. Menettelyä kutsutaan kapseloinniksi (encapsulation/decapsulation). Eri kerroksissa syntyvistä kehyksistä

käytetään vakiintuneita nimiä. Sovelluskerroksen kehys on datakehys. Kuljetuskerroksen kehyksestä käytetään nimitystä segmentti ja IP-kerroksen kehyksestä nimitystä paketti, tietosähke tai datagrammi. Alimpien kerrosten kehys on yksinkertaisesti kehys. [2.]

2.1 Ethernet-protokolla

Ethernet on pakettipohjainen lähiverkkoratkaisu (Local Area Network, LAN), joka on yleisin ja ensimmäisenä laajasti hyväksytty lähiverkkotekniikka. Ethernet toteuttaa OSI-mallin kerrokset 1 ja 2. Nykyisin yleisimmin käytössä olevat Ethernet-versio on Ethernet II, joka tunnetaan myös nimellä DIX Ethernet (Digital, Intel, Xerox Ethernet). Sen versio 1 julkistettiin vuonna 1980, ja nykyinen versio on 2. IEEE-standardi Ethernetistä tunnetaan nimellä IEEE 802.3. Ethernet-kehyksen (MAC-kehyksen) rakenne ja siihen VLAN-ympäristössä lisättävä 802.1Q-standardin mukainen VLAN-merkintäkenttä on esitetty kuvassa 2. [10.]



Kuva 2. Ethernet-kehys.

Kehyksen minimipituus on standardin mukaan vähintään 64 tavua ja maksimipituus, MTU (Maximum Transmission Unit), 1518 tavua. Pituuteen ei lasketa alkukenttiä (tahdistuskuvio preamble ja Start Frame Delimiter). VLANien käyttö kasvattaa maksimipituutta neljällä tavulla. Uusissa sovelluksissa voidaan lisäksi käyttää ns. jumbo-kehyksiä, jolloin kehyksen koko voi olla jopa 9000 tavua.

Kehys alkaa alkukentillä (seitsemän tavun tahdistuskuvio ja tavun mittainen aloitusmerkki). Seuraavana tulevat kuuden tavun kohde- ja lähdeosoitteet ja kahden tavun tyyppikenttä. Ethernet-osoitteita kutsutaan usein MAC-osoitteiksi.

Datakentän pituus vaihtelee välillä 46 - 1500 tavua, ja siihen voidaan lisätä ylimääräisiä täytetavuja (pad) 64 tavun minimipituuden saavuttamiseksi. Kehys päättyy tarkistussummaan (Frame Check Sequence), joka on 32-bittinen CRC (Cyclic Redundancy Check) koko kehyksestä lukuun ottamatta alkukenttiä.

Ethernet II:ssa tyyppikenttä määrittää datakentän sisältämän ylemmän OSI-kerroksen paketin protokollan, esimerkiksi IP:n. IEEE 802.3 -standardin mukaisessa kehyksessä tyyppikentän paikalla on kahden tavun pituuskenttä, joka ilmaisee kehyksen databittien määrän.

Nykyiset Ethernet-verkot ovat pääsääntöisesti kytkentäisiä. Verkon solmut liitetään toisiinsa kytkimien (switch) avulla ja kehykset ohjataan oikeaan segmenttiin kytkimen ylläpitämän MAC-osoitetaulun avulla. Etuina pakettikytkentäisillä verkoilla on, että yhteyden perustamisesta johtuvaa viivettä ei merkittävästi ole ja verkon resursseja käytetään tehokkaasti, koska samalla yhteydellä voi kulkea useita pakettivirtoja. Suurimmat ongelmat pakettikytkentäisissä verkoissa ovat tietopakettien välinen viive ja viiveen vaihtelu. On huomattava, että alkuperäisessä Ethernet-kehyksessä ei ole tiedonsiirron laadun määrittelyyn käytettävää informaatiota.

IEEE 802.3 -standardi sisältää määrittelyt Ethernet-kehyksen lisäkentille, joiden avulla protokollan ominaisuuksia laajennetaan. Yksi niistä on VLAN (Virtual LAN), jonka avulla lähiverkko voidaan jakaa loogisiin segmentteihin. Kytkentäisessä Ethernetissä jokainen segmentti muodostaa oman törmäysalueensa, mutta koko kytkin on yhtä broadcast-aluetta ja kaikista segmenteistä on pääsy muihin segmentteihin. VLAN-käytännön avulla segmentit voidaan erottaa toisistaan, jolloin niiden välinen liikenne on mahdollista vain verkkokerroksen palveluja käyttämällä.

IEEE 802.1Q-standardin mukaista VLAN-tekniikkaa käytettäessä VLAN-tunnistekenttä (tag) sijoitetaan kehykseen kohdeosoitekentän jälkeen. VLAN-tunnistekenttä muodostuu kahdesta kahden tavun mittaisesta osasta, Protokollatunnisteesta (Protocol Identifier) ja Tunnisteen ohjaustiedosta (Control Information). Ohjaustieto-kenttä jakautuu kolmeen alakenttään, Käyttäjän prioriteetti (User Priority), CFI (Canonical Format Indicator) ja VLAN ID. Kahdentoista bitin VLAN-ID-kenttä kertoo, mihin VLANiin kehys kuuluu. Kahdeksan bitin Käyttäjän prioriteetti -kentän (QoS) avulla voidaan määritellä 8 eri tärkeysluokkaa kehyksen kuljettamiseen. QoS-kenttä korjaa osittain

alkuperäisessä Ethernet-standardissa olleen tiedonsiirron laadun määrittelevän kentän puuttumisen. [10.]

2.2 Internet-protokolla versio 4

Internet-protokolla (IP) on on OSI-mallin verkkokerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa. IP-protokolla on yhteydetön, mikä tarkoittaa, että paketit kulkeutuvat verkossa ilman kiinteätä reittiä. Näin ollen paketit voivat kulkeutua verkossa eri reittejä lähettäjältä vastaanottajalle ja saapua vastaanottajalle väärässä järjestyksessä. Yhteydettömyydestä johtuen IP-protokolla tarjoaa vain epäluotettavan yhteyden eri verkon laitteiden välille. Käytännössä tämä tarkoittaa sitä, että ylempien protokollakerrosten on huolehdittava, että vastaanottaja on saanut informaation eheänä. [2.]

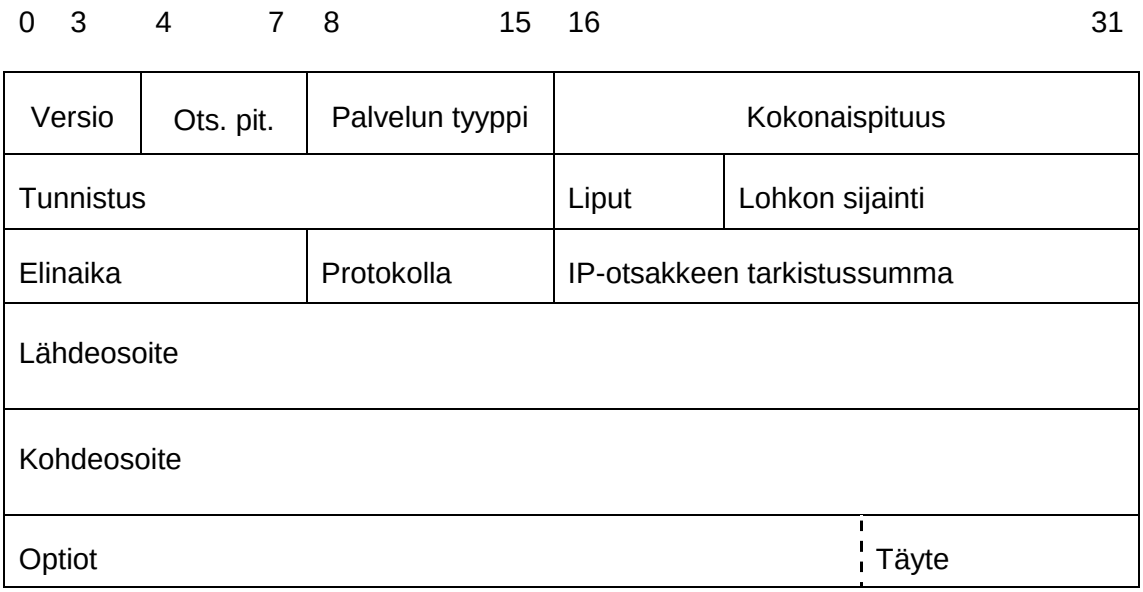
IP-paketti on Internet-protokollan perusyksikkö. Se muodostuu otsakkeesta (header) ja sitä seuraavasta data-alueesta (payload). Teoriassa IP-paketin maksimikoko on 65 535 tavua, mutta useimmiten liikennöivät koneet pyrkivät käyttämään suurinta mahdollista OSI-2-kerroksen verkkotekniikoille sopivaa pakettikokoa, joka on yleisesti n. 1 500 tavua. Mikäli koneet lähettävät sitä suurempia paketteja, joutuu liian ahtaan verkon reunalla oleva laite lohkomaan tai paloittelemaan paketit pienempiin osiin (fragment).

Tällä hetkellä käytetään yleisimmin IP-protokolla versio 4:ää, mutta uudempi, versio 6 on vähitellen syrjäyttämässä sen. IPv4-osoitteen pituus on 32 bittiä. Se esitetään tavallisesti jaettuna neljään kahdeksan bitin mittaiseen osaan, oktettiin, jotka on koodattu desimaaliseksi ja erotettu toisistaan pisteellä. Osoitteesta käytetään joskus myös nimitystä pisteosoite (dotted decimal). IPv4-osoite on hierarkkinen. Sen alkuosa määrittelee verkon ja loppuosa työaseman osoitteen verkossa. Osoiteavaruus on jaettu viiteen luokkaan, joista kolme ensimmäistä on tarkoitettu täsmälähetysosoitteiksi (unicast), neljäs ryhmälähetykseen (multicast) ja viides on varattu tulevaisuuden tarpeisiin.

Classless Interdomain Routing (CIDR) -menettelyssä osoiteluokilla ei ole merkitystä, vaan IP-osoite määritellään osoitteen ja verkkopeitteen avulla. Verkkopeitteen 1-bitit kertovat verkon ja loppuosa osoitteesta työaseman tunnuksen verkossa. CIDR-osoite esitetään prefiksimuodossa osoite /n, jossa n on prefiksin pituus eli verkkopeitteen 1-

bittien lukumäärä. Tämä esitystapa on otettu käyttöön myös luokallisten osoitteiden esittelyssä ja myöhemmin IPv6-osoitteissa. [2.]

IPv4:n perusotsake on esitetty kuvassa 3. Se koostuu vähintään viidestä 32-bittisestä sanasta ja 12 kentästä. Otsakkeen minimipituus on 20 tavua. Lisäksi siinä voi olla optiokenttä, joka lisää otsakkeen pituutta. Kenttien rajat bitteinä on merkitty kuvan yläpuolelle. [2.]



Kuva 3. IPv4-otsake. [2.]

IPv4-otsake alkaa 4 bitin Versio-kentällä, jonka arvo on yleensä 4. Seuraava 4 bitin kenttä on Otsakkeen pituus. Siinä määritetään otsakkeen pituus 32-bittisinä sanoina.

Palvelun tyyppi -kentässä (ToS) määritetään palvelun tyyppi. Kentän pituus on 8 bittiä, se on jaettu kolmeen osaan. Ylimmillä kolmella bitillä ilmaistaan prioriteetti, seuraavilla neljällä liikenteen tyyppi ja alin bitti on aina 0.

Kentässä Kokonaispituus ilmoitetaan paketin pituus. Kentän pituus on 16 bittiä, joten pituus voi olla suurimmillaan 216 -1 eli 65 535 tavua. Käytännössä näin pitkiä paketteja ei käytetä. Standardi määrittelee vain, että laitteiden on kyettävä ottamaan vastaan vähintään 576 oktetin mittaisia paketteja.

Tunnistus-kenttä on pituudeltaan 16 bittiä. IP-paketit tunnistetaan tässä kentässä olevan yksilöllisen tunnisteen avulla esimerkiksi silloin, kun lohkotut paketit kootaan kohteessa.

Liput-kentän pituus on kolme bittiä. Ylimmän bitin arvo on asetettu kiinteästi nollaksi. Kun toinen bitti (Älä lohko, Don't Fragment) on 1, paketin lohkominen (paloittelu, fragmentointi) on sallittu. Jos alin bitti (Lisää lohkoja tulossa, More Fragments) on 1, pakettiin kuuluvia lohkoja on tulossa vielä tämän lohkon jälkeen. Jos se on 0, tämä on alkuperäisen paketin viimeinen lohko.

Lohkon sijainti -kenttä on pituudeltaan 13 bittiä. Sen avulla ilmaistaan lohkon sijainti alkuperäisessä paketissa. Elinaika-kenttä (Time To Live, TTL) on kahdeksan bitin mittainen ja ilmaisee paketin elinajan hyppyinä. Jokainen siirtotiellä oleva reititin vähentää reitityksen yhteydessä kentän arvoa yhdellä. Kun se menee nollaksi, paketti tuhotaan ja lähettäjälle lähetetään ICMP-sanoma. Tällä menettelyllä varmistetaan, että verkkoon ei jää orpoja paketteja. Kentän maksimiarvo voi olla 255, mutta nykyisten suositusten mukainen käytäntö on 64.

Protokolla-kenttä on kahdeksan bitin mittainen ja siinä kerrotaan ylemmässä kerroksessa käytettävä protokolla. Yleisimmin käytössä ovat protokollat ICMP (1), IGMP (2), TCP (6) ja UDP (17). Tarkistussumma on pituudeltaan 16 bittiä. Sen avulla varmistetaan, etteivät otsake-kentän tiedot muutu matkan aikana.

Kentät Lähdeosoite ja Kohdeosoite ovat 32 bittiä pitkiä. Niihin sijoitetaan lähettäjän ja vastaanottajan IP-osoitteet. On huomattava, että IPv4-protokollassa nämä osoitteet eivät muutu paketin lähetyksen aikana, poikkeuksena NAT-osoitekäännös (Network Address Translation).

Optiot-kentän pituus on korkeintaan 320 bittiä (40 oktettia). Siinä voidaan määritellä turvallisuuteen ja reitittämiseen liittyviä asioita Käytännössä optioita käytetään melko harvoin. Optiot-kenttä täytetään 32 bitin rajalle, mikäli sen pituus jäisi pienemmäksi. [2.]

QoS tarkoittaa pakettikytkentäisen verkon tietoliikenteessä datapakettien luokittelua ja priorisointia. Sen avulla voidaan saada jokin haluttu liikenne käyttämään maksimaalista siirtokapasiteettia tai vastaavasti pudottaa koko liikenne pois siirtokapasiteetin sitä vaatiessa. Kuten IP-otsakkeen rakenteesta havaittiin, siinä on varauduttu tiedonsiirron laadun ohjaamiseen Palvelun tyyppi -kentän (ToS) avulla. Tarkoitus oli, että ToS-bittehin perustuvan luokittelun perusteella paketteja käsitellään verkon solmussa eri tavoin. ToS-käsittely on kuitenkin erittäin harvoin käytössä. Sen

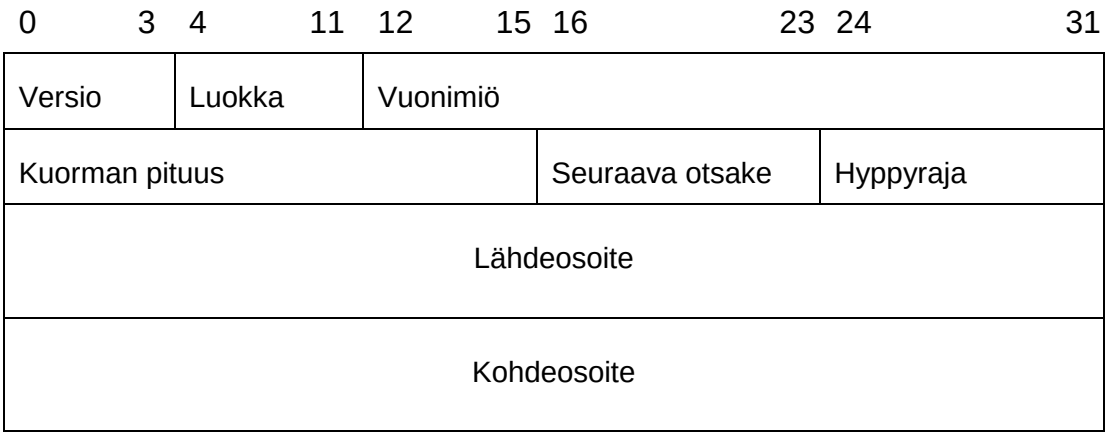
sijaan kentän kahdeksan bitin avulla on kuitenkin mahdollista rakentaa kehittyneempiä ratkaisuja. Niistä kerrotaan lähemmin luvussa 4.

2.3 Internet-protokolla versio 6

Vaikka tässä työssä käytetään Internet-protokolla versio 4:ään pohjautuvia ratkaisuja, on syystä esitellä lyhyesti uusi, tulevaisuudessa valta-asemaan nouseva versio 6. IPv6-otsakkeen suunnittelussa keskeisenä tekijänä oli minimoida sen käsittelystä aiheutuva kuorma. Se sisältää vain lähetyksessä tarvittavat kentät ja lisämäärittelyt on sijoitettu omiin otsakkeisiinsa, jotka sijoitetaan pääotsakkeen perään.

IPv6-osoiteavaruus on 128 bittiä. Tämä tarkoittaa, että teoreettisesti saadaan 2^{128} eli $3{,}4 \times 10^{38}$ osoitetta. IPv6-osoitteissa 64 bittiä on varattu oletuksena verkolle ja 64 bittiä työasemalle. Osoitteet koodataan heksadesimaalisena neljän numeron (16 bittiä, sana) ryhmiin kaksoispisteillä erotettuina.

IPv4- ja IPv6 -otsakkeet eivät ole yhteensopivia. Työasema tai reititin, joka käyttää molempia, on konfiguroitava sisältämään kummatkin protokollat. IPv6-otsake on kooltaan vain kaksinkertainen verrattuna IPv4-otsakkeeseen, vaikka osoiteavaruus on moninkertainen. Kuvasta 4 selviävät IPv6:n otsakkeen rakenne ja siihen kuuluvat 8 kenttää. Kenttien rajat bitteinä on merkitty kuvan yläpuolelle. [13.]



Kuva 4. IPv6-otsake. [13.]

IPv6:n otsake on 40 tavua pitkä. Se alkaa 4 bitin Versio-kentällä, jonka arvo IPv6:ssa on aina 6. Seuraava kenttä on 8-bittinen Luokka-kenttä (Traffic Class, TC). Sen avulla paketit luokitellaan ja priorisoidaan. Jos kentän arvo on välillä 0 - 7, liikenne voi

hidastua ja pakettien järjestys saa muuttua ruuhkatilanteissa, ns. ruuhkavalvottu liikenne. Arvot 8 - 15 kertovat, että paketit sisältävät tosiaikaista dataa, jolloin halutaan vakionopeus ja viive. Luokka-kentän arvot on esitetty taulukossa 1. [13.]

Taulukko 1. Luokka-kentän mahdolliset arvot.

Arvo	Kuvaus	Esimerkkisovellus
Ruuhkavalvottu liikenne		
0	Määrittelemätön liikenne (uncharacterized traffic)	
1	Täyttöliikenne (filler traffic)	Verkkouutiset
2	Ei-osallistuva liikenne (unattended data traffic)	Sähköposti
3	Ei vielä käytössä	
4	Osallistuva massasiirto (attended bulk traffic)	FTP, HTTP
5	Ei vielä käytössä	
6	Vuorovaikutteinen liikenne (interactive traffic)	Telnet, X/Window
7	Verkon valvontaliikenne (Internet control traffic)	SNMP, OSPF, BGP
Ruuhkavalvomaton liikenne		
8	Sopivin hävitettäväksi	Teräväpiirtovideo
…		
15	Vähiten sopiva hävitettäväksi	VOIP-puhelu

Vuonimiö-kentän pituus on 20 bittiä (vuon tunnus, Flow Label). Se määrittelee samasta lähteestä samalle vastaanottajalle lähetetyn peräkkäisten pakettien jonon, jota reitittimen halutaan käsittelevän samalla tavalla. Kuorman pituus -kentässä (Payload Length) ilmoitetaan paketin koko ilman otsaketta. Kentän pituus on 16 bittiä, eli suurin arvo, joka tähän voidaan sijoittaa, on 65535. Suurempien pakettien (jumbogram) käyttö on mahdollista lisäotsakkeen avulla, jossa paketin koko ilmaistaan 32 bitillä (paketin maksimikoko on 2^{32} eli yli neljä miljardia tavua).

Perusotsake ei sisällä kehittyneempiä palveluita. Nämä on toteutettu otsakkeen Seuraava otsake -kentän (Next Header) avulla. Sitä käyttäen IPv6-otsakkeeseen voidaan linkittää lisäotsakkeita (laajennusotsakkeita).

Hyppyraja (Hop Limit) on 8 bitin laskuri, jonka arvoa vähennetään jokaisessa hypyssä. Kun arvo menee nollaksi, paketti hävitetään. Otsakkeen lopussa ovat 128-bittiset (16 oktettia) lähde- ja kohdeosoitekentät. [13.]

IPv6 ei tarjoa automaattisesti palvelunlaatua, mutta sisältää tuen sille. Vuonnimiökentän avulla tunnistetaan samaan yhteyteen kuuluvat paketit, mikä mahdollistaa niiden samanlaisen käsittelyn verkon solmuissa. Luokka-kentän avulla IP-paketteihin lisätään tieto siitä, miten pakettia tulisi käsitellä verkkoliikenteessä.

2.4 Kuljetuskerroksen protokollat

Yleisimmät kuljetuskerroksen protokollat ovat TCP ja UDP. TCP (Transmission Control Protocol) on yhteydellinen ja luotettava protokolla. Luotettavuus saavutetaan pakettien numeroinnin ja uudelleenlähetyksen avulla. UDP (User Datagram Protocol) on yhteydetön tiedonsiirtoprotokolla, eikä se vaadi kättelyä ennen lähetystä. Myös UDP valvoo datan eheyttä, mutta vahingoittuneet paketit heitetään lattialle ilman virheilmoituksia, ja mahdollinen uudelleenlähetys jää sovellustason protokollan tehtäväksi. TCP ja UDP käyttävät porttinumeroita erottamaan liikennevirat toisistaan.

UDP-otsakkeen rakenne on yksinkertainen. Siinä ovat vain 16-bittiset lähde- ja kohdeportit, segmentin pituus ja varmistussumma. Data sijoitetaan otsakekentän perään. Segmentin maksimipituus on 65535 tavua.

Reaaliaikaisen IP-liikenteen kuljettamiseen käytetään RTP-protokollaa. Sitä käytetään tavallisimmin UDP-protokollan kanssa. RTP ei takaa pakettien oikeaa saapumisjärjestystä eikä muitakaan laadunvarmistuskeinoja. Se sisältää tiedon kehyksen järjestyksestä, aikaleimasta, kuljetettavan datan tyypistä ja toimituksen seurannasta. Vaikka RTP on yhteydetön protokolla, se mahdollistaa kadonneiden pakettien seurannan järjestysnumeroiden avulla.

RTP:n rinnalla toimii RTCP-protokolla. Sen pääasiallinen tarkoitus on antaa tietoa RTP-yhteyden palvelun laadusta. Tämän lisäksi se mittaa yhteyden datamääriä ja mahdollistaa ryhmäneuvotteluiden toiminnan.

RSVP (Resource ReSerVation Protocol) on kuljetuskerrosprotokolla, joka on suunniteltu varaamaan riittävä kapasiteetti yhdelle yksisuuntaiselle datavuolle verkon läpi asiakkaan vaatimustason mukaisesti. Reitittimet käyttävät RSVP:tä välittämään palvelutasovaatimukset solmupisteille ja varmistamaan vaaditun palvelun toimivuuden. RSVP on pelkästään ohjausprotokolla, joka ei osallistu datan kuljetukseen.

2.5 VoIP

VoIP eli IP-puhe on puheen välittämistä IP-verkossa IP-protokollaa käyttäen. Äänidata kulkee verkossa IP-paketeissa. VoIP:n ydinprotokolla on SIP (Session Initiation Protocol). SIP-protokollan tehtävänä on muodostaa, hallita ja lopettaa istuntoja. Sen toiminta perustuu yksinkertaisiin tekstisanomiin. Toinen yleisesti käytetty protokolla on H.323. H.323 määrittelee mm. merkinannon, median ohjauksen ja käytettävän ääni- ja videokoodekin.

Koodekin tehtävä on muuttaa analoginen signaali digitaaliseksi. Sitä käytetään VoIP-tekniikassa muuttamaan analoginen signaali digitaaliseksi, jotta se voidaan siirtää IP-pakettina vastaanottajalle. Vastaanottajalla koodekki muuttaa signaalin takaisin digitaalisesta analogiseksi.

VoIP-paketin rakenne on esitetty kuvassa 5.

14 B	20 B	8B	12 B	20 B
Ethernet-otsake	IP-otsake	UDP-otsake	RTP-otsake	Äänidata

Kuva 5. Tyypillinen VoIP-paketti.

3 Multiprotocol Label Switching (MPLS)

Reititys on keskeinen osa IP-liikennöinnissä. Sen avulla IP-paketit ohjataan verkossa lähettäjältä vastaanottajalle. Mikäli vastaanottaja on samassa verkossa kuin lähettäjä, ei reititystä tarvita, vaan asema osaa lähettää paketin suoraan vastaanottajalle. Reitityksestä huolehtiva laite on reititin, jonka tehtävänä on valita IP-paketille paras reitti kohti vastaanottajaa ja ohjata paketti sitten verkkoon. Reitittimet pitävät yllä reititystietokantaa (routing table, reititystaulu), jonka avulla paketti ohjataan kohteeseen. Reititystaulun ylläpitoon käytetään reititysprotokollia, jotka rakentavat ja ylläpitävät kuvausta verkon topologiasta.

Perinteinen IP-paketin välitys perustuu siis kohteen IP-osoitteen analysointiin. Lähde- ja kohdeosoitteet on talletettu jokaisen datapaketin otsakkeeseen. Reitittimet

analysoivat kohdeosoitteet ja tekevät reitityspäätökset itsenäisesti jokaisella hypyllä matkalla verkon yli.

Multiprotocol Label Switching (MPLS) on protokolla, jossa yhdistyvät kytkentäisten verkkojen suorituskyky ja reititysverkkojen skaalautuvuus. Erona puhtaisiin IP-verkkoihin on, että MPLS mahdollistaa liikenteen välittämisen verkon yli ilman, että se on reititettävä jokaisella hypyllä erikseen. MPLS-arkkitehtuuria kutsutaan lippukytkentäiseksi (leimakytkentäinen), ja se yhdistää parhaat puolet OSI-mallin 2. kerroksen (Layer 2, L2) kytkentäverkoista ja 3. kerroksen reititysverkoista (Layer 3, L3).

Keskeistä MPLS-verkoissa on myös mahdollisuus tunneloida eri protokollien liikenne ja kuljettaa ne saman verkkoinfrastruktuurin yli. Tunnelointi on tehokas ja tietoturvallinen menettely, sillä vain verkon reunalaitteiden tarvitsee osata käsitellä liikenne sen perusmuodossaan. Muut verkon laitteet vain välittävät liikennettä, eikä niiden tarvitse ymmärtää tunnelien sisällä kulkevaa liikennettä. [3. s. 7-12.]

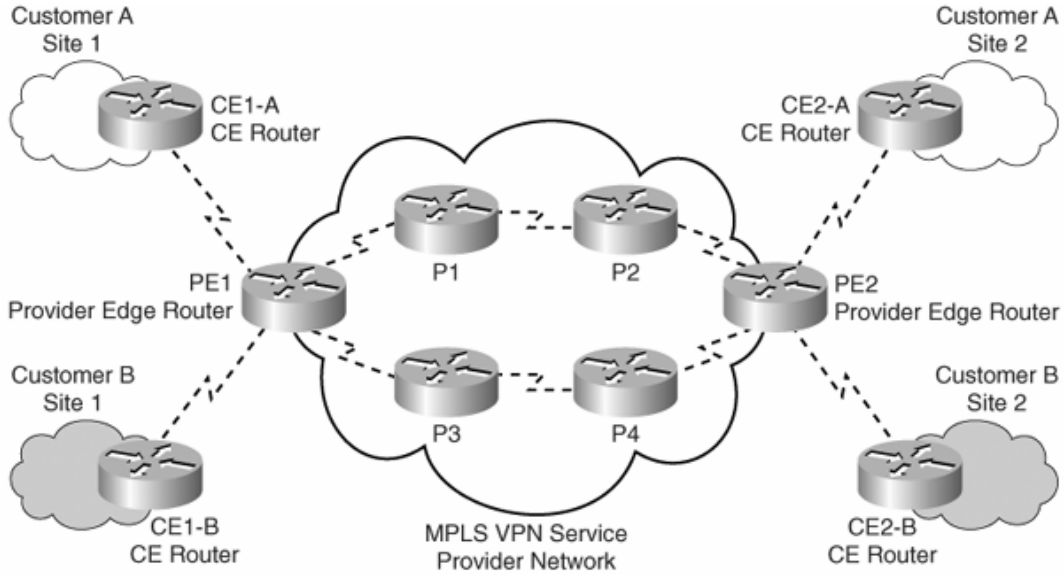
3.1 MPLS-verkon toiminta

Normaalissa IP-verkossa välitettävän IP-paketin reititys perustuu otsakkeessa olevan IP-osoitteen analysointiin. Joissain tapauksissa käytetään myös muita otsakkeen kenttiä. Otsake on analysoitava ja reititys tehtävä jokaisessa reitittimessä, jonka läpi paketti kulkee, mikä kuormittaa verkkoa ja vaikuttaa liikenteen sujuvuuteen. MPLS-verkossa IP-paketin L3-otsake analysoidaan vain kerran ja sen jälkeen sille annetaan lukuarvo, jota kutsuntaan lipuksi (leima, label). Matkan varrella olevat reitittimet tekevät reitityspäätökset lippumerkinnän perusteella.

IP-reititys on kuitenkin edellytys MPLS:n toiminnalle verkossa. Kuvassa 6 on esitetty MPLS-verkon toiminnallinen rakenne. CE-laite (Customer Edge) on asiakkaan toimipisteen laite, joka kytkeytyy palveluntarjoajan verkkoon liityntäverkon (access network) välityksellä. Verkko rakentuu reunalaitteista, joita kutsutaan LER- tai PE-laitteiksi (Label Edge Router / Provider Edge) ja runkolaitteista, jotka tunnetaan LSR- tai P-laitteina (Label Switching Router / Provider Router). PE-laite on siis palveluntarjoajan runkoverkon laite, johon asiakas on liittyneenä. Yleensä PE-laite on leimakytketyn runkoverkon reunareititin. Runkoverkko (Provider Network) on verkko, joka yhdistää PE-laitteet toisiinsa. PE-laitteet käyttävät runkoverkkoa liikenteen kuljettamiseen ja kommunikointiin toistensa kanssa. PE-laitteiden välille muodostetaan

yksisuuntaisia lippukytkentäpolkuja (LSP, Label Switched Path), joita pitkin liikenne kulkee.

Kun PE-reititin vastaanottaa paketin asiakkaan CE (Customer Edge) -reitittimeltä, se määrittelee MPLS-lipun arvon perusteella, mihin Forwarding Equivalence Class (FEC) -luokkaan paketti kuuluu. Jokainen samaan FEC-luokkaan kuuluva paketti kuljetetaan samaa LSP-polkua pitkin vastaanottavalle laitteelle. P-reitittimet lippukytkentäpolun varrella edelleenvälittävät liikennettä lippumerkinnän perusteella. P-laite lukee paketin lippumerkinnän ja valitsee merkinnän perusteella oikean lipputiedon käytettäväksi seuraavalla hypyllä. [4.]

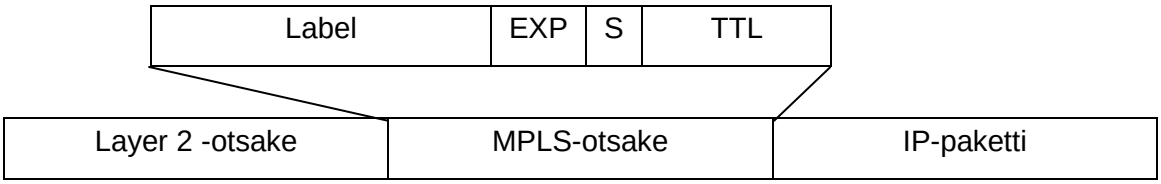


Kuva 6. MPLS-verkon rakenne. [11.]

FEC-luokkia voidaan käyttää avuksi liikenteen priorisoinnissa ja luokittelussa. Rajoittamalla pienemmän prioriteetin liikenteen kaistanleveyttä saadaan korkeammalle prioriteetille enemmän kaistaa käyttöön.

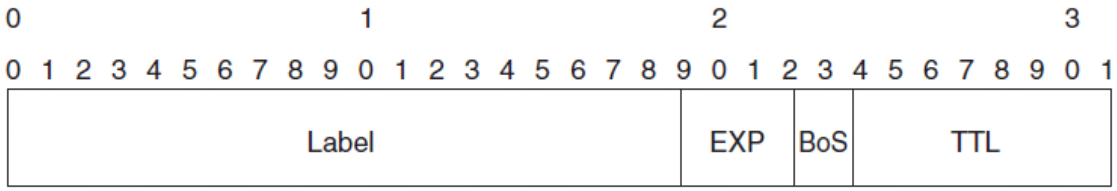
3.2 MPLS-otsake

Ennen paketin välittämistä MPLS-verkon kuljetettavaksi PE-reititin kapseloi paketin MPLS-paketiksi. MPLS-kapseloinnissa paketin L2- ja L3-kehyksen väliin lisätään 32 bitin pituinen MPLS-otsake (ks. kuva 7). On huomattava, että IP-paketti säilyy tässä operaatiossa muuttumattomana.



Kuva 7. MPLS-otsakkeen sijoittuminen. [4.]

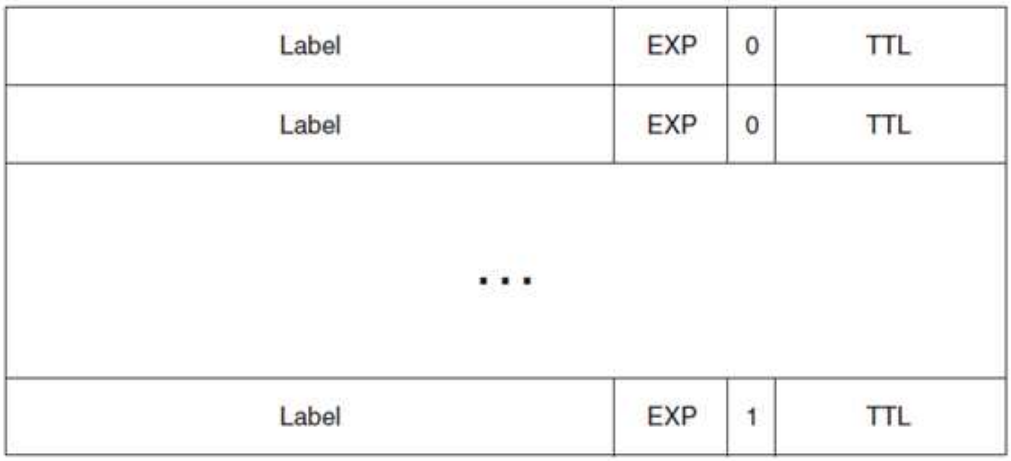
MPLS-otsake rakentuu neljästä kentästä. Alun 20 bittiä on varattu lippumerkinnälle, jonka perusteella paketti lippu kytketään. Kentän arvo on välillä 0 … 2^{20-1} (1048575). Bitit 20-22 on varattu Experimental-kentälle (EXP) ja kenttää käytetään yksinomaan QoS-priorisointiin (QoS). MPLS-otsakkeen rakenne on esitetty kuvassa 8.



Kuva 8. MPLS-otsakkeen rakenne. [4.]

MPLS-otsikoita voidaan pinota päällekkäin (Label Stacking). Otsakkeen bitti 23, BoS (Bottom of Stack) -bitti kertoo, onko kyseessä pinon alimmainen otsikko. BoS-bitin arvo on 1, jos lippu on kasan alin, muuten se on nolla. MPLS-otsakepino on esitetty kuvassa 9.

Viimeistä kenttää, bitit 24-31, käytetään estämään, ettei paketti jää pyörimään silmukkaan loputtomiksi ajoiksi. Jokaisella hypyllä reititin vähentää tämän kentän arvoa yhdellä ja paketti pudotetaan pois verkosta, jos kentän arvo laskee nollaan.



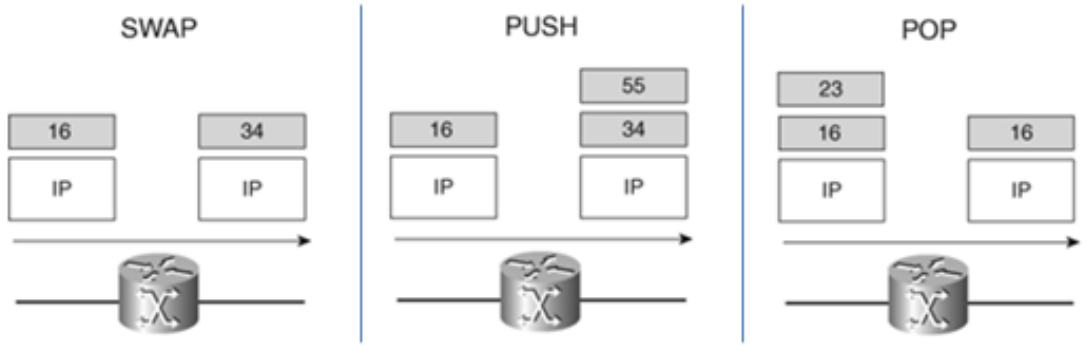
Kuva 9. MPLS-otsakepino. [4.]

MPLS-verkon yli siirrettävällä liikenteellä on aina yksi tai useampi MPLS-otsake. Kuitenkin jossain tapauksissa, kuten julkisen IP-liikenteen kuljettamisessa MPLS-verkon läpi, yksi MPLS-otsake on riittävä. Kun paketti on perillä, sen L3-otsake tutkitaan ja paketti reitittetään eteenpäin perinteisen IP-reitityksen keinoin.

Jotkin MPLS-sovellukset vaativat useamman kuin yhden lipun otsakepinossa. Esimerkki tällaisesta on MPLS-VPN. VPN-palveluita käytettäessä PE-reitittimillä täytyy olla tieto, mihin palveluun ja mihin tämän palvelun instanssiin vastaanotettu liikenne kuuluu. Tämä tieto voidaan kuljettaa liikenteen mukana lisäämällä paketteihin toinen MPLS-otsake. Tällöin päällimmäinen lippu ohjaa liikenteen oikealle runkolaitteelle alemman lipun erotellessa palvelun. [4. s. 25-27]

Lippu on linkkikohtainen, ja MPLS-verkon reitittimet voivat tarvittaessa joutua tekemään paketille lisätoimenpiteitä ennen sen välittämistä eteenpäin. Toimenpiteitä on kolme erilaista (ks. kuva 10):

- Reititin vaihtaa päällimmäisen lipun arvoksi seuraavan hypyn leiman (SWAP).
- Reititin poistaa leiman esimerkiksi silloin, kun paketti poistuu MPLS-verkosta ja jatkoreititys tapahtuu IP-osoitteen perusteella (POP).
- Kun paketti saapuu MPLS-verkkoon, reititin lukee PE-reititin paketin otsikkotiedoista sen kohdeosoitteen sekä palveluvaatimukset, joiden mukaan suoritetaan LSP:n asettaminen sekä leiman valinta. Vanhoja leimoja siirretään alaspäin ja uusi leima sijoitetaan pinon päälle. (PUSH). [3.]



Kuva 10. MPLS-lippuoperaatiot. [3.]

3.3 Label Distribution Protocol, LDP

PE-reitittimet käyttävät Label Distribution Protocol -protokollaa (LDP) leimojen jakamiseen kahden LSR:n välillä. Kaksisuuntaisen viestien lähetyksen ansiosta LSR saa paluuviestinä tiedot naapurireitittimien tarjoamista mahdollisuuksista reitittää paketit verkon läpi annetuilla määrityksillä sekä niiden muodostamat leima- ja FEC-tiedot.

LDP-protokollan avulla MPLS-verkon laitteet sopivat lippujen merkityksestä ja sen avulla jokainen laite jakaa paikallisesti määritellyt lippumerkinnät muille laitteille sekä ylläpitää Label Information Base (LIB) -taulua, johon tiedot lippumerkintöjen merkityksistä tallennetaan. LDP-protokolla ei itse suorita reititystä. Siihen käytetään IGP-reititysprotokollia (Interior Gateway Protocol). LSP-polut noudattavat käytössä olevan IGP-protokollan ilmoittamia lyhyimpiä reittejä ja mukautuvat verkon mukaan, jos IGP:n reittitiedot muuttuvat.

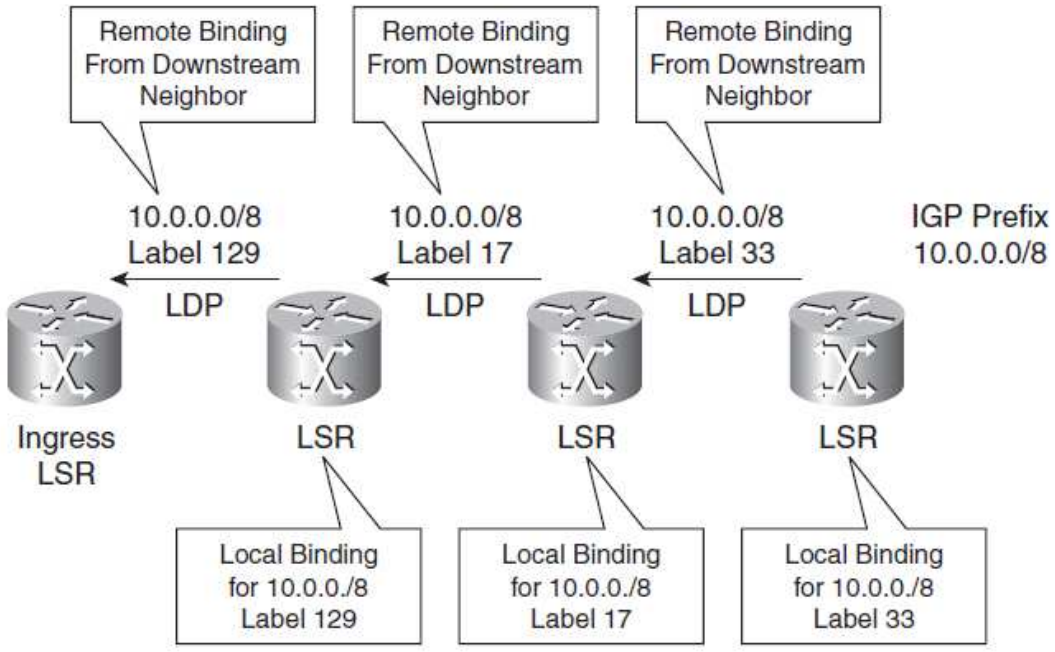
LDP-protokollalla on neljä päätarkoitusta:

- toisten LDP-protokollaa käyttävien LSR-reitittimien havainnointi
- istunnon aloitus ja ylläpito
- sidoksien mainostus
- tiedotusviestit tapahtuneista virheistä.

Kun kaksi LDP-protokollaa käyttävää LSR-reititintä kytketään toisiinsa yhdellä tai useammalla linkillä, ne löytävät toisensa Hello-viestien avulla, jonka jälkeen ne avaavat

istunnon TCP-yhteyttä käyttäen (init). LDP-protokolla mainostaa TCP-yhteyden yli sidoksiaan kahden reitittimen välillä LDP-PDU-paketeilla käyttäen UDP- ja TCP-protokollia. LDP-PDU-viestejä käytetään sidoksien mainostamiseen, vaihtamiseen tai poistamiseen. Reititin voi ilmoittaa LDP-naapurille virheviesteistä lähettämällä tiedotusviestejä. [7, 4.]

Kuva 11 näyttää, kuinka IP-paketti − kohdeosoitteenaan verkko 10.0.0.0/8 − saapuu MPLS-verkkoon Ingress LSR:n läpi. Tässä vaiheessa paketille annetaan laitteessa lippuarvo 129, joka ohjaa paketin kohti seuraavaa laitetta. Toinen LSR vaihtaa saapuvan lipun arvon 129 ulospäin lähtevään arvoon 17 ja ohjaa paketin kohti seuraavaa PE-reititintä. Kolmas laite vaihtaa taas lipun arvon, tällä kertaa tilalle määritellään 33, ja paketti ohjataan taas eteenpäin. Tämä toistuu niin kauan, että paketti saapuu kohteeseensa. [4.]



Kuva 11. Lippukytkentäpolun toimintaperiaate. [4.]

3.4 MPLS VPN

Virtuaaliverkko, VPN, on tiedonsiirtoverkko, jossa yhteydet on toteutettu käyttäen jaettua infrastruktuuria ja jolla on samat turvallisuusominaisuudet kuin yksityisellä verkolla. MPLS VPN -yhteyksissä on kolme eri toteutustapa:

- L3 VPN

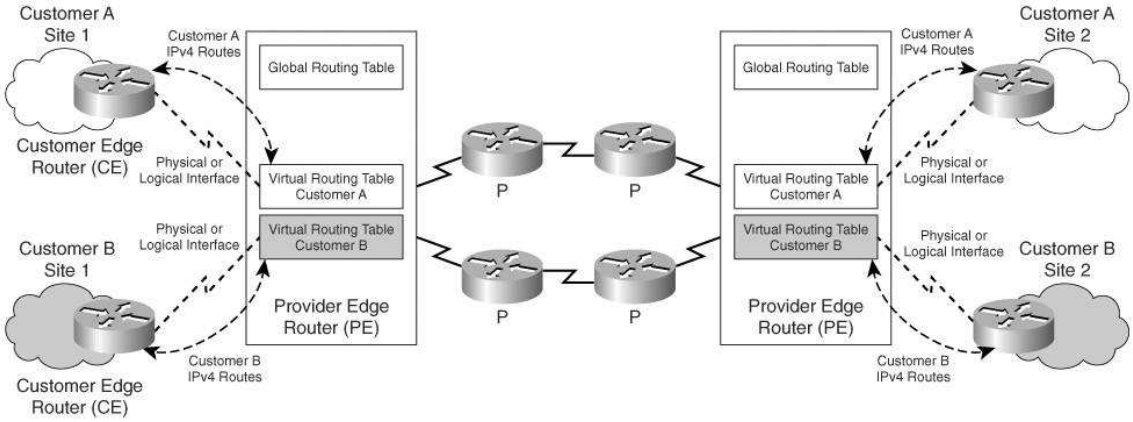
- L2 VPN
- Virtual Private LAN -palvelut.

L3 VPN -ratkaisussa palveluntarjoajan MPLS VPN -verkko liittyy asiakkaan reititinverkkoon. Asiakkaan CE-reitin käyttää BGP- tai OSPF-protokollaa ja keskustelee palveluntarjoajan PE-reitittimen kanssa. Tässä työssä käsitellään L3 VPN -ratkaisuja.

L2 VPN -toteutuksessa palveluntarjoajan verkko yhdistää asiakkaan OSI-2-kerroksen verkkoja, esimerkiksi Ethernet-verkkoja toisiinsa. Verkkokerroksen protokollat eivät siis näy kehysten siirron aikana.

Virtual Private LAN -palveluita käytettäessä palveluntarjoajan verkko käyttäytyy Ethernet-kytkimen tavoin ja voi tarjota laajan maantieteellisen ulottuvuuden. [8.]

L3 MPLS VPN -toteutuksessa tilaajan jokainen toimipiste liitetään suoraan operaattorin runkoverkon PE-reunareitittimeen omalla yhteydellään. Jokainen PE-reititin voi sisältää useita VPN-yhteyksiä. Yhteyksiä käsitellään operaattorin puolelta omina yksityisverkkoinaan ja niitä voidaan tarvittaessa yhdistää (ks. kuva 12).



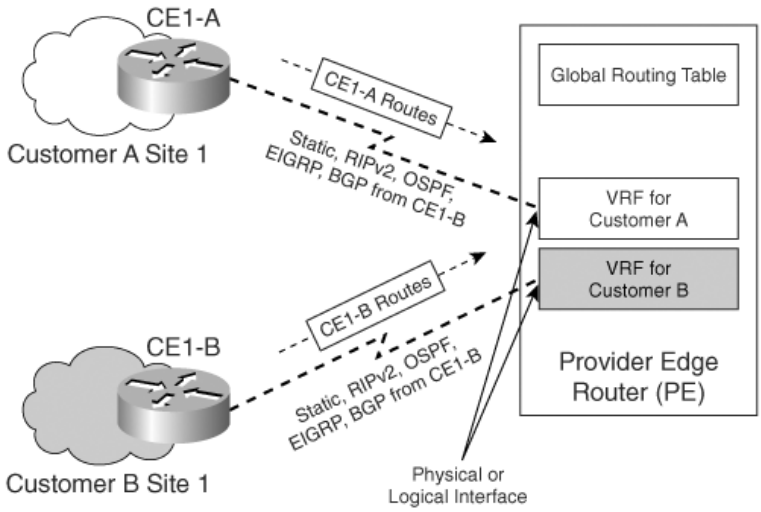
Kuva 12. L3 MPLS VPN -periaatekuva. [11.]

Vaikka pakettien välitykseen käytetäänkin yhteistä verkkoa, paketit kulkevat vain samaan VPN-yhteyteen määritettyjen toimipisteiden välillä. Tämän takia ulkopuoliset eivät näe niitä. Toimipiste voi kuulua yhteen tai useampaan VPN-yhteyteen ja voi olla yhteydessä vain saman VPN-alueen sisällä oleviin verkkoihin. [4.]

3.4.1 Virtual Routing and Forwarding, VRF

MPLS VPN -asiakkaiden erotus PE-reitittimissä tapahtuu virtuaalisten reititystaulujen avulla (Virtual Routing and Forwarding, VRF). Ne sisältävät ainoastaan samaan VPN:ään kuuluvat reitit. VRF-taulu sijoitetaan PE-reitittimeen asiakkaan sisääntuloliitynnälle, jolloin liitynnästä saapuvat paketit voidaan reitittää VRF-taulun mukaisesti runkoverkon läpi kohdeosoitteeseen. IP-reititystauluihin ei tule tietoa asiakkaan käyttämästä sisääntuloliitynnästä eikä sen takana sijaitsevista verkoista, jolloin ne näkyvät ainoastaan kyseisen VRF:n reititystaulussa. VPN-yhteyden ulkopuolisilla alueilla ei ole tietoa sisäpuolen verkosta tai liikenteestä, joten MPLS VPN on hyvin tietoturvallinen, vaikka yhteyksiä ei salattaisikaan erillisellä liikenteensalausprotokollalla.

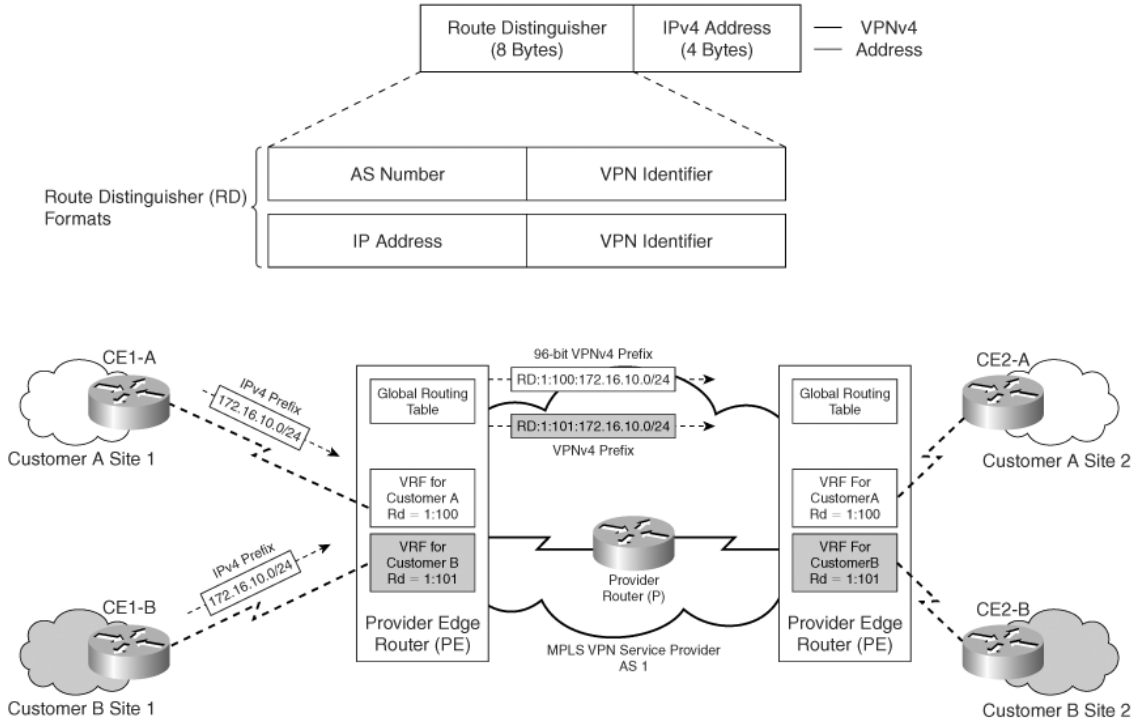
MPLS-verkossa PE-reitittimet määrittävät yksilöllisen lipun jokaiselle VPN:lle. Määritys suoritetaan, vaikka seuraavan paketin reitti pysyisikin samana. VPN-lippujen ja normaaleiden MPLS-lippujen levitys saadaan pidetyksi erillään käyttämällä kaksikerroksista lippupinoa. VPN-reititysinformaatio PE-reitittimien välillä MPLS-verkossa levitetään käyttämällä tarkoitukseen sopivaa Multiprotocol BGP -reititysprotokollaa (MP-BGP). Reititettävän paketin saapuessa reunareitittimelle muunnetaan sen IPv4-prefiksi VPNv4-prefiksiksi (Virtual Private Network version 4), jonka jälkeen paketti kuljetaan runkoverkon läpi. Muunnoksessa IPv4-prefiksiin lisätään 64-bittinen Route Distinquisher eli RD. VRF.toiminta on esitetty kuvassa 13. [11.]



Kuva 13. VRF:n toiminta. [11.]

3.4.2 Route Distinquisher, RD

Route Distinquisher (RD) on 64-bittinen tunniste, jota käytetään yksilöimään CE-reitittimeltä saadut reitit. Alkuperäinen 32-bittinen prefiksi sekä lisätty RD muodostavat yhdessä 96-bittisen osoitteen, VPNv4-osoitteen (VPN versio 4 -osoite). RD:n muodostamiseen on kaksi vaihtoehtoa. Jos asiakkaalla on BGP AS -tunnus, RD muodostetaan siitä. Jos AS-tunnusta ei ole, käytetään IP-osoitemuotoa (ks. kuva 14). Kuvassa nähdään myös, kuinka kahdelta asiakkaalta saatu sama prefiksi 172.16.10.0/24 erotetaan käyttämällä eri RD-arvoja (1:100 ja 1:101).



Kuva 14. RD-toiminta MPLS VPN -verkossa. [11.]

VPNv4-reittien välitykseen käytetään MultiProtocol BGP -protokollaa (MP-BGP). Sen lisäksi PE-reitittimissä tarvitaan IGP-reititysprotokollaa, esimerkiksi OSPFv2 tai ISIS, NLRI-informaation välittämiseksi. Network Layer Reachability Information -arvo (NLRI), viittaa kohteen verkko-osoitteeseen. Lisäys tarjoaa eri asiakkaille mahdollisuuden käyttää päällekkäisiä IPv4-osoitteita lähiverkoissaan ilman, että ne kuitenkaan vaikuttavat runkoverkon toimintaan. PE-reititin lisää RD-arvon siinä vaiheessa, kun asiakkaalta mainostuva reitti lisätään BGP-tauluun ja siitä tulee VPN-reitti.

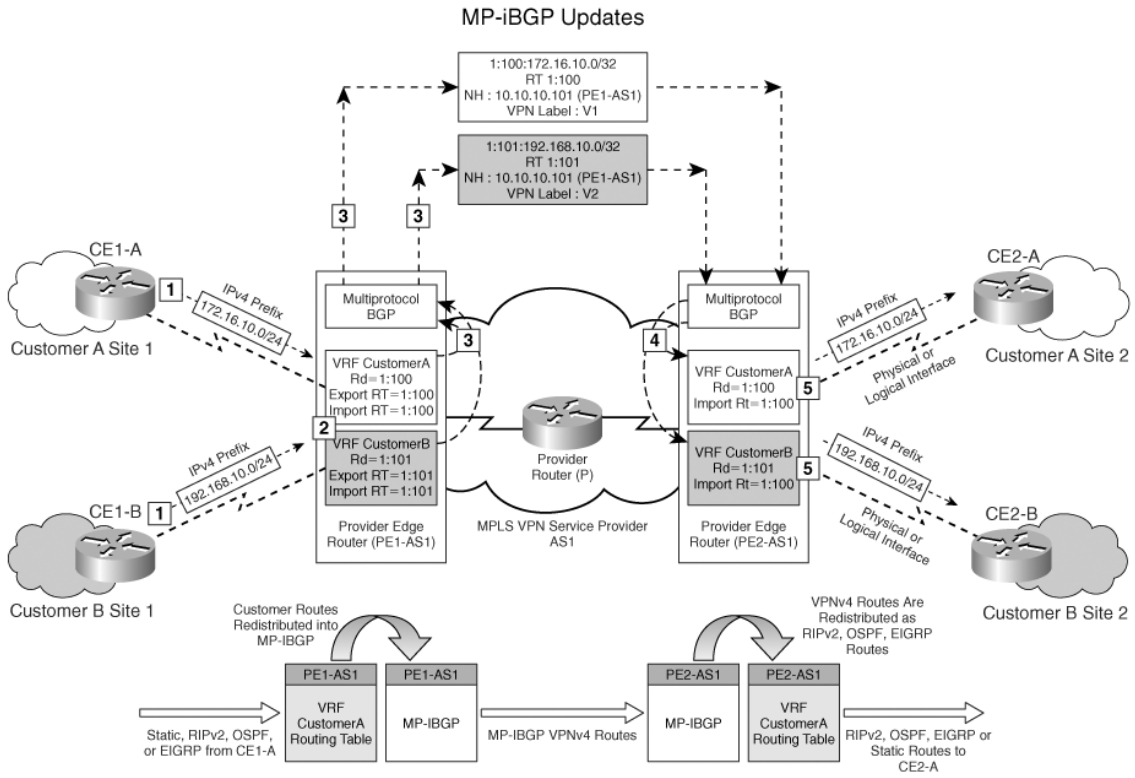
Jokainen PE-reititin MPLS-verkossa tarvitsee yksikäsitteisen tunnisteen (RID, Router-ID), jota käytetään pakettien vastaanottoon ja lähetykseen. Yleisesti RID-tunnisteena käytetään suurinta reitittimeen konfiguroitua 32-bittistä loopback-osoitetta. Jos loopback-osoitetta ei ole asetettu, Router-ID:ksi tulee suurin reitittimen liitynnän osoite.

3.4.3 Route Target, RT

Kun VPN:n tunnisteena käytetään pelkästään RD:tä, eri VPN:n välinen kommunikaatio on vaikeaa. Esimerkiksi yrityksen A toimipiste ei voisi kommunikoida yrityksen B toimipisteen kanssa, koska ne toimivat eri RD-tunnisteilla. Tätä varten kehitettiin Route Target -tunnisteet (RT), jotka kertovat, mitkä reitit pitää vastaanottaa toiselta VPN:ltä. RT muodostetaan BGP:n extended communities -attribuutin avulla lisäämällä sen ylimpiin 16 bittiin tieto VPN-jäsenyydestä.

Kuva 15 näyttää, miten RT ohjaa tietoa, mitkä VPN-reititystaulut importoidaan (tuodaan) PE-reitittimiltä ja mitkä VPN-reititystaulut exportoidaan (viedään) muihin laitteisiin. [11.]

1. Reitittimeltä CE1-A tulee prefiksi 172.16.10.0/24, joka kuuluu Customer A:n VRF-tauluun reitittimellä PE1-AS1.
2. PE1-AS1:ssä Customer A:n VRF-taulussa ovat RD 1:100 ja export RT 1:100.
3. Reitittimeltä CE1-A opitut reitit välitetään MP-BGP-prosessissa niin, että prefiksin 172.16.10.0/24 eteen liitetään RD 1:100 ja oerään export RT 1:100 ennen lähettämistä MP-iBGP-päivityksessä PE-reitittimille.
4. PE2-AS1 saa MP-BGP-päivitykset ja reitti talletetaan Customer A:n VRF-tauluun.
5. MP-BGP-reitit välitetään CE2-A:lle.



Kuva 15. RD- ja RT-periaatekuva. [11.].

3.5 MPLS ja IPv6

Siirtyminen IPv4:stä versioon kuusi on edessä jossain vaiheessa, sillä vapaat IPv4-osoitteet ovat loppumassa. IP-osoitteiden jakamisesta vastaava Internet Assigned Numbers Authority (IANA) jakoi helmi-kuussa 2011 viimeiset /8-prefiksiin osoitealueet alueellisille organisaatioille (Regional Internet Registry, RIR). Toistaiseksi RIR-organisaatioilla riittää vielä osoitteita, mutta nekin tulevat pian loppumaan.

Todennäköisin toimintatapa siirtymisessä on migraatio, jossa IPv6 MPLS VPN -yhteydet toteutetaan olemassa olevassa IPv4-verkossa. Raskaampi vaihtoehto on päivittää verkko heti IPv6-tasolle.

Yksinkertaisin migraatioratkaisu on tunneloida IPv6-yhteydet IPv4 MPLS VPN -yhteyksien läpi. Se edellyttää, että CE-reitittimissä on kaksoispino (dual-stack), eli niissä ovat rinnakkaiset IPv4- ja IPv6-protokollat, ja IPv6-liikenne tunneloidaan niiden välillä VPN-yhteyden yli.

Käyttökelpoisin menettely on 6PE-malli, jossa vain PE-reitittimet ovat dual-stack-tilassa, eikä P-reitittimiin tarvitse tehdä muutoksia. MP-iGP-protokolla hoitaa IPv6-prefiksien ja niihin liittyvien lippujen levityksen PE-laitteiden välillä. IPv6-paketteihin tulee kaksi lippua, alimmaiseksi BGP-protokollan jakama lippu ja ylimmäiseksi IGP-protokollan lippu. Edellistä käytetään PE-reitittimillä IPv6-prefiksin selvittämiseen ja jälkimmäisen avulla paketti kuljetetaan MPLS-verkon läpi.

4 Palvelun laatu, Quality of Service (QoS)

Quality of Service (QoS), palvelun laatu, on määritelmä, jolla on monia merkityksiä. Usein QoS:n tarkoituksena on taata siedettävä palvelutaso riittävän datasiirron osalta. Jotkin palvelut kuten VoIP, videokonferenssisovellukset sekä suoratoistosovellukset (striimaus, streaming) taas vaativat tietyn minimikaistan toimiakseen.

QoS-tekniikat poikkeavat normaalisti verkoissa käytettävästä ns. Best Effort -mallista, jossa verkko yrittää parhaansa mukaan toimittaa paketit perille ilman varsinaisia laatutakuita. QoS-menettelyissä käytössä olevista verkkoresursseista pidetään kirjaa ja tietyt liikenneluokat asetetaan prioriteetiltaan eri tasoille palvelutason mukaan. QoS-tekniikoita on kahdenlaisia. Luokittelutekniikat keskittyvät QoS-tiedon jakamiseen ja liikenteen luokitteluun, kun taas suodatintekniikat ovat erilaisia algoritmeja itse reitittimissä, jotka toteuttavat itse suodatusta ja priorisointia.

Tässä työssä QoS:llä tarkoitetaan resurssien varaamismekanismeja sekä työkaluja, joilla pyritään takaamaan palveluille tietty palvelutaso. QoS-työkaluilla tarjotaan eri prioriteetteja sovelluksille, käyttäjille tai liikennevirroille. Työssä keskitytään jonojen käsittelyyn ja liikennevirtojen priorisoimiseen niiden luokituksien perusteella.

4.1 QoS-luokat

QoS-käsittely voidaan jakaa kahteen alakategoriaan palvelutason perusteella: palveluluokkaan ja palvelun tyyppiin. Palveluluokilla määritetään sovelluskohtaisesti kaistanleveyksiä ja viiveitä verkossa. Käytännössä se tapahtuu siirtoyhteyskerroksessa IEEE 802.1Q -kehyksen (vrt. kuva 2) otsikkokentän kolmella CoS-bitillä. Niiden avulla voidaan ilmaista 7 erilaista palveluluokkaa, joista luokka 7 on prioriteetiltaan korkein. Eri liikennetyypit kategorisoidaan palveluluokkien sisään, jolloin

tietoliikennevaatimuksiltaan samankaltainen liikenne voidaan käsitellä yhtenä ryhmänä. Koska data kapseloidaan ylemmältä verkkokerroksilta alaspäin mentäessä, CoS-määritykset eivät vaikuta reitittimien QoS-politiikkaan, mutta saattavat olla käyttökelpoisia L2-tason kytkinverkoissa.

Joissain järjestelmissä verkkokerroksen priorisointitieto voidaan siirtää kytkimessä siirtoyhteyskerrokselle, mikä mahdollistaa ennalta määritellyn joukon liikennetyyppejä. Ciscon kytkimissä tästä käytetään nimitystä Auto-QoS, Kun toiminto otetaan käyttöön, pakettien luokittelu ja merkintä astuu voimaan taulukon 2 mukaisesti.

Taulukko 2. Liikennetyypit, pakettimerkintä ja jonot. [14.]

	VoIP[1] Data Traffic	VoIP Control Traffic	Routing Protocol Traffic	STP BPDU Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP	46	24, 26	48	56	34	-	
CoS	5	3	6	7	4	-	
CoS-to-Ingress Queue Map	2, 3, 4, 5, 6, 7 (queue 2)					0, 1 (queue 1)	
CoS-to-Egress Queue Map	5 (queue 1)	3, 6, 7 (queue 2)			4 (queue 3)	2 (queue 3)	0, 1 (queue 4)

[1] VoIP = voice over IP

Palvelun tyyppimäärittelyt suoritetaan verkkokerroksessa. Palvelun tyyppi (ToS) -kenttää IPv4-otsakkeessa (ks. kuva 3) ja Luokka (TC) -kenttää IPv6-otsakkeessa (ks. kuva 4) käytetään IP-pakettien luokitteluun. Sen avulla reitittimet voivat tehdä QoS-päätökset siitä, kuinka paketit välitetään verkossa.

Alkuperäisessä IPv4-määrittelyssä RFC791:ssä ToS-kentän ensimmäiset kolme bittiä (precedence) määriteltiin liikenteen luokitteluun ja merkkaukseen. Seuraavat neljä bittiä sisältävät toivomuksen palvelulaadusta. Vaikka ToS on ollut mukana TCP/IP:ssä alusta lähtien, sitä ei käytännössä ole juurikaan käytetty. Sen sijaan edistyneemmät tekniikat, kuten DiffServ ja RSVP, voivat käyttää kenttää hyväkseen.

IPv6:ssa IPv4:n ToS-bitit on korvattu TC-kentän prioriteettibiteillä, joiden arvo määrää eri pakettien prioriteetin (ks. taulukko 1). Selkeä parannus on vuon Vuonimiö (Flow

Label) -kenttä, jonka avulla reitittimissä voidaan ohjata paketteja vuon tunnisteen mukaan, eikä paketin kohdeosoitteen perusteella tehtävää seuraavan solmun hakemista tarvitse tehdä.

4.2 QoS-mallit

QoS-malleja on käytössä kolme:

- Best Effort
- Integrated Services (IntServ)
- Diffrentiated Services (DiffServ).

4.2.1 Best Effort -malli

Best Effort -mallissa, ei käytetä QoS-työkaluja ollenkaan, vaan kuten nimikin kertoo, paketit pyritään toimittamaan määränpäähänsä kaikilla mahdollisilla keinoilla. Kuitenkaan Best Effort -mallia käytettäessä ei ole takeita siitä, että paketti saapuu koskaan aiottuun määränpäähän, vaan kaikki paketit käsitellään samanarvoisesti ja siirtonopeus sekä viive ovat ennalta-arvaamattomia. Dataa voidaan lähettää aina, kun tarvitaan ilman, että verkolle erikseen ilmoitetaan tai pyydetään siihen lupaa. Tietyt sovellukset voivat toimia hyvin tätä mallia käytettäessä, esimerkkeinä FTP tai HTTP. Tämä ei kuitenkaan ole optimaalinen malli palveluille, jotka ovat herkkiä pakettien häviämiselle, verkon viiveelle ja viiveen vaihteluille. Verkoissa on sovelluksia, jotka vaativat yhdenmukaisen määrän kaistanleveyttä toimiakseen kunnolla. Jos verkossa ei ole käytössä QoS-menetelmiä, tämä on oletusmalli kaikelle liikenteelle.

4.2.2 Integrated Services, IntServ

Integrated Services -mallilla (yhdistetyt palvelut -malli) voidaan taata korkean luokan palvelutaso IP-paketeille alusta loppuun. Verkon resurssit varataan ennakolta ennen liikenteen välittämistä. Paketteja ei välitetä, ennen kuin verkolta saadaan lupa ja tieto, että liikenne pystytään välittämään päämääräänsä sovitulla palvelutasolla. IntServ-palvelu toteutetaan Resource Reservation (RSVP) -protokollalla, jolla yhteyden resurssien varaukset tehdään dynaamisesti. Dynaamisuus tarkoittaa sitä, että yhteyden ominaisuuksia voidaan muuttaa tarvittaessa yhteyden aikana ilman koko varausoperaation tekemistä uudestaan. RSVP toimii IPv4- ja IPv6-verkoissa. Oletus

kuitenkin on, että TCP-protokollan sijasta käytetään RTP (Real-time Transfer Protocol) -protokollaa, joka tarjoaa paremman tuen QoS:n käytölle.

RSVP-protokolla estää pakettien välittämisen verkon ollessa varattu, eikä verkko lähetä signaalia sovellukselle, jos pyynnön palvelutasoa ei voida taata. Kun sovellus alkaa lähettää liikennettä, verkon resursseja on varattu sovelluksen käyttöön päästä päähän. Niitä ylläpidetään niin kauan, että sovelluksen ajama liikenne loppuu. Jos verkko ei pysty varaamaan pyydettyjä resursseja, joita ovat tarvittava siirtonopeus, viive sekä maksimipakettihäviö, paketteja ei lähetetä ollenkaan.

RSVP:n avulla voidaan varata tietyt resurssit yhteyskohtaisesti datan välittämiseen. Se ei sovi kovin hyvin lyhytkestoisten ja purskeisten yhteyksien perustamiseen yhteyden perustamiseen kuluvan ajan vuoksi. Lisäksi RSVP sopii parhaiten lähinnä pieniin intranetympäristöihin, joissa varattujen yhteyksien määrä on pieni. [9.]

4.2.3 Diffrential Services, DiffServ

Differential Services (DiffServ) -malli eli eriytetyt palvelut -malli tarjoaa karkeammat ja skaalautuvammat mekanismit kuin edellä mainitut Best Effort- ja Integrated Services -mallit. DiffServ on palveluiden luokitukseen perustuva menetelmä, jossa verkossa liikkuviin paketteihin liitetään palveluluokkatieto, jonka perusteella paketit käsitellään verkon reitittimissä eri tavalla. DiffServ ei siis perustu yhteydellisyyteen kuten IntServ, vaan kaikki verkossa liikkuvat paketit käsitellään samojen sääntöjen perusteella.

DiffServ toimii ennalta määrätyn QoS-rakenteen mukaan, jossa liikenne jaetaan eri luokkiin sen saapuessa verkon alueelle. Hypyn yli käyttäytyminen (Per-Hop Behavior, PHB) paketeille suoritetaan verkon sisäisissä reitittimissä, kun ne kulkevat verkon lävitse. Luokittelu (classification) voidaan tehdä minkä tahansa standardin tai laajennetun pääsylistan perusteella. Pääsylistoissa tarkastellaan osumia (match condition) esimerkiksi lähde-IP- tai kohde-IP -osoitteen, protokollan ja porttien perusteella. Eri luokille tarjotaan siten verkosta eritasoista palvelua. Esimerkiksi ääniliikenteelle annetaan usein korkein prioriteetti sen vaatiman pienen viiveen ja viiveen vaihtelun vuoksi, kun taas sähköpostiliikenteelle tarjotaan vain Best Effort -luokiteltua palvelua. Kaikelle yritykselle tarpeettomalle tai vähempiarvoiselle liikenteelle voidaan tarjota hyvin pieni palvelutaso tai mahdollisuus estää tämä liikenne kokonaan.

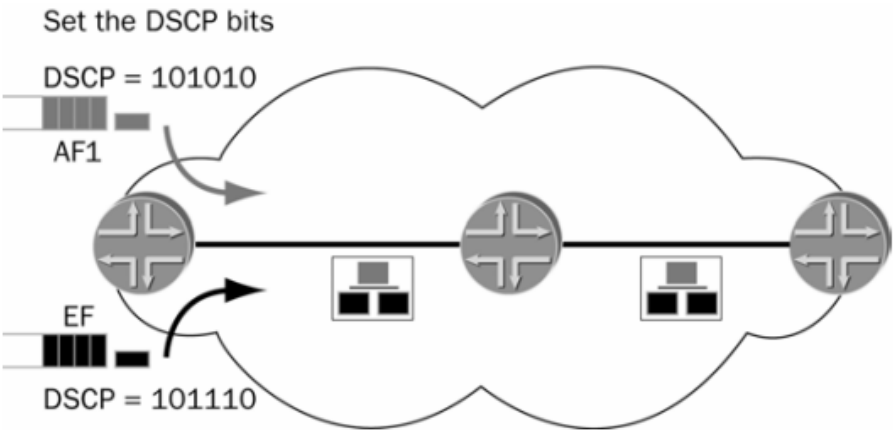
Taulukossa 3 on kuvattu DiffServ-mallin toimintaketju liikenteen luokittelussa ja sen perusteella tehtävistä toimenpiteistä.

Taulukko 3. DiffServ-mallin mukainen QoS-toimintaketju ja vaihtoehdot. [16.]

Match Conditions Keyword: Class-Map	Policy Actions Keyword: Policy-Map		
Classification (luokittelu)	Ennen jonoon asettamista (Pre-Queuing)	Jonotus ja järjestely (Queuing and Schedul-ing)	Jonotuksen jälkeiset toimet (Post-Queuing)
Liikenteen luokittelu (Classifify Traffic)	Välittömät toimet (Immediate Actions)	Ruuhkan hallinta ja välttäminen (Congestion Management and Avoidance)	Linkin tehostusmekanismit (Link Efficiency Mechanisms)
Osumat (Match one or more attributes) • Access Control List (ACL) • COS • Differentiated Ser-vices Code Point (DSCP) • Tuloliitäntä • Media Access Control (MAC) -osoite • Paketin pituus • Presedenssi • Protokolla • VLAN	QoS-asetukset (Set QoS values) • Police • Drop • Count • Estimate bandwidth	• Queue-limit • Random-detect • Bandwidth • Fair-queue • Priority • Shape	• Otsakkeen pakkaus (Compress header) • Fragmentointi (link fragmentation and interleaving, Layer 2)

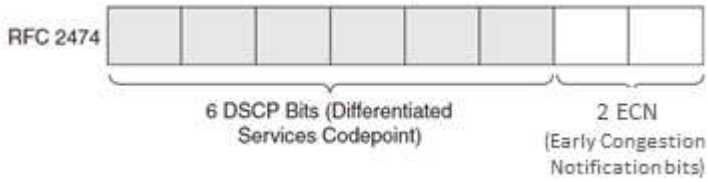
DiffServ on tehokkaasti skaalautuva, useita erilaisia sovelluksia tukeva ja vähän reitittimien muistia ja suorituskykyä vaativa toteutus, koska sisäänpääsypolitiikan käyttäminen, liikenteen luokittelu, muotoilu, mittaaminen ja merkintä on siirretty reunareitittimille.

Kuvassa 16 on esitetty toiminta paketin saapuessa verkkoon.



Kuva 16. DiffServ-alue. Äänidata (alempi vuo) saa saapuessaan DSCP-merkinnän EF ja muu datamerkinnän BE. [12.]

DiffServ-malli käyttää IPv4 Palvelun tyyppi -kentän (IPv6:n Luokka-kentän) kuutta ensimmäistä bittiä liikenteen luokittelussa. Kentän osaa kutsutaan nimellä DSCP (Differentiated Services Code Point). Kuuden bitin avulla voidaan määritellä yhteensä 64 palveluluokkaa, kun aikaisemman käytännön avulla saatiin vain kahdeksan luokkaa. Kentän kolme ensimmäistä bittiä muodostavat pääluokan (major) ja kolme keskimmäistä bittiä alaluokan (minor). Kentän kaksi viimeistä bittiä on varattu vuonohjauksen käyttöön ja niistä käytetään nimitystä ECN (Early Congestion Notification). Yhteensopivuus vanhojen reitittimien kanssa on saavutettu sopimalla normaalin Best Effort -käsittelyn paketin Palvelun tyyppi -kentän arvon olevan nolla.



Kuva 17. DiffServ-kentän rakenne. [9.]

DiffServ-kentän kolme ylintä bittiä määrittelevät prioriteettitasot. Niiden avulla voidaan ilmaista 8 arvoa. Arvo 0 määrittelee Best Effort -käytännön, mikä siis antaa yhteensopivuuden nykyisiin sovelluksiin. Arvo 5 määrittelee Expedited Forwarding (EF) -luokan, oletettava välittäminen, joka on toinen DiffServ-mallissa määritelty välitysluokka. EF-luokalle taataan pieni viive ja latenssi, vähäinen pakettien poisto ja pieni viiveen vaihtelu polun päästä päähän. Prioriteettiarvot on esitetty taulukossa 4.

Taulukko 4. DiffServ-prioriteetit

Prioriteetti (Precedence Level)	Kuvaus
7	Pysyy samana (siirtoyhteyskerros ja reititysprotokollat)
6	Pysyy samana (IP-reititysprotokollat)
5	Express Forwarding (EF)
4	Class 4
3	Class 3
2	Class 2
1	Class 1
0	Best Effort

Toinen välitysluokka, Assured Forwarding (AF) eli varmistava välittäminen sisältää prioriteettiluokat 1−4, jotka on esitetty DSCP-kentän ylimmillä kolmella bitillä (ks. taulukko 4). AF-luokat ovat AF1x−AF4x, missä x saa arvot 1−3 ja määrittelee pakettien pudottamistodennäköisyydet (drop probability). Bitit x ovat DSCP-kentän prioriteettibittejä seuraavat kaksi bittiä. Kentän alin bitti on aina nolla. Mitä suurempi kiireellisyysarvo AF-luokalla on, sitä vähemmän luokkaa priorisoidaan. AF-luokitukset on esitetty taulukossa 5.

Taulukko 5. AF-luokitukset.

Drop	**Class 1**	**Class 2**	**Class 3**	**Class 4**
Alhainen (low)	**001**010 AF11 DSCP 10	**010**010 AF21 DSCP 18	**011**010 AF31 DSCP 26	**100**010 AF41 DSCP 34
Keskitaso (Medium)	**001**100 AF12 DSCP 12	**010**100 AF22 DSCP 20	**011**100 AF32 DSCP 28	**100**100 AF42 DSCP 36
Korkea (High)	**001**110 AF13 DSCP 14	**010**110 AF23 DSCP 22	**011**110 AF33 DSCP 30	**100**110 AF43 DSCP 38

Verkon rajalla reitittimet pitävät huolen siitä, ettei asiakkailta päästetä enempää liikennettä kussakin luokassa verkkoon, kuin mistä on maksettu. EF on ainoa luokka, jolle normaalisti annetaan priorisoitu kohtelu jokaisessa reitittimessä. Tarkoitus on, että EF-ryhmä saa sellaista palvelua, jollaista kiinteä linja toimittaisi; kapasiteetti on aidosti varattu, ja viive on vakio, mutta ylimenevä liikenne tippuu linjalta. Muille luokille linkkien kapasiteetti yksinkertaisesti jaetaan jossain suhteessa, mutta viiveelle ei anneta takeita.

Muiden kuin EF-ryhmän kohdalla kyse on siis useasta rinnakkaisesta Best Effort -verkosta. Ei tarvita neljää linkkiä, vaan neljä loogista palveluluokkaa. Ratkaisu on skaalautuva, sillä runkoreitittimien ei tarvitse pitää kirjaa kuin 4 luokasta.

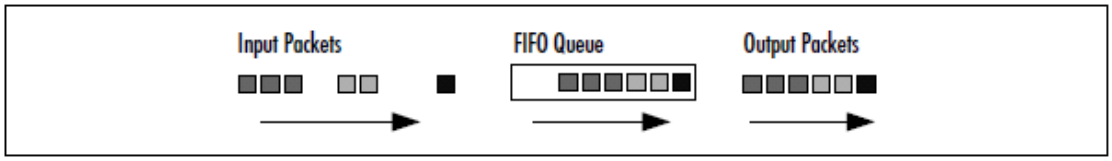
DiffServ-mallin toimintaa voisi verrata perinteiseen postipakettipalveluun. Ostetaan lähetykselle tietyn palvelutason palvelu, kun paketti postitetaan. Koko paketin matkan pyydetty taso tunnistetaan ja lähetys saa joko kuriiripalvelua tai menee normaalin postin mukana. DiffServ-malli tarjoaa parhaan skaalautuvuuden ja joustavuuden QoS:n käytössä. Verkkolaitteet tunnistavat liikenteen eri luokat ja tarjoavat eri palvelutasoja eri liikennetyypeille. Tämä malli onkin tällä hetkellä ylivoimaisesti suosituin käytössä olevista malleista. [9.]

4.3 Jonotus ja ruuhkanhallinta

Liikenteen- ja ruuhkanhallintaa tapahtuu sekä kuljetuskerroksen palveluissa että reitittimissä. Tässä tarkastellaan reitittimissä käytettyjä menettelyitä. Normaalisti paketit lähtevät reitittimestä siinä järjestyksessä, kuin ne ovat sinne saapuneetkin. Jos jono täyttyy, paketit joudutaan hylkäämään. Käsittelyjärjestystä voidaan muuttaa palvelutason parantamiseksi. Tähän jonojen hallintaan on useita erilaisia menetelmiä. Seuraavassa vuo tai virta (flow) tarkoittaa sarjaa peräkkäisiä toisiinsa kuuluvia IP-paketteja.

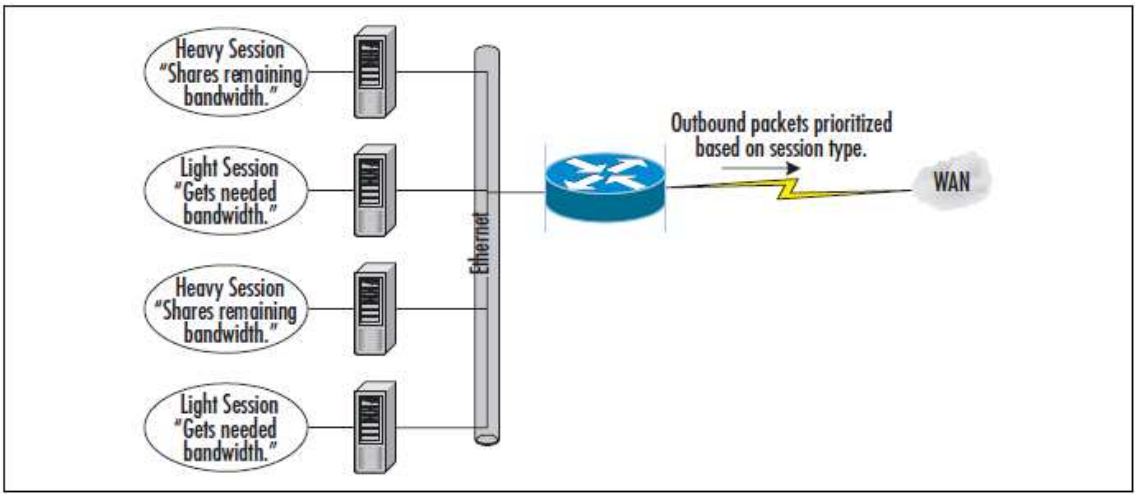
4.3.1 Pakettien hallinta

Pakettien hallinnalla (scheduling, jononhallinta) tarkoitetaan seuraavaksi reitittimestä edelleen lähetettävän paketin valintaa. First In First Out (FIFO) -jonomalli on oletusmenetelmä, jossa ensimmäisenä tullut paketti myös lähtee ensimmäisenä. FIFO tasoittaa hyvin purskeita, kun kuormitus on alhainen. Nykyaikainen liikenne edellyttää kuitenkin priorisointia. Palvelunlaatu ei voi toteutua, jos paketit ruuhkautuvat reitittimissä ja korkean prioriteetin saaneet paketit joutuvat odottelemaan jonoissa. Jos jono täyttyy, kaikki paketit hylätään.



Kuva 18. FIFO-jono. [6.]

Reilu jono -menettelyssä (Fair Queuing, FQ) pienet paketit lähtevät ennen isoja. Painotettu reilu jono -menettely (Weighted Fair Queing, WFQ) on edellisen kaltainen, mutta kapasiteettia jaetaan liikenteen määrän perusteella. Pienikapasiteettiselle liikenteelle annetaan etusija ja loppukapasiteetti jätetään suurikapasiteettiselle liikenteelle. Liikenne jaetaan virtoihin ja jokainen virta sijoitetaan jonoon liikenteen määrän perusteella. Etuna tässä on, että yksi virta ei tuki kaikkea liikennettä. Huonoja puolia ovat laskennasta aiheutuva ylimääräinen kuorma ja luokittelun määritteleminen.

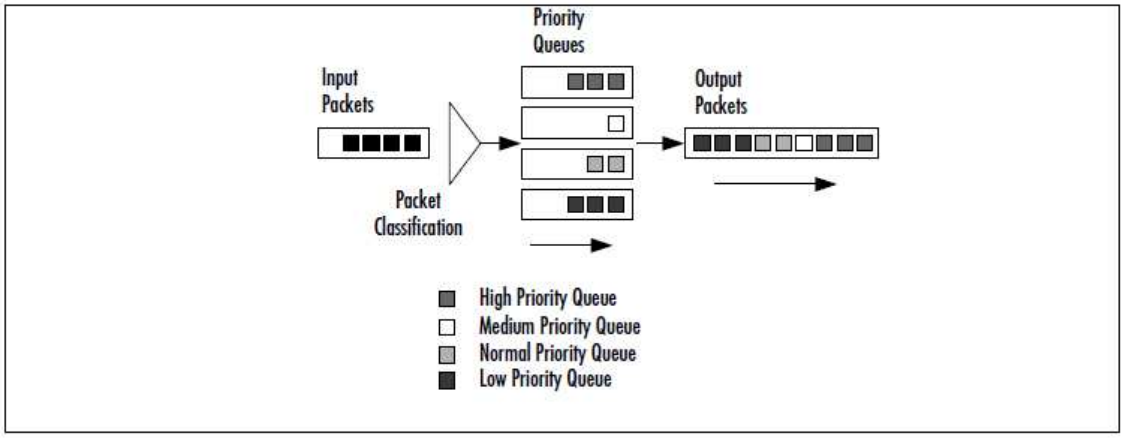


Kuva 19. Painotettu reilu jono. [18.]

Luokkiin perustuva jonomalli (Class Based WFQ, CBWFQ) muistuttaa edellistä, mutta ylläpitäjä voi määritellä vuot ja se, miten liikenne niihin jaetaan. Ruuhkatilanteissa tietylle liikenteelle taataan tietty kaista. Se on yksinkertainen tapa jakaa liikennettä eri palveluluokkiin. Toisaalta menetelmä skaalautuu heikosti, jonojen ohjaus saattaa hidastaa nopeaa liikennettä.

Alhaisen viiveen jono -menettely (Low Latency Queuing, LLQ) on painotetun reilun jonomallin muunnos, jossa liikenteelle taataan aina tietty kaista.

Prioriteettijonokäsittely (Priority Queuing, PQ) on yksinkertainen tapa järjestellä pakettien välitysjärjestystä. Siinä esimerkiksi reaaliaikaiselle liikenteelle voidaan antaa korkea prioriteetti. Pakettien luokittelu generoi kuitenkin ylimääräistä kuormaa.



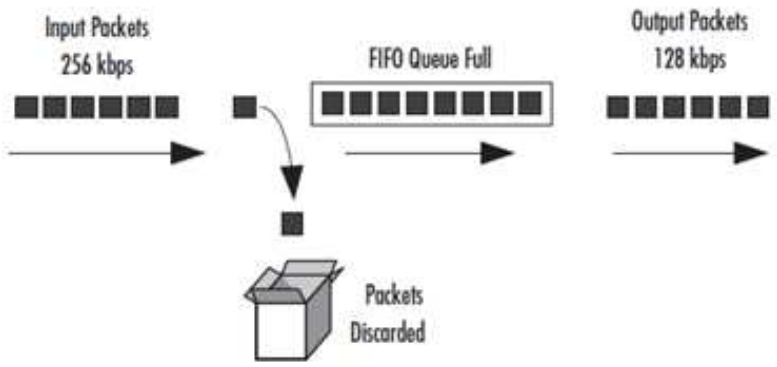
Kuva 20. Prioriteettijono. [6.]

Liikennetyyppikohtaisessa (Custom Queuing, CQ) jokaiselle liikennetyypille annetaan tietty prosenttiosuus kaistasta.

4.3.2 Ruuhkan hallinta

Jos reitittimen tai kytkimen liitäntä ruuhkautuu ja jonot alkavat täyttyä, tarvitaan ruuhkan hallintaa poistettavien pakettien valintaan. Ainoa pakollinen ruuhkanhallintamekanismi internetissä on Source Quench (SQ). Reititin, joka joutuu karsimaan liikennettä, lähettää tiedon siitä ICMP Source Quench -sanomalla lähettävälle päätelaitteelle, jonka tulisi reagoida pienentämällä lähetysnopeuttaan. Ongelmana on, että ICMP-sanomat käsitellään IP:n päällä omana kokonaisuutenaan, eikä niillä ole yhteyttä yhteysprotokollaan.

Reititintasolla on neljä perusmenetelmää, jotka on käyty lyhyesti läpi seuraavassa.
Tail Drop (TD) eli häntäkarsinta on yksinkertaisin menettely. Siinä FIFO vuotaa yli ja pitää samalla liikenteen kurissa. Ylivuotava liikenne generoi SQ-sanomia lähettäville päätelaitteille, ja vastaanottavat laitteet reagoivat uudelleenlähetyspyynnöillä. Ongelmina Tail Drop -menettelyssä ovat painotus tasaiselle liikenteelle, tukkeutumisen aiheuttama heijastusefekti verkossa ja ongelmat reaaliaikaisen liikenteen kanssa suurilla puskureilla.



Kuva 21. Tail Drop [9.]

Random Drop (RD) eli satunnaiskarsinta perustuu olettamukseen, että paketti, joka valitaan satunnaisesti, kuuluu lähteelle todennäköisyydellä, joka on suoraan verrannollinen lähteen keskinopeuteen. Pois tiputettava paketti valitaan nyt jonon sisältä eikä hännältä. Koska menetelmä on satunnainen, myös ne yhteydet, jotka kuluttavat alle osuutensa resursseista, kärsivät pakettihukkaa.

Random Early Detection (RED) on edellisen muunnos. Kun puskuri täyttyy tiettyyn rajaan asti, paketteja aletaan pudottaa satunnaisesti. Kun ns. maksimiraja-arvo on saavutettu, pudotetaan kaikki uudet paketit, kuten Tail Dropissa.

Weighted RED (WRED) asettaa raja-arvot, kuten RED, mutta ymmärtää myös CoS-asetuksia. Esim. CoS-arvoille 0 ja 1 asetetaan raja-arvoksi 50 % ja CoS-arvoille 2 ja 3 80 %. Kun puskurista 50 % on täynnä, aletaan pudottaa satunnaisesti paketteja, joiden CoS-arvo on 0 tai 1. Puskurin täytyttyä 80-prosenttisesti pudotetaan satunnaisesti myös paketteja CoS-arvoilla 3 ja 4. [15.]

4.4 QoS-ratkaisun suunnittelu

QoS-ratkaisun suunnittelu lähtee aina halutun liikenteen ominaisuuksista ja käytettävien verkkojen rakenteen ja toiminnan selvittämisellä. Liikenteen laadun perusteella määritellään luokat palvelunlaatua varten. Verkkojen rakenteen perusteella taas suunnitellaan ja toteutetaan käytettävät ratkaisut.

Suunnittelun aloituksen vaiheet ovat seuraavat:

- Määritellään liikenteen luokat. Mitkä niistä ovat tärkeitä? Mitkä ovat vaatimukset liikennemäärien suhteen? Mitkä voidaan jättää käsittelyn ulkopuolelle? Mitkä ovat tulevaisuuden laajentumisnäkymät (skaalautuvuus)?
- Määritellään menettelytavat (policies) luokille. Mitä liikenteelle tehdään? Millä tasolla ratkaisut toteutetaan (L2 vai L3)?
- Riittääkö nykyinen laitteisto, vai onko hankittava uusia aktiivilaitteita? Voidaanko linjanopeuksia ja suorituskykyä kasvattaa?

Esisuunnitteluprosessi jakautuu viiteen pääosaan, jotka ovat:

- liiketoimintasuunnittelu
- pitkän- ja keskipitkän tähtäyksen verkkosuunnittelu
- lyhyen tähtäimen verkkosuunnittelu
- IT-suunnittelu
- käytön ja ylläpidon suunnittelu. [17]

Varsinainen verkkosuunnittelu on kolmivaiheinen prosessi:

- topologiasuunnittelu
- verkkosuunnittelu
- verkon toteuttaminen. [17.]

Keskeisiä suunnittelussa huomioon otettavia asioita ovat

- verkon laitteet
- asiakasverkkojen liitäntä runkoverkkoon
- verkon topologia
- käytettävät osoitteet
- runkoverkon reititys
- asiakasverkkojen reititys
- runkoverkon toiminnan verifiointi.

QoS-suunnittelussa on tärkeää varmistaa, ettei yhden luokan priorisointi aiheuta ongelmia muiden, etenkään yritykselle tärkeiden, luokkien liikenteelle. On myös vältettävä yli-investointeja; käypä perusratkaisu kannattaa aina selvittää ennen investointipäätöksiä.

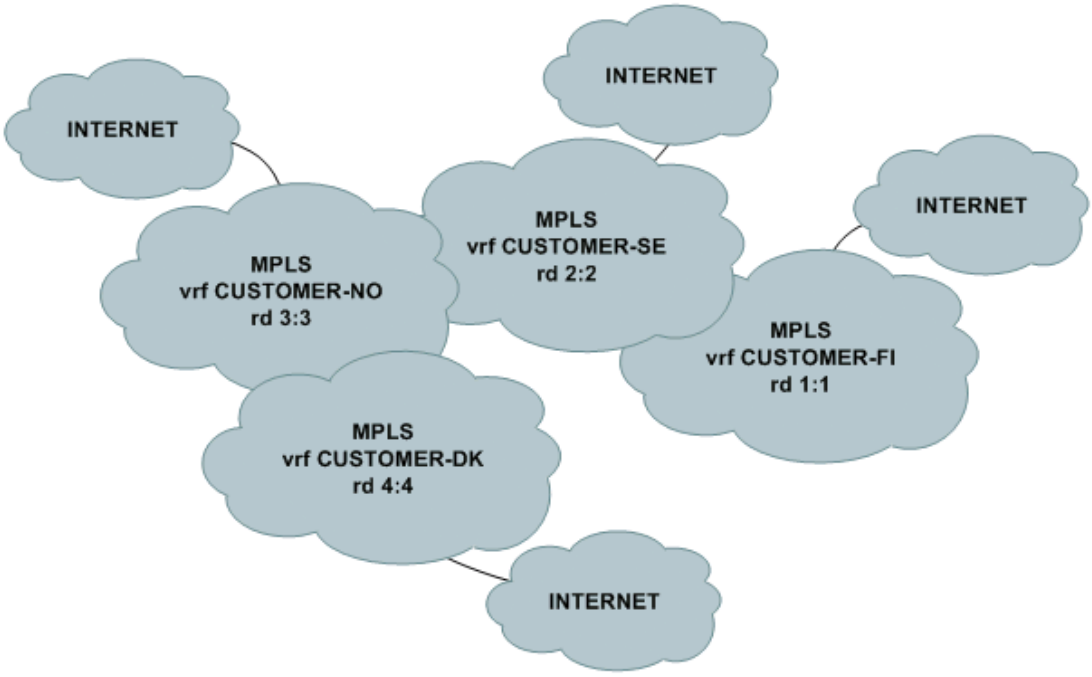
5 Yrityksen verkon päivittäminen

Työn kohteena on yritys, jolla on toimipisteitä Suomessa, Ruotsissa, Norjassa ja Tanskassa. Tässä työssä keskitytään Suomen verkkotopologiaan tehtäviin muutoksiin. Verkot on rakennettu kaikissa maissa samalla lailla. Myös priorisoinnin toteutus on samanlainen jokaisessa maassa.

Kuva 22. Yrityksen toimipisteet kartalla.

5.1 Verkon rakenne

Yrityksen MPLS-verkko on jaoteltu maantieteellisesti. Suomen rd-tunnus on 1:1. Ruotsin, Norjan ja Tanskan verkoilla on omat rd-tunnuksensa. Yrityksen verkon looginen rakenne on esitetty kuvassa 23.



Kuva 23. Yrityksen MPLS-verkkorakenne.

Jokaisella maalla on oma internet-liittymänsä ja näin ollen oma oletusreittinsä. Verkot viedään ja tuodaan vrf:ien välillä import- ja export-komennoilla, kuitenkin huomioon ottaen että maakohtaiset oletusreitit eivät saa mainostua kyseessä olevan maan ulkopuolelle.

```
ip vrf CUSTOMER-FI
 rd 1:1
 import map default-import
 route-target export 1:1
 route-target export 2:2
 route-target export 3:3
 route-target export 4:4
 route-target import 1:1
 route-target import 2:2
 route-target import 3:3
 route-target import 4:4
```

Oletusreittien suodatus vrf:ien välillä tehdään route-map-komennoilla:

```
route-map default-import permit 100
 match extcommunity customer-fi
route-map default-import deny 200
 match ip address prefix-list default
route-map default-import permit 300
```

Route-mapiin liitetään asiakkaan rt 1:1. Tämän jälkeen kielletään muista rt:stä mainostuvat default-reitit.

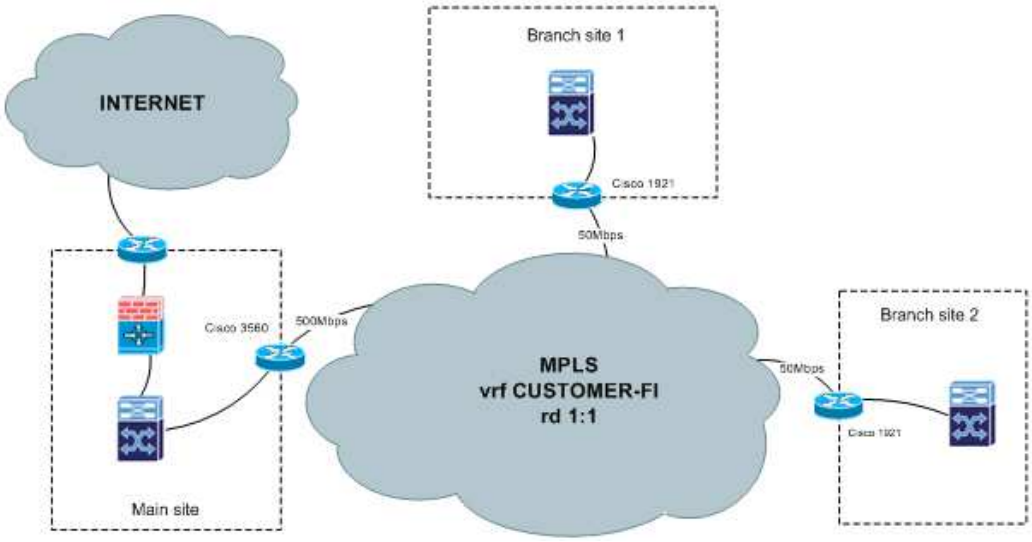
```
ip extcommunity-list standard customer-fi permit rt 1:1
!
ip prefix-list default seq 5 permit 0.0.0.0/0
```

5.1.1 Verkon kriittiset sovellukset

Verkon käyttäjät käyttävät hyvin viivekriittisiä keskitettyjä tietojärjestelmiä sekä IP-puhelinjärjestelmää ja IP-puhelimia. Niiden käytössä on esiintynyt sekä suoristukyky- että laatuongelmia, joiden poistamiseksi tämä hanke käynnistettiin.

5.2 Verkon fyysinen rakenne

Yrityksen verkon fyysinen rakenne Suomen osalta on esitetty kuvassa 24.



Kuva 24. Fyysisen verkon rakenne.

Päätoimipisteen (Main site) liityntänopeus on 500 Mbps. Muiden yhteyksien nopeus on 50 Mbps. Päätoimipaikan asiakaspäätelaitteena käytössä L3-tason Cisco 3560 -kytkin, etätoimipisteillä Cisco 1921 -reitittimet. Liityntätyyppinä yhteyksissä käytetään

valokuitua, joko SFP- tai Ethernet-rajapinnalla. Yrityksen internet-yhteys, internet-palomuuri ja niiden hallinta ovat toisen operaattorin hoidossa.

Koska verkon laitteet ja linjat ovat ajanmukaiset ja toimivat, ne päätettiin säilyttää sellaisinaan.

5.3 Uudistukset ja uuden verkon looginen rakenne

Quality of Service -määittelyiden suunnittelu aloitettiin neuvottelulla asiakkaan kanssa, jossa käytiin läpi eri vaihtoehtoja ja sovittiin käytettävistä menettelyistä. Vakiotarjontaan kuuluvat vaihtoehdot on esitetty taulukossa 6.

Taulukko 6. Liikennöintiprofiilit.

Profile	Voice	Video	Data	QoS Basic	QoS Advanced
1	25%	0%	0%	x	x
2	25%	25%	0%		x
3	25%	50%	0%		x
4	25%	25%	25%		x
5	25%	0%	50%		x
6	50%	0%	0%	x	x
7	50%	25%	0%		x
8	50%	0%	25%		x
9	75%	0%	0%	x	x
10	5%	25%	25%		x
11	5%	0%	0%	x	x
12	10%	0%	0%	x	x
13	10%	25%	25%		x
14	35%	25%	15%		x
15	20%	0%	0%	x	x

Neuvottelun tuloksena päädyttiin käyttämään profiilia 13, jossa liikenne priorisoidaan seuraavasti:

Luokitus	Prioriteetti
GOLD	10 %
SILVER	25 %
BRONZE	25 %
BEST EFFORT	40 %

5.4 Asiakasyhteydet verkkoon

Asiakkaan toimittama listaus QoS-hierarkioista Suomen osalta on esitelty taulukossa 7:

Taulukko 7. Verkkojen QoS-hierarkiat

Priority class	**Source IP network**	**Destination IP network**	**TCP/UDP port**
GOLD	VoIP	VoIP	
Priority class	**Source IP network**	**Destination IP network**	**TCP/UDP port**
SILVER	ANY	172.25.0.0/24	TCP 80, TCP 1494, TCP 2598
SILVER	ANY	172.25.8.64/26	ANY
SILVER	ANY	172.25.8.192/27	ANY
SILVER	172.22.30.0/24	ANY	ANY
SILVER	172.25.8.160/27	ANY	ANY
SILVER	172.25.81.128/26	ANY	ANY
Priority class	**Source IP network**	**Destination IP network**	**TCP/UDP port**
BRONZE	ANY	172.25.0.0/24	ANY
BRONZE	ANY	172.25.14.0/24	TCP 80, TCP 443
BRONZE	ANY	172.27.0.192/27	TCP 80, TCP 443
BRONZE	ANY	10.158.1.0/24	TCP 80, TCP 443
BRONZE	ANY	10.158.8.0/24	TCP 139, TCP 445
BRONZE	ANY	10.158.26.0/24	TCP 1494, TCP 2598
BRONZE	ANY	10.242.0.0/24	TCP 80, TCP 443

Jokaisen maan osalta toimitettiin vastaavanlainen listaus IP-osoitteiden ja porttien perusteella jaoteltuna. Asiakkaan toimittama listaus käännettiin jokaiselle reitittimelle pääsylistoiksi, joilla hoidetaan liikenteen merkkaaminen DSCP-arvoille. Yrityksen edustajan toiveesta liikenteen paluupaketit käsitellään oletuskäytännön mukaisesti, eikä niille näin ollen aseteta DSCP-arvoa erikseen. Yritys tulee tarkistelemaan tilannetta uudelleen tulevaisuudessa.

```
ip access-list extended CUST-SILVER
permit tcp any 172.25.0.0 0.0.0.255 eq 80
permit tcp any 172.25.0.0 0.0.0.255 eq 1494
permit tcp any 172.25.0.0 0.0.0.255 eq 2598
permit ip any 172.25.8.192 0.0.0.31
permit ip any 172.25.8.64 0.0.0.63
permit ip 172.22.30.0 0.0.0.255 any
permit ip 172.25.8.160 0.0.0.31 any
permit ip 172.25.81.128 0.0.0.63 any
```

```
ip access-list extended name CUST-BRONZE
permit ip any 172.25.14.0 0.0.0.255
permit tcp any 172.25.0.0 0.0.0.255 eq 80
permit tcp any 172.25.0.0 0.0.0.255 eq 443
permit tcp any 172.27.0.192 0.0.0.31 eq 80
permit tcp any 172.27.0.192 0.0.0.31 eq 443
permit tcp any 10.158.1.0 0.0.0.255 eq 80
permit tcp any 10.158.1.0 0.0.0.255 eq 443
permit tcp any 10.158.26.0 0.0.0.255 eq 1494
permit tcp any 10.158.26.0 0.0.0.255 eq 2598
permit tcp any 10.158.8.0 0.0.0.255 eq 139
permit tcp any 10.158.8.0 0.0.0.255 eq 445
permit tcp any 10.242.0.0 0.0.0.255 eq 80
permit tcp any 10.242.0.0 0.0.0.255 eq 443
```

Tämän jälkeen tehtiin class-mapit eri luokille.

```
class-map match-any MARK-GOLD
 match ip precedence 5
 match ip dscp cs5  ef
class-map match-any  MARK-SILVER
 match access-group name CUST-SILVER
class-map match-any MARK-BRONZE
 match access-group name CUST-BRONZE
```

”Class-map match-any MARK-SILVER” -komennon tarkoituksena on ohjata kaikki siihen kuuluvat luokat (class) tunnistautumaan reitittimen pääsylistoja hyväksi käyttäen. Tässä tapauksessa viitataan access-listaan ”CUST-SILVER”. Access-listat on asetettu tietyin parametrein tunnistamaan priorisoitava liikenne muusta liikenteestä. Ensimmäisen rivin mukaisesti havaitaan TCP-portin 80 liikenne kohdeverkkoon 172.25.0.0/24.

Tämän jälkeen luotiin policy-map luokille, jossa sisään tuleville paketeille määrätään tietty presedenssiarvo class-mappien perusteella.

```
policy-map MARK-CUST-TRAFFIC
 class MARK-GOLD
  set precedence 5
 class MARK-SILVER
  set precedence 4
 class MARK-BRONZE
  set precedence 3
```

”Policy-map”-komento pitää sisällään tiedon, mitä luokan sisältävälle liikenteelle tehdään, kun se on tunnistettu. Konfiguraatioesimerkissä asetetaan luokan ”GOLD” presedenssiarvoksi 5, luokan ”SILVER” presedenssiarvoksi 4 ja luokan ”BRONZE” arvoksi 3.

Policy-map liitettiin asiakasreitittimen LAN-liityntään, jossa tutkitaan kaikki sisääntuleva liikenne.

```
interface GigabitEthernet0/1
 description LAN
 ip address 172.0.1.1 255.255.255.254
 no ip redirects
 no ip proxy-arp
 duplex full
 speed 100
 service-policy input MARK-CUST-TRAFFIC
```

Luokille jaettava kapasiteetti määritellään toisella policy-mapilla runkoverkon suuntaan hierarkkisesti. Koska liittymän fyysinen nopeus on 1 Gbps, joudutaan pääpolitiikaksi määrittelemään liittymän kapasiteetin mukainen 50 Mbps:n rajoitin.

```
policy-map PROFILE-13-50M-parent
 class class-default
  shape average 50000000
  service-policy PROFILE-13-child
```

On kaksi tapaa rajoittaa verkkoliitännästä tulevan liikenteen määrää: polisointi (policing) ja muotoilu (shaping). Kun liitäntäpiste on polisoitu ja lähtevä liikenne ylittää määritetyn kynnyksen, aletaan pudottaa paketteja. Muotoilu taas puskuroi purskeita alkaen välittää niitä, kun liikennettä linkillä on vähemmän. Muotoilulla on mahdollista tehostaa kaistanleveyden käyttöä kehysrakenteiden siirtämisen kustannuksella (overhead). Tämän työn kohdalla käytetään liittymänopeuden rajoittamisessa muotoilua.

Luodun pääpolitiikan alle tehdään alipolitiikka, joka hoitaa kapasiteetin varaamisen määrittelyn mukaisesti.

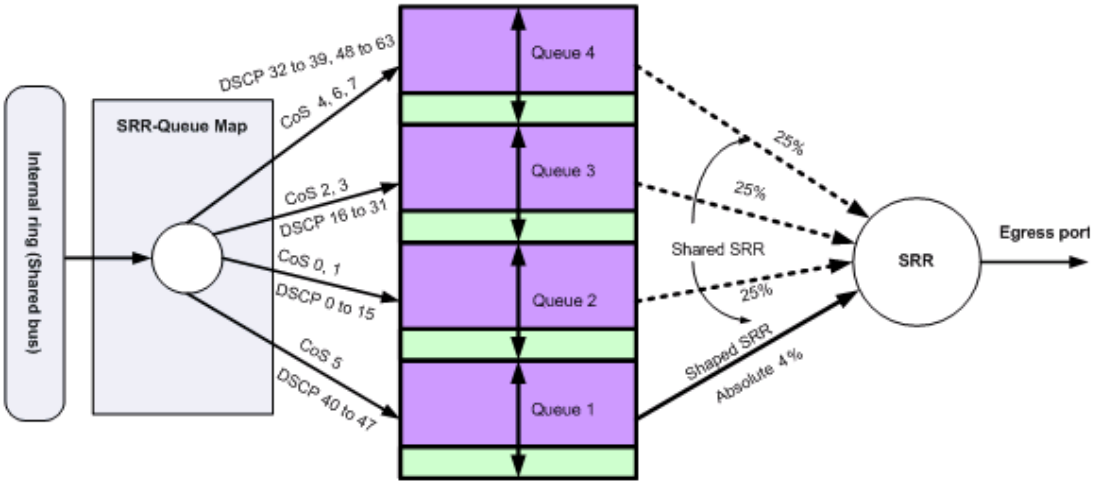
```
policy-map PROFILE-13-child
 class voice
  police cir percent 10
 class video
  bandwidth percent 25
 class data
  bandwidth percent 25
 class class-default
  bandwidth percent 40
```

Policy-map liitetään asiakasreitittimen WAN-liitäntään.

```
interface GigabitEthernet0/0
 description WAN
 ip address 192.168.1.1 255.255.255.254
 duplex auto
 speed auto
 service-policy output PROFILE-13-50M-parent
```

Koska yrityksellä on päätelaitteinaan sekä reitittimiä että L3-kytkimiä, jouduttiin konfiguraatioita tekemään useampia erilaisia, koska reitittimille tarkoitettu konfiguraatio ei toimi Ciscon reitittävissä kytkimissä.

Kytkintä käytettäessä paketit jaetaan neljään jonoon ja oletusarvoisesti jokaiselle jonolle annetaan 25 % käytössä olevista puskureista. Jonoille annetaan prosentuaalinen osuus taattua kaistaa (shaping) suhteissa 1:25, 2:0, 3:0 ja 4:0, mikä tarkoittaa, että ensimmäiselle jonolle taataan 1/25 kapasiteetista, mutta samalla kaista rajoitetaan (rate limit); 1/25 = 4 %, joten L3 -kytkimille tehtävä priorisointi vaatii hieman enemmän laskemista ja ajattelua kuin vastaava toimenpide reitittimille tehtynä.



Kuva 25. Kaaviokuva reitittävän kytkimen oletusjonoista.

Globaalit komennot Cisco 3560-kytkimen priorisoinnin konfigurointiin:

```
mls qos
no mls qos rewrite ip dscp
mls qos srr-queue input buffers 90 10
mls qos srr-queue input priority-queue 2 bandwidth 10
```

”mls qos”-komento käynnistää priorisoinnin globaalisti reitittävällä kytkimellä. ”no mls qos rewrite ip dscp” -komento estää lähiverkosta saapuvien pakettien DSCP-merkinnän uudelleenkirjoittamisen nollaksi, jos paketit saapuvat luottamattomasta (untrusted) liitännästä. Näin ollen lähiverkosta saapuvan liikenteen olemassaolevat DSCP-merkinnät säilyvät ennallaan. Komento “mls qos srr-queue input buffers 90 10” määrittelee, miten jonot 1 ja 2 jakavat puskurin prosentuaalisesti sisään tuleville paketeille. Kun jonojen 1 ja 2 puskurit täyttyvät sataprosenttisesti, aletaan jonoista

tiputtaa paketteja. Raja-arvot (treshold) ovat jonoille oletusarvoiset. Esimerkinomaisesti puskurien raja-arvot voitaisiin määritellä seuraavalla tavalla.

```
mls qos srr-queue input threshold 1 90 10
mls qos srr-queue input threshold 2 34 66
```

Määritetyt asetukset nähdään seuraavasti.

```
#sh mls qos input-queue
Queue     :       1       2
-----------------------------------------
buffers   :      90      10
bandwidth :       4       4
priority  :       0      10
threshold1:     100     100
threshold2:     100     100
```

WAN-porttiin käytettävät komennot:

```
mls qos trust dscp
priority-queue out
srr-queue bandwidth share 1 62 38 1
srr-queue bandwidth shape 10 0  0 4
```

“priority-queue out”-komento määrittää, että prioriteettijono tyhjennetään liikenteestä ennen kuin muita jonoja palvellaan.

LAN-portin priorisointi:

```
mls qos trust dscp
priority-queue out
```

Kun SRR scheduler on määritetty shared-tilaan, kunkin jonon kaistanleveys perustuu suhteelliseen painoarvoon. Esimerkinomaisesti:

```
srr-queue bandwidth share 30 20 25 25
```

Edellistä tutkittaessa saadaan painon summaksi 100. Tämä voi olla muutakin, mutta lukemista helpottaa, jos lukujen summa edustaa 100 prosenttia. Suhteelliset osuudet ovat näin ollen "30/100", "20/100", "25/100", "25/100" ja näistä voidaan laskea tehollinen taattu kaistanleveys jonokohtaisesti kertomalla tämä painoarvo liittymän kaistanleveydellä.

Esimerkkinä 100 Mbps:n liittymällä on $30/100 \cdot 100$ Mbps = 30 Mbps ja 10 Mbps:n liittymällä $30/100 \cdot 10$ Mbps = 3 Mbps. Nämä arvot otetaan ainoastaan huomioon silloin, kun liittymän kapasiteetti alkaa täyttyä.

Kun SRR scheduler on määritelty shaped-tilaan, kaistanleveyden rajoitukset perustuvat kunkin jonon käänteiseen absoluuttiseen painoarvoon.

```
srr-queue bandwidth shape 10 0 0 4
```

Edellinen rajoittaa ensimmäisen jonon kymmenesosaan liittymän käytettävissä olevasta kaistanleveydestä, 1/10 · 1000/2 eli 50 Mbps GOLD-profiilin mukaisesti. Arvon asettaminen nollaksi tarkoittaa, ettei liikennettä rajoiteta. Shaped-määrittelyn ollessa käytössä SRR scheduler ei käytä jaettua painoarvoa.

Shaped- ja shared-tiloja voidaan myös yhdistellä. Esimerkkinä kaksi jonoa voidaan konfiguroida shared-moodiin ja toiset kaksi shaped-moodiin.

```
interface FastEthernet0/13
 srr-queue bandwidth share 100 100 40 20
 srr-queue bandwidth shape  50  50  0  0
```

Oletetaan, että liittymän nopeus on 100 Mbps, jolloin jonot 1 ja 2 saavat kaistaa 2 Mpbs seuraavasti: 1/50 · 100 = 2. Jonoille 3 ja 4 jaetaan jäljelle jäävä osuus kaistasta suhteessa 2:1. Huomioitavaa on, että jonoille 1 ja 2 taataan ja rajataan nopeudeksi 2 Mbps samaan aikaan.

Päätelaitteella käytetään oletuskarttaa CoS-arvojen sijoittamiseen jonoihin.

```
#sh mls qos maps cos-output-q
   Cos-outputq-threshold map:
               cos:  0   1   2   3   4   5   6   7
               ------------------------------------
  queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1
```

Edellisen mukaan CoS 5, GOLD-luokka, sijoitetaan jonoon 1, CoS 4, SILVER-luokka asetetaan jonoon 4 ja BRONZE-luokka asetetaan jonoon 3.

Tämän perusteella asiakkaan pääyhteyden liittymän priorisointia varten tehtiin seuraava konfiguraatio:

```
mls qos trust dscp
priority-queue out
srr-queue bandwidth share 1 62 38 1
srr-queue bandwidth shape 10 0  0 4
srr-queue bandwidth limit 50
```

Jonoille annetaan konfiguroinnissa käyttöön seuraavat kapasiteetit:

Jono	Luokitus	Kaista
queue1	GOLD	1/10 × 1000 / 2 = 50 Mps
queue4	SILVER	1/4 × 1000 / 2 = 125 Mbps

Loput jonot jakavat jäljelläolevan kaistan 325 Mbps keskenään:

Jono	Luokitus	Kaista
queue3	BRONZE	0,38 · 325 = 123,5 Mbps
queue2	BEST EFFORT	0,62 · 325 = 201,5 Mbps

Komennolla ”sh mls qos interface g0/1 statistics” varmistetaan presedenssimerkattujen pakettien välitys verkkoliitännässä.

```
#sh mls qos interface g0/1 statistics
GigabitEthernet0/1

  dscp: incoming
-------------------------------

  0 -  4 :       47684            5          9865            0          242
  5 -  9 :           0            4             0           46            0
 10 - 14 :         295            0             1            0            0
 15 - 19 :           3            1             0          171            0
 20 - 24 :           0            0             3            0          995
 25 - 29 :           0          540             0            0            0
 30 - 34 :           1            0         60241            0          237
 35 - 39 :           0            0             0           68            0
 40 - 44 :       64431            0             0            0            0
 45 - 49 :           0         9331             0         9747            0
 50 - 54 :           0            0             0            0            0
 55 - 59 :           0         9360             0            0            0
 60 - 64 :           0            0             0            0
  dscp: outgoing
-------------------------------

  0 -  4 :       44334            0          8871            0           38
  5 -  9 :           0            0             0            9            0
 10 - 14 :           0            0             0            0            0
 15 - 19 :           0            0             0            2            0
 20 - 24 :           0            0             0            0          441
 25 - 29 :           0            0             0            0            0
 30 - 34 :           0            0         48459            0            0
 35 - 39 :           0            0             0            0            0
 40 - 44 :       33931            0             0            0            0
 45 - 49 :           0         7612             0        52704            0
 50 - 54 :         642            0             0            0            0
 55 - 59 :           0            0             0            0            0
 60 - 64 :           0            0             0            0
```

Mahdolliset pakettien pudotukset tarkistetaan L3-kytkimellä seuraavasti.

```
#sh platform port-asic stats drop gi0/1

  Interface Gi0/1 TxQueue Drop Statistics
    Queue 0
      Weight 0 Frames 0
      Weight 1 Frames 0
      Weight 2 Frames 0
```

```
    Queue 1
      Weight 0 Frames 0
      Weight 1 Frames 0
      Weight 2 Frames 0
    Queue 2
      Weight 0 Frames 0
      Weight 1 Frames 0
      Weight 2 Frames 0
    Queue 3
      Weight 0 Frames 0
      Weight 1 Frames 0
      Weight 2 Frames 0
```

Huomioitavaa edellisessä on, että tulosteen Queue 0 on CoS-kartan jono 1.

PE-reitittimien priorisointikonfiguraatiot vastaavat etätoimipisteiden reitittimissä käytettäviä policy-mappeja.

Main site, policy map

```
policy-map PROFILE-13-500M-parent
  class class-default
    shape average 500000000
   service-policy PROFILE-13-child
!
policy-map PROFILE-13-child
  class voice
    priority
    police cir percent 10
  class video
    bandwidth percent 25
  class data
    bandwidth percent 25
  class class-default
    bandwidth percent 40
```

Pääpolitiikka rajoittaa kaistan rungosta 500 megabittiin fyysisesn liitännän ollessa 1 gigabitti.

```
policy-map PROFILE-13-500M-parent
  class class-default
    shape average 500000000
   service-policy PROFILE-13-child
```

Alipolitiikka hoitaa luokkien kaistanrajoitukset aiemmin määritellyn mukaisesti.

```
policy-map PROFILE-13-child
  class voice
    priority
    police cir percent 10
  class video
    bandwidth percent 25
  class data
    bandwidth percent 25
  class class-default
    bandwidth percent 40
```

Policy-map kytkettiin PE-reitittimen asiakasinterfaceen. Input-suunnan policy-map rajoittaa ainoastaan kaistan. Tämän suunnan priorisointi on hoidettu asiakasreitittimen WAN-interfacessa.

```
service-policy input 500M
service-policy output PROFILE-13-500M-parent
```

Branch site 1, policy map

```
policy-map PROFILE-13-50M-parent
  class class-default
    shape average 50000000
   service-policy PROFILE-13-child
!
policy-map PROFILE-13-child
  class voice
    priority
    police cir percent 10
  class video
    bandwidth percent 25
  class data
    bandwidth percent 25
  class class-default
    bandwidth percent 40
```

Branch site 1, PE-reitittimen interface

```
interface GigabitEthernet2/1.100
 description V: Customer
 encapsulation dot1Q 100
 ip vrf forwarding CUSTOMER-FI
 ip address 192.168.1.0 255.255.255.254
 no ip redirects
 no ip proxy-arp
 service-policy input 50M
 service-policy output PROFILE-13-50M-parent
```

Reitittimien täydelliset konfiguraatiot ovat liitteessä.

5.5 Testaus

Testaus aloitettiin liikenteen seuraamisella ja tarkastelemalla aktiivilaitteiden kuormitusta. Testeillä pyrittiin selvittämään, miten liikenteen laatu riippuu muusta verkon liikenteestä.

```
Class-map: MARK-GOLD (match-any)
  944 packets, 133172 bytes
Class-map: MARK-SILVER (match-any)
  3512 packets, 495894 bytes
Class-map: MARK-BRONZE (match-any)
  2109 packets, 297791 bytes
Class-map: class-default (match-any)
  2099 packets, 1318127 bytes
```

Edellisestä huomataan, että Branch Site 1 lähiverkosta tuleville paketeille asetetaan presedenssiarvot sovitun mukaisesti. Samalla seurattiin myös WAN-liitännän policy-mappia ja kaistanjakoa

```
Service-policy : PROFILE-13-child

  Class-map: GOLD (match-any)
    944 packets, 133172 bytes
    5 minute offered rate 82000 bps, drop rate 0 bps
    Match: ip precedence 5
     944 packets, 133172 bytes
     5 minute rate 182000 bps
    Match: ip dscp cs5 (40) ef (46)
     0 packets, 0 bytes
     5 minute rate 0 bps
    police:
        cir 10 %
        cir 5000000 bps, bc 156250 bytes
      conformed 944 packets, 133172 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 234000 bps, exceed 0 bps

  Class-map: SILVER (match-any)
    3512 packets, 495894 bytes
    5 minute offered rate 119000 bps, drop rate 0 bps
    Match: ip precedence 4
     3512 packets, 495894 bytes
     5 minute rate 79000 bps
    Match: ip dscp cs4 (32) af41 (34) af42 (36) af43 (38)
     0 packets, 0 bytes
     5 minute rate 0 bps
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 3512/495894
    bandwidth 25% (12500 kbps)

  Class-map: BRONZE (match-any)
    2109 packets, 297791 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 3
     2109 packets, 297791 bytes
     5 minute rate 0 bps
    Match: ip dscp cs3 (24) af31 (26) af32 (28) af33 (30)
     0 packets, 0 bytes
     5 minute rate 0 bps
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 2109/297791
    bandwidth 25% (12500 kbps)

  Class-map: class-default (match-any)
    2099 packets, 1318127 bytes
    5 minute offered rate 232000 bps, drop rate 0 bps
    Match: any
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 2099/1318127
    bandwidth 40% (20000 kbps)
```

Samaan aikaan selvitettiin myös käyttäjien kokemuksia viivekriittisten sovellusten toiminnassa. Kokonaisuudessaan verkon toiminta parani merkittävästi. Varsinkin viivekriittisten sovellusten toimivuudessa esiintyneet ongelmat katosivat lähes täydellisesti.

6 Tulosten tarkastelu ja yhteenveto

Työssä suunniteltiin ja konfiguroitiin yrityksen MPLS VPN-pohjaiseen verkkoon QoS-ratkaisu, jonka avulla aikakriittisten sovellusten käyttö muuttui toimivammaksi. Verkossa kulkee paljon aikakriittistä dataa, mm. VoIP-puheluita, joiden toiminta ei ennen verkon päivitystä ollut tyydyttävällä tasolla.

Työn alussa kuvattiin taustatekniikat painopisteen ollessa IP-protokollissa. Seuraavaksi käytiin läpi MPLS-verkkojen ja tietoliikenteen luokittelun ja priorisoinnin käytännöt.

Käytännön osuudessa suunniteltiin ja implementoitiin käyttöön QoS-ratkaisut, jotka konfiguroitiin asiakkaan verkon aktiivilaitteisiin. Työssä esiteltiin konfiguroinnin keskeiset osat ja aktiivilaitteiden konfiguraatiot. Lopuksi testattiin liikenteen toimintaa ja verkon käyttäytymistä eri tilanteissa.

Konfiguraatioiden laatiminen reitittimiin ja kytkimiin oli varsin suoraviivainen tehtävä. Testaus vaati jonkin verran työtä, mutta kokonaisuudessaan konfigurointi sujui juohevasti. Koska työ tehtiin toimivassa verkossa, toiminnan häiriötön takaaminen työn aikana asetti omat haasteensa.

Käyttäjien kokemukset työn aikana ja sen jälkeen olivat voittopuolisesti myönteisiä.

Tuloksena saatiin toimiva tietoverkko, jonka välityskyky riittää mainiosti asiakkaan nykytarpeisiin ja jota voidaan helposti laajentaa tarpeiden kasvaessa.

Lähteet

1 Day J D, Zimmermann H. The OSI reference model. Proceedings of the IEEE 1983;71(12):1334-1340.

2 Stevens WR. TCP/IP illustrated. Volume 1, The protocols. Reading (MA): Addison-Wesley; 1994.

3 Pepelnjak Ivan. MPLS and VPN Architectures. ISBN 158-705-002-1 Cisco Press.

4 De Ghein Luc. MPLS Fundamentals. ISBN 158-705-197-4 Cisco Press.

5 DiffServ - The Scalable End-to-End QoS Model. White paper. http://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.pdf.

6 Flannagan Mike. Administering Cisco QoS in IP Networks. ISBN 192-899-421-0.

7 rfc3037. LDP Applicability. http://www.ietf.org/rfc/rfc3037.txt. Luettu 10.10.2012.

8 Doyle, Jeff. Understanding MPLS VPNs, Part I. Network World . http://www.networkworld.com/community/node/24781. Luettu 10.10.2012.

9 Jaakohuhta Hannu. Lähiverkot – Ethernet. ISBN 951-826-787-1 IT Press 2005.

10 Lobo L. MPLS Configuration on Cisco IOS Software. Cisco Press. 2005.

11 MPLS DiffServ-aware Traffic Engineering. White paper. http://www.terabitsystems.com/juniper-docs/MPLS%20DiffServ-aware%20Traffic%20Engineering.pdf. Luettu 10.10.2012.

12 Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. 1998.

13 Luentomoniste. http://www.tml.tkk.fi/Opinnot/T-111.2350/2007/Kalvot/QoS_6.pdf. Luettu 10.10.2012.

14 Palvelun laatu. Teleware. https://events.kpmg.fi/Portals/1/kurssit/Puolustusvoimat_OSPF-MPLS/QoS.pdf. Luettu 11.10.2012.

15 Cisco Whitepapers: DiffServ - The scalable end to end quality of service model MPLS-runkoverkko

16 Penttinen A. Luentomoniste. Network Planning and Dimensioning. TKK. 1999.

17 Riley Charles. Cisco Internetworking. Syngress. ISBN 1-931836-91-4.

Liite 1. Main Site, PE-laitteen konfiguraatio

```
policy-map PROFILE-13-500M-parent
  class class-default
    shape average 500000000
   service-policy PROFILE-13-child
!
policy-map PROFILE-13-child
  class voice
    priority
    police cir percent 10
  class video
    bandwidth percent 25
  class data
    bandwidth percent 25
  class class-default
    bandwidth percent 40
!
ip vrf CUSTOMER-FI
 rd 1:1
 import map default-import
 route-target export 1:1
 route-target export 2:2
 route-target export 3:3
 route-target export 4:4
 route-target import 1:1
 route-target import 2:2
 route-target import 3:3
 route-target import 4:4
 maximum routes 4000 80
!
interface GigabitEthernet1/1.100
 description V: Customer Main Site
 encapsulation dot1Q 100
 ip vrf forwarding CUSTOMER-FI
 ip address 192.168.0.0 255.255.255.254
 no ip redirects
 no ip proxy-arp
 service-policy input 500M
 service-policy output PROFILE-13-500M-parent
!
router bgp 3292
 !
 address-family ipv4 vrf CUSTOMER-FI
  no synchronization
  redistribute static
  redistribute connected
  neighbor 192.168.0.1 remote-as 65535
  neighbor 192.168.0.1 ttl-security hops 1
  neighbor 192.168.0.1 transport path-mtu-discovery
  neighbor 192.168.0.1 transport connection-mode passive
  neighbor 192.168.0.1 disable-connected-check
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community
  neighbor 192.168.0.1 as-override
  neighbor 192.168.0.1 soft-reconfiguration inbound
 exit-address-family
!
ip extcommunity-list standard customer-fi permit rt 1:1
!
ip prefix-list default seq 5 permit 0.0.0.0/0
!
route-map default-import permit 100
 match extcommunity customer-fi
route-map default-import deny 200
 match ip address prefix-list default
route-map default-import permit 300
!
end
```

Liite 2. Branch Site 1, PE-konfiguraatio

```
policy-map PROFILE-13-50M-parent
  class class-default
    shape average 50000000
   service-policy PROFILE-13-child
!
policy-map PROFILE-13-child
  class voice
    priority
    police cir percent 10
  class video
    bandwidth percent 25
  class data
    bandwidth percent 25
  class class-default
    bandwidth percent 40
!
ip vrf CUSTOMER-FI
 rd 1:1
 import map default-import
 route-target export 1:1
 route-target export 2:2
 route-target export 3:3
 route-target export 4:4
 route-target import 1:1
 route-target import 2:2
 route-target import 3:3
 route-target import 4:4
 maximum routes 4000 80
!
interface GigabitEthernet2/1.187
 description V: Customer Branch Site 1
 encapsulation dot1Q 100
 ip vrf forwarding CUSTOMER-FI
 ip address 192.168.1.0 255.255.255.254
 no ip redirects
 no ip proxy-arp
 service-policy input 50M
 service-policy output PROFILE-13-50M-parent
!
router bgp 3292
 !
 address-family ipv4 vrf CUSTOMER-FI
  no synchronization
  redistribute static
  redistribute connected
  neighbor 192.168.1.1 remote-as 65534
  neighbor 192.168.1.1 ttl-security hops 1
  neighbor 192.168.1.1 transport path-mtu-discovery
  neighbor 192.168.1.1 disable-connected-check
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 send-community
  neighbor 192.168.1.1 as-override
  neighbor 192.168.1.1 soft-reconfiguration inbound
 exit-address-family
!
ip extcommunity-list standard customer-fi permit rt 1:1
!
ip prefix-list default seq 5 permit 0.0.0.0/0
!
route-map default-import permit 100
 match extcommunity customer-fi
route-map default-import deny 200
 match ip address prefix-list default
route-map default-import permit 300
!
end
```

Liite 3. Main Site, reititinkonfiguraatio

```
version 12.2
parser config cache interface
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption service unsupported-transceiver
!
hostname Customer_Main_Site_cpe
!
boot-start-marker
boot-end-marker
!
ip subnet-zero
no ip source-route
ip routing
no ip dhcp use vrf connected
!
mls qos
!
no setup express
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp selective-ack
ip tcp timestamp
ip tcp mss 1460
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip ssh logging events
ip ssh version 2
!
class-map match-any MARK-GOLD
 match ip precedence 5
 match ip dscp cs5  ef
class-map match-any MARK-SILVER
 match access-group name CUST-SILVER
class-map match-any MARK-BRONZE
 match access-group name CUST-BRONZE
!
policy-map MARK-CUST-TRAFFIC
 class MARK-GOLD
  set precedence 5
 class MARK-SILVER
  set precedence 4
 class MARK-BRONZE
  set precedence 3
!
interface GigabitEthernet0/1
 description WAN
 no switchport
 ip address 192.168.0.1 255.255.255.254
 srr-queue bandwidth share 1 62 38 1
 srr-queue bandwidth shape  10  0  0  4
 srr-queue bandwidth limit 50
 priority-queue out
 mls qos trust dscp
 no ip redirects
 no ip proxy-arp
!
interface GigabitEthernet0/2
 description LAN
 no switchport
```

```
 ip address 172.0.0.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 service-policy input MARK-CUST-TRAFFIC
!
interface Vlan1
 no ip address
 shutdown
!
router bgp 65535
 no synchronization
 bgp log-neighbor-changes
 redistribute connected
 neighbor 192.168.0.1 remote-as 3292
 neighbor 192.168.0.1 description PE-router
 neighbor 192.168.0.1 version 4
 neighbor 192.168.0.1 timers 10 30
 neighbor 192.168.0.1 send-community
 neighbor 192.168.0.1 soft-reconfiguration inbound
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.0.0.2
ip route 10.158.0.0 255.255.0.0 172.0.0.2
ip route 10.242.0.0 255.255.0.0 172.0.0.2
ip route 172.22.30.0 255.255.255.0 172.0.0.2
ip route 172.25.0.0 255.255.0.0 172.0.0.2
ip route 172.27.0.0 255.255.255.0 172.0.0.2
!
no ip http server
no ip http secure-server
!
ip access-list extended CUST-SILVER
permit ip 172.22.30.0 0.0.0.255 any
permit tcp any 172.25.0.0 0.0.0.255 eq 80
permit tcp any 172.25.0.0 0.0.0.255 eq 1494
permit tcp any 172.25.0.0 0.0.0.255 eq 2598
permit ip any 172.25.8.192 0.0.0.31
permit ip any 172.25.8.64 0.0.0.63
permit ip 172.25.8.160 0.0.0.31 any
permit ip 172.25.81.128 0.0.0.63 any
!
ip access-list extended name CUST-BRONZE
permit ip any 172.25.14.0 0.0.0.255
permit tcp any 172.25.0.0 0.0.0.255 eq 80
permit tcp any 172.25.0.0 0.0.0.255 eq 443
permit tcp any 172.27.0.192 0.0.0.31 eq 80
permit tcp any 172.27.0.192 0.0.0.31 eq 443
permit tcp any 10.158.1.0 0.0.0.255 eq 80
permit tcp any 10.158.1.0 0.0.0.255 eq 443
permit tcp any 10.158.26.0 0.0.0.255 eq 1494
permit tcp any 10.158.26.0 0.0.0.255 eq 2598
permit tcp any 10.158.8.0 0.0.0.255 eq 139
permit tcp any 10.158.8.0 0.0.0.255 eq 445
permit tcp any 10.242.0.0 0.0.0.255 eq 80
permit tcp any 10.242.0.0 0.0.0.255 eq 443
!
logging trap debugging
logging facility local2
!
control-plane
!
banner motd ^C
**********************************************************
* This system belongs to TDC and may only be            *
* accessed by authorized employees at TDC.              *
* People who are unauthorized will be prosecuted if     *
* they attempt or succeed in accessing, interfering or  *
* taking any other action which may disturb the system. *
**********************************************************
^C
!
line con 0
 exec-timeout 30 0
```

```
 exec-character-bits 8
 special-character-bits 8
 transport preferred none
 escape-character 3
line vty 0 4
 exec-timeout 30 0
 exec-character-bits 8
 special-character-bits 8
 transport preferred none
 transport input telnet ssh
 escape-character 3
line vty 5 15
!
scheduler max-task-time 5000
end
```

Liite 4. Branch Site 1, reititinkonfiguraatio

```
version 15.1
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service compress-config
!
hostname Customer_Branch1_cpe
!
boot-start-marker
boot-end-marker
!
!
logging buffered 64000
logging rate-limit all 10
no logging console
enable secret 5 $1$Au8X$H/CZdOcMMxV3knncdNPAD.
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
no ipv6 cef
no ip source-route
ip cef
!
no ip bootp server
no ip domain lookup
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO1921/K9 sn FCZ1533217K
license boot module c1900 technology-package datak9
!
!
redundancy
!
!
ip tcp mss 1460
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip ftp source-interface GigabitEthernet0/0
ip tftp source-interface GigabitEthernet0/0
!
class-map match-any MARK-GOLD
 match ip precedence 5
 match ip dscp cs5  ef
class-map match-any MARK-SILVER
 match access-group name CUST-SILVER
class-map match-any MARK-BRONZE
 match access-group name CUST-BRONZE
class-map match-any default
 match any
!
!
policy-map PROFILE-13-child
```

```
 class voice
  police cir percent 10
 class video
  bandwidth percent 25
 class data
  bandwidth percent 25
 class class-default
  bandwidth percent 40
policy-map PROFILE-13-50M-parent
 class class-default
  shape average 50000000
  service-policy PROFILE-13-child
!
policy-map MARK-CUST-TRAFFIC
 class MARK-GOLD
  set precedence 5
 class MARK-SILVER
  set precedence 4
 class MARK-BRONZE
  set precedence 3
!
interface GigabitEthernet0/0
 description WAN
 ip address 192.168.1.1 255.255.255.254
 duplex auto
 speed auto
 service-policy output PROFILE-13-50M-parent
!
interface GigabitEthernet0/1
 description LAN
 ip address 172.0.1.1 255.255.255.254
 no ip redirects
 no ip proxy-arp
 duplex full
 speed 100
 service-policy input MARK-CUST-TRAFFIC
!
router bgp 65534
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 192.168.1.0 remote-as 3292
 neighbor 192.168.1.0 ttl-security hops 1
 neighbor 192.168.1.0 timers 7 21
 neighbor 192.168.1.0 send-community
 neighbor 192.168.1.0 soft-reconfiguration inbound
 no auto-summary
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard GLOB-VPN-MGMT permit 3292:40001
no ip http server
no ip http secure-server
!
ip route 172.25.81.0 255.255.255.0 172.0.1.2
ip route 172.25.88.0 255.255.255.0 172.0.1.2
ip route 172.25.91.0 255.255.255.0 172.0.1.2
!
ip access-list standard MGMT-VTY
 permit 192.168.1.0
 permit 172.25.255.94
 permit 213.88.253.2
 permit 172.25.35.4
 permit 193.162.146.71
 permit 193.162.146.72
 permit 193.163.24.224 0.0.0.31
 permit 213.131.136.64 0.0.0.63
 permit 62.65.31.64 0.0.0.63
 permit 213.225.90.0 0.0.0.63
 permit 195.10.132.192 0.0.0.63
ip access-list standard SNMP-CUST-RO
 remark *** Customer Hosts with allowed SNMP read only access ***
 remark *** Customer Hosts with allowed SNMP read only access (Tamro NMS) ***
```

```
 permit 172.25.0.148
ip access-list standard SNMP-TDC-RW
 permit 213.88.253.2
 permit 193.163.24.224 0.0.0.31
 permit 213.131.136.64 0.0.0.63
 permit 62.65.31.64 0.0.0.63
 permit 213.225.90.0 0.0.0.63
 permit 195.10.132.192 0.0.0.63
!
ip access-list extended CUST-SILVER
permit ip 172.22.30.0 0.0.0.255 any
permit tcp any 172.25.0.0 0.0.0.255 eq 80
permit tcp any 172.25.0.0 0.0.0.255 eq 1494
permit tcp any 172.25.0.0 0.0.0.255 eq 2598
permit ip any 172.25.8.192 0.0.0.31
permit ip any 172.25.8.64 0.0.0.63
permit ip 172.25.8.160 0.0.0.31 any
permit ip 172.25.81.128 0.0.0.63 any
!
ip access-list extended name CUST-BRONZE
permit ip any 172.25.14.0 0.0.0.255
permit tcp any 172.25.0.0 0.0.0.255 eq 80
permit tcp any 172.25.0.0 0.0.0.255 eq 443
permit tcp any 172.27.0.192 0.0.0.31 eq 80
permit tcp any 172.27.0.192 0.0.0.31 eq 443
permit tcp any 10.158.1.0 0.0.0.255 eq 80
permit tcp any 10.158.1.0 0.0.0.255 eq 443
permit tcp any 10.158.26.0 0.0.0.255 eq 1494
permit tcp any 10.158.26.0 0.0.0.255 eq 2598
permit tcp any 10.158.8.0 0.0.0.255 eq 139
permit tcp any 10.158.8.0 0.0.0.255 eq 445
permit tcp any 10.242.0.0 0.0.0.255 eq 80
permit tcp any 10.242.0.0 0.0.0.255 eq 443
!
logging esm config
logging trap debugging
logging facility local2
logging source-interface GigabitEthernet0/0
!
control-plane
!
banner motd ^C
**********************************************************
* This system belongs to TDC and may only be            *
* accessed by authorized employees at TDC.              *
* People who are unauthorized will be prosecuted if     *
* they attempt or succeed in accessing, interfering or  *
* taking any other action which may disturb the system. *
**********************************************************
^C
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 30 0
 logging synchronous
 transport input all
line vty 5 15
 exec-timeout 30 0
 logging synchronous
 transport input all
!
scheduler allocate 20000 1000
end
```