TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

PALVELUN LAADUN VARMISTAMINEN VOIP-VERKOSSA:
teoriaa ja harjoituksia opiskelijoille

Jesse Laamanen

Tietojenkäsittelyn koulutusohjelma
huhtikuu 2007
Työn ohjaaja: Paula Hietala

TAMPERE 2007

TAMPEREEN AMMATTIKORKEAKOULU

Tekijä(t)	Jesse Laamanen
Koulutusohjelma(t)	Tietojenkäsittely
Opinnäytetyön nimi	Palvelun laadun varmistaminen VoIP-verkossa: teoriaa ja harjoituksia opiskelijoille
Työn valmistumis-kuukausi ja -vuosi	huhtikuu 2007
Työn ohjaaja	Paula Hietala
Sivumäärä:	51+47

TIIVISTELMÄ

Puhelut ovat siirtymässä perinteisistä puhelinverkoista IP-verkkoihin IT-hallinnon piiriin. Äänipuheluiden tuominen dataverkkoihin tuo uusia haasteita ja vaatimuksia tietoverkoille. Suurin osa vaatimuksista johtuu äänipuheluiden reaaliaikaisuudesta. Vaatimusten täyttäminen vaatii verkkovastaavalta palvelun laadun varmistamiseen liittyviä toimia ja VoIP-tekniikan ymmärrystä.

Työ tehtiin toimeksiantona Tampereen ammattikorkeakoululle. Sen pääasiallinen tarkoitus oli luoda VoIP-liikenteen palvelun laadusta harjoitustehtäviä Cisco Systemsin laitteilla. Valmiit harjoitustehtävät teetettiin ohjatusti opiskelijoilla, ja ne jäivät koululle jatkokäyttöä varten. Harjoitukset suunniteltiin kurssille, joka pohjautuu Cisco Systemsin tuottamiin materiaaleihin ja laitteisiin. Harjoituksiin on mahdollista lisätä multicast-ominaisuuteen liittyvää tietosisältöä, jos harjoituksia halutaan lähteä tulevaisuudessa laajentamaan.

Opinnäyteraportti käy läpi VoiP-tekniikkaa keskeisimmiltä osiltaan ja kertoo myös siitä, mitä vaatimuksia se asettaa tietoverkoille. Raportissa selvitetään myös, mitä keinoja Ciscon laitteilla on riittävän palvelun laadun varmistamiseksi äänipuheluille. Työn loppuosassa kuvataan harjoitustehtävien tuottamiseen liittynyttä prosessia sekä analysoidaan oppituntien onnistumista.

Työn lähdemateriaali koostuu palvelun laadun varmistamisen osalta suurimmaksi osaksi Ciscon julkaisemasta materiaalista, koska työssä käytetyt laitteet ovat tämän laitevalmistajan laitteita. Tietoa on haettu VoIP-tekniikasta myös muista lähteistä, kuten laitevalmistajasta riippumattomista lähteistä. Harjoitustehtävien sisältö ja rakenne pohjautuvat kurssia opettavien opettajien haastatteluihin sekä minun, kurssin suorittaneen opiskelijan, omiin näkemyksiin.

Avainsanat Palvelun laatu Voice over IP DiffServ Oppimateriaali

TAMPERE
POLYTECHNIC

Author(s)	Jesse Laamanen
Degree Programme(s)	Business Information Systems
Title	Ensuring Quality of service in VoIP network: theory and exercises for students
Month and year	April 2007
Supervisor	Paula Hietala

Pages: 51+47

ABSTRACT

Nowadays phone calls are shifting from traditional telephony networks to IP-networks and under the administration of IT-personnel. By bringing phone calls to the data networks, new challenges and requirements are emerging. Most of strains are originated from the fact that voice traffic is real time traffic. Complying with the new requirements requires that network administrator ensures proper quality of service and has a good comprehension of VoIP technology.

The outcome of this thesis was commissioned by Tampere Polytechnic. The aim was to produce exercises that cover the management of quality of service in VoIP network using Cisco Systems devices. Finalized exercises where performed by students under my guidance and left at school for future usage. Exercises were designed to a course that is based on literature and devices produced by Cisco Systems. In the future, multicast features can be implemented to the exercises, if thought necessary.

Thesis examines all the main parts of VoIP technology and brings out the new requirements that are introduced to data networks. Thesis states features that Cisco devices include and which of them can be used to ensure sufficient quality of service to VoIP calls. Rest of the thesis describes the process of producing the exercises and analyzes the success of the lessons.

References related to ensure quality of service are mainly composed of materials published by Cisco, because all the devices are manufactured by it. Information about VoIP technology was also gathered elsewhere, for instance from sources independent of the manufacturer. The content and structure of the exercises are based on interviews of teachers who teach the subject and on my opinions as a student who has completed the course.

Keywords QoS Voice over IP DiffServ

Sisällysluettelo

1 Johdanto

Nykyisten puhelinverkkojen vanhahtava tekniikka ja korkea kustannustaso ovat siirtämässä puheluita perinteisestä puhelinverkosta IP-verkkoihin. Puheluiden siirtäminen IP-verkkoihin mahdollistaa puheliikenteen hallinnon siirtämisen IT-ylläpidon piiriin. Samalla on mahdollista vapautua puhelinverkon puhelukohtaisista maksuista ja erillisistä kaukopuheluhinnoista. Yritysten omien sisäverkkojen sisällä kulkevat puhelut mahdollistavat suurimmat puhelukohtaiset hyödyt.

Ääniliikenteen tuominen dataliikennettä kuljettavaan verkkoon asettaa verkolle uusia vaatimuksia, jotka ovat ominaisia reaaliaikaiselle liikenteelle. Näiden vaatimuksien täyttäminen vaatii uuden tekniikan omaksumista verkon ylläpitäjältä, sekä uusien ominaisuuksien käyttöön ottamista kaikilla verkkolaitteilla.

Tämän opinnäytetyön toimeksianto koostuu ääniliikenteen palvelun laadun varmistamiseen liittyvistä harjoitustehtävistä ja niiden teettämisestä opiskelijoilla. Pääasiallinen tavoite on tuottaa harjoitusmateriaali, joka antaa opiskelijoille mahdollisuuden tutustua VoIP (Voice over Internet Protocol) -tekniikan vaatimuksien huomioimiseen Ciscon kytkimillä ja reitittimillä. Sivutuotteena aihetta opettavat opettajat saavat tietoa uusista laitteista, joita he ovat saaneet opetusvälineiksi. Oppimateriaali on liitteenä (liite 1) opinnäytetyön lopussa.

Opinnäytetyössä käydään aluksi lyhyesti läpi olennaisia osia IP-verkosta. Tämän jälkeen selitetään VoIP-tekniikan keskeiset komponentit sekä niiden vaatimukset. VoIP-tekniikan vaatimuksien täyttämistä varten esitellään eri keinoja palvelun laadun varmistamiseksi. Erillinen kappale kuvaa harjoitustehtävissä käytettyjen laitteiden QoS (Quality of Service) -ominaisuudet. Loppuosa työstä kuvaa harjoitustehtävien tuottamiseen liittynyttä prosessia. Viimeisenä arvioidaan työn tuloksia ja suunnataan katse harjoitustehtävien jatkokehittämiseen.

Työ painottuu Cisco Systemsin laitteille, koska työn tuloksena muodostuneet harjoitukset on toteutettu Cisco Catalyst 2960 ja 3560 -sarjan kytkinten sekä 2620-sarjan reitittimien avulla. Lähdemateriaali koostuu pääasiassa Ciscon julkaisemista kirjoista ja verkkodokumenteista. QoS-ominaisuuksien esilletuonnissa olen pyrkinyt rajaamaan ne hyvin tarkasti Ciscon laitteiden ominaisuuksien mukaan.

Ciscon kirjallisuus on asiantuntevaa ja hyvin perusteltua, vaikka välillä sortuukin korostamaan omien teknisten ratkaisuiden paremmuutta ja jättää analysoimatta omien laitteiden puutteita. Osittain tämän takia tuon yleistä näkökulmaa aiheeseen laitteistoriippumattomista VoIP-kirjoista sekä eri standardien määritelmistä. VoIP-tekniikkaan liittyvät teokset käsittelevät aihetta hyvin tekniseltä näkökulmalta, mutta olen yrittänyt tulkita niitä QoS-tekniikan tarpeet huomioiden. Ciscon konfigurointioppaat

ovat mielestäni vaikealukuisia, joka johtuu osittain niiden laajuudesta. Ne kuitenkin sisältävät erittäin yksityiskohtaiset ohjeet ja selitykset laitteiden ominaisuuksista. Työn aihe on erittäin ajankohtainen, ja se ilmenee VoIP-tekniikkaa käsittelevien lehtiartikkeleiden määrän kasvuna, joista työssäni mainitsen muutamia.

Harjoitustehtävien rakennetta ja sisältöä lähdin rakentamaan kurssia opettaville opettajille tekemäni haastattelun pohjalta. Heidän kokemuksensa Cisco Systemsin laitteista ja niiden opettamiseen käytetyistä opetustavoista antavat minulle mahdollisuuden hyödyntää heidän ammattitaitoaan.

Tämän opinnäytetyön sisällön ymmärtäminen edellyttää, että lukija hallitsee verkkotekniikan perusteet (esim. CCNA- ja CCNP-kurssien sisällön), jotta käsitelty aihe tulee täysin ymmärretyksi.

2 Työn tausta ja tarkoitus

TAMKin tietojenkäsittelyn koulutusohjelmassa on valittavissa kaksi Cisco Systemsin tuottamaan materiaaliin ja laitteisiin pohjautuvaa kurssia. Kurssit ovat laajuudeltaan 10 ja 15 opintopistettä, ja molemmat kestävät yhden kokonaisen lukukauden. Niiden opetus tähtää Ciscon CCNA- ja CCNP-sertifikaattien sisällön hallitsemiseen. Kursseja pitävien opettajien (Haapakangas 6.11.2006, haastattelu; Hakonen 31.10.2006, haastattelu) mielestä jälkimmäisellä kurssilla esiintyvä VoIP-materiaali ja siihen liittyvä palvelun laadun varmistaminen ovat teoriasisällöltään puutteelliset. Haastateltujen mielestä myös QoS:n liittyvät asiat ovat huonosti jäsenneltyjä. Lisäksi VoIP:iin liittyvät harjoitteet ovat mahdottomia toteuttaa nykyisellä laitekannalla.

Käsittelen työssä IP-tekniikasta vain VoIP-tekniikkaan liittyvät keskeiset osat. Työ perustuu vallitsevaan ipv4-tekniikkaan ja jättää tulevaisuuden tarpeisiin kehitetyn ipv6-tekniikan käsittelemättä. VoIP-tekniikka käsitellään tärkeimpien komponenttien osalta sekä hieman laajemmin sen tuomia vaatimuksia IP-verkolle. Tärkeimpänä aiheena työssä on palvelun laadun varmistaminen ääniliikenteen näkökulmasta Ciscon kytkinten ja reitittimien osalta. Erityisen tärkeä osa-alue on lähiverkkotekniikan QoS-ominaisuudet. Näitä ominaisuuksia käsittelen vielä perusteellisemmin harjoituksiin käytettävissä olevien laitteiden osalta. WAN (Wide Area Network) -tekniikan käsittelen hyvin yleisellä tasolla. Siitä jätän mm. vähenemässä määrin käytetyn FrameRelay-tekniikan kokonaan käsittelemättä.

Olen työstänyt aihetta Ciscon laitteiden toiminnallisesta näkökannasta. Työssä on keskitytty toimeksiantoon liittyvien kytkinten QoS-ominaisuuksiin ja raotettu hieman Ciscon reitittimien QoS-ominaisuuksien kirjoa. Työssä ei paneuduta aiempien eikä uudempien laitteiden ominaisuuksiin, mutta niistä saatetaan mainita.

Harjoitustehtävissä varmistetaan ääniliikenteen saama palvelun laatu esittämällä yksi mahdollinen ratkaisukeino vallitsevaan tilanteeseen. Tämän vuoksi kyseiseen ratkaisumalliin liittyvät QoS-toimet käydään työssä perusteellisemmin läpi. Muita mahdollisia QoS-toimia sivutaan ja tuodaan esille siinä määrin, kuin olen nähnyt tarpeelliseksi. Harjoitustehtävien sisältöön ja rajaamiseen paneudun harjoitustehtäviä kuvaavassa luvussa.

3 IP-tekniikka

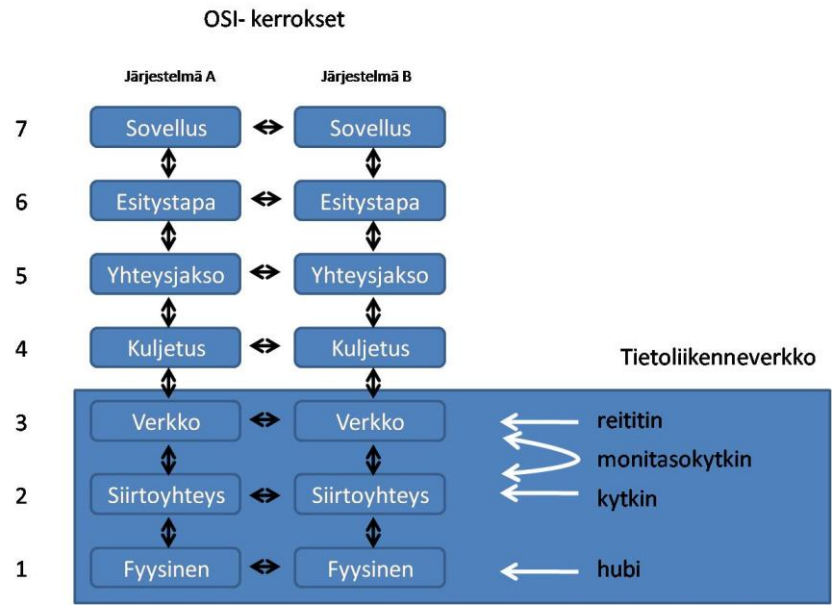
IP-tekniikka on levinnyt nykyisten tietoverkkojen tärkeimmäksi tekniikaksi. Tämä luku käsittelee IP-tekniikasta keskeisimpiä protokollia ja OSI (Open Systems Interconnection) -viitemallia. Näiden käsitteiden ja tekniikoiden ymmärtäminen on välttämätöntä, jotta VoIP-tekniikkaa pystytään käsittelemään tarkemmin.

3.1 OSI-viitemalli

OSI on ISOn (International Organization for Standardization) kehittelemä *viitemalli*, jonka tarkoituksena on standardisoida protokollia. Se jakaa protokollien toiminnan *seitsemään kerrokseen*. OSI-mallia käytetään yleisesti uusien protokollien kehityksessä ja tietoliikenteen opetuksen välineenä. (Davidson & Peters 2002: 151.)

OSI:n seitsemän kerroksen tarkoitus on eriyttää verkon tietoliikenneongelmakohdat toisistaan. Tämä tarkoittaa sitä, että yhden kerroksen täytyy pystyä kommunikoimaan vain toisessa koneessa olevan saman kerroksen kanssa. Vaikka kerros ei kommunikoi muiden kerrosten kanssa, se kuitenkin palvelee ylempien kerrosten toimintoja ja tarvitsee palveluja alapuolella olevilta kerroksilta. (Davidson & Peters 2002: 151.)

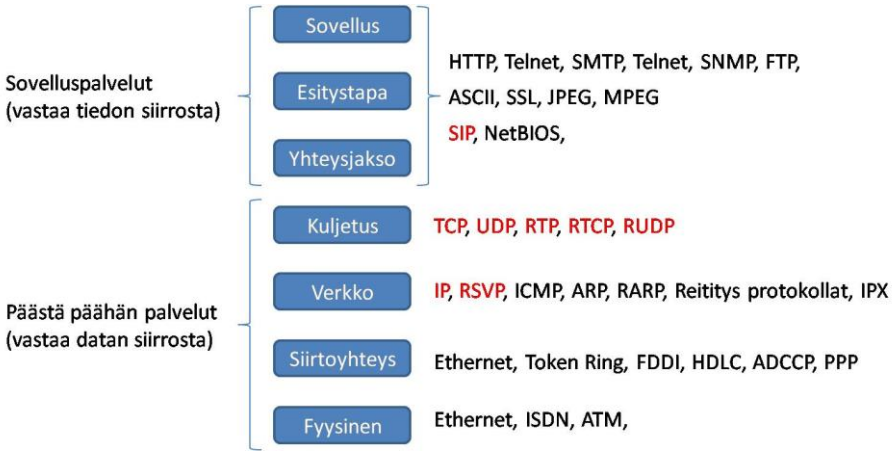
Kuva 1 havainnollistaa OSI-mallia. Siitä voidaan nähdä kaikki seitsemän eri kerrosta. Kuva osoittaa tietoliikenneverkon toimintojen sijoittumisen kolmelle alimmaiselle kerrokselle. Tietoliikenneverkon laitteille on osoitettu myös kerros, jolla ne toimivat. Myöhemmin työssä käytetään OSI-mallin mukaisia kerroksia selvittämään, missä protokolla toimii.



Kuva 1: OSI-viitemalli

3.2 Protokollat

IP-verkossa toimii monia eri protokollia kaikissa OSI-mallin kerroksissa. Kuvassa 2 on korostettu ne protokollat, joiden toiminta tulee ymmärtää, jotta VoIP-tekniikkaa pystytään käsittelemään ymmärrettävällä tavalla. *IP-protokolla* on keskeisin komponentti IP-verkossa. Tämän päällä käytetään normaalisti TCP (Transmission Control Protocol)- tai UDP (User Datagram Protocol) -kehystä. VoIP-liikenne käyttää yleisesti UDP-kehystä yhdessä RTP (Real-time Transport Protocol) -protokollan kanssa. Näiden lisäksi ääniliikenne saattaa käyttää RTCP (Real-Time Transfer Control Protocol)- tai RUDP (Reliable User Protocol) -protokollaa.



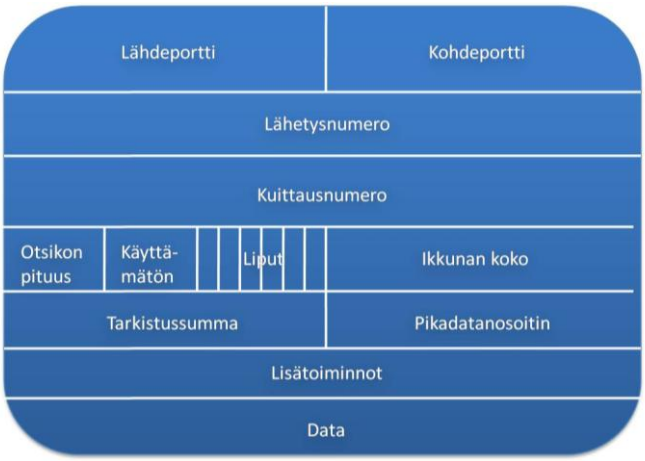
Kuva 2: Protokollat OSI-viitemallissa

3.2.1 IP

IP-protokolla sijaitsee OSI-mallin kolmannella kerroksella. Sen tehtäviin kuuluu pakettien fragmentointi, liikenteen reititys ja yksilöllisen osoitteistuksen tarjoaminen. Se on yhteydetön protokolla, mikä mahdollistaa pakettien reitityksen eri reittejä pitkin molempiin liikennesuuntiin. IP-protokolla ei anna varmuutta siitä, että paketit lähetettäisiin oikein. Tätä tehtävää varten käytetään ylemmän kerroksen protokollia kuten TCP:tä. Myöhemmin alaluvun 5.3.2 kuvissa 9 ja 10 esitellään IP-paketin otsikkokentät ja niiden selitykset.

3.2.2 TCP

TCP on yhteydellinen protokolla, jonka tarkoitus on luoda luotettava yhteys epäluotettavassa verkossa. Tämä tarkoittaa sitä, että jokaista datavirtaa, joka osapuolten välillä siirretään, edeltää yhteyden synkronointiprosessi. Synkronointi varmistaa, että molemmat osapuolet ovat valmiita vastaanottamaan lähetyksen ja pakettien järjestysnumerot ovat molemmilla tiedossa. Järjestysnumeroinnin avulla TCP pystyy uudelleen järjestelemään eri aikaan saapuneet paketit ja varmistamaan, että kaikki paketit ovat saapuneet. (Tanenbaum 2003: 532-552.) Kuvasta 3 voidaan nähdä TCP-kehyksen rakenne.



Kuva 3: TCP-kehys

TCP luo virtuaalisen yhteyden lähettäjän ja vastaanottajan välille, mikä tarkoittaa, että yhteyden muodostaminen tapahtuu verkon päästä päähän. TCP-yhteyden liikenteen hallinta tapahtuu seuraavasti. Ensin lähettävä osapuoli lähettää vastaanottavalle osapuolelle sovitun määrän paketteja, jonka jälkeen vastaanottaja lähettää kuittauksen onnistuneesti vastaanotetuista paketeista. Mikäli paketteja ei kuitata saapuneiksi, lähetetään ne automaattisesti uudestaan. Jos vastaanottaja jatkaa pakettien kuittaamista yhtäjaksoisesti, yrittää lähettäjä nostaa lähetysnopeutta. Lähetysnopeutta kasvatetaan kunnes uudelleenlähetysten määrä alkaa nousta ja kuittauspyyntöjä ei saavu toistuvasti. Tällöin TCP aloittaa lähetysnopeuden hidastamisen. Kuittausten jälleen saapuessa normaalisti yhteysnopeuden pudottaminen lopetetaan. Jos taas paketit kuitataan onnistuneesti saapuneiksi toistuvin ajanjaksoin, aloitetaan nopeuden nostaminen uudestaan. (Tanenbaum 2003: 532-552.)

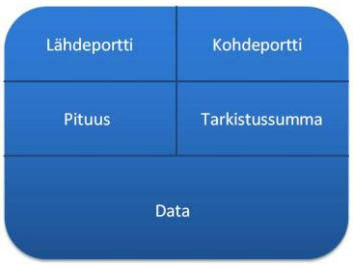
Edellä kuvatusta liikenteen hallinnasta seuraa, että TCP-liikenne pystyy mukautumaan verkonkäyttöasteen vaihteluihin. Varjopuolena TCP:n toimintatavassa ovat kadonneet paketit, jotka haittaavat erityisesti reaaliaikaisia sovelluksia. Vaikka paketti lähetetäänkin uudestaan, tapahtuu lähetys monesti liian myöhään, jotta siitä olisi mitään hyötyä.

3.2.3 UDP

UDP on IP-paketin päällä toimiva yhteydetön protokolla. Sen sisältämän porttinumerotiedon perusteella voidaan kohteessa erotella liikennevirtoja toisistaan. UDP soveltuu ääni- ja videoliikenteen kuljettamiseen TCP:tä paremmin, vaikka se ei sisällä luetettavan tiedonsiirron ominaisuuksia. Sen etu on katkeamaton lähetys ilman ylimääräisiä kuittauskomentoja.

UDP-kehys rakentuu neljästä kahden tavun otsikkokentästä ja lopussa sijaitsevasta datakentästä. Otsikkokentät ovat lähdeportti, kohdeportti, pituus ja tarkistussumma. Kuva 4 esittää UDP-kehyksen rakenteen. Lähde-

ja kohdeportit erottavat liikennevirrat toisistaan. Pituuskenttä määrittelee UDP-otsikon ja dataosuuden yhteyspituuden. Tarkistussummakenttää käytetään paketin eheyden tarkistukseen, mutta se ei ole pakollinen. Otsikkotietojen jälkeen tuleva datakenttä sisältää kuljetettavan datan.



Kuva 4: UDP-kehys

3.2.4 RTP

RTP on kuljetuskerroksen protokolla, joka kuljettaa reaaliaikaista liikennettä IP-verkoissa. Sitä käytetään yleisimmin UDP-protokollan kanssa, koska se mahdollistaa kanavoinnin (usean linjan yhdistäminen yhdeksi) ja virhesumman laskemisen paketeille. RTP ei takaa pakettien oikeaa saapumisjärjestystä eikä muitakaan laadunvarmistuskeinoja. Se sisältää tiedon kehyksen järjestyksestä, aikaleimasta, kuljetettavan datan tyypistä ja toimituksen seurannasta. On hyvä huomioida, että vaikka RTP on yhteydetön protokolla, se mahdollistaa kadonneiden pakettien seurannan järjestysnumeroiden avulla. (RFC 3550… 2003: 4.) Laadunvarmistus toteutetaan ylemmän kerroksen protokollilla, jotka saavat tarvittavat tietueet RTP:ltä.

3.2.5 RTCP

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. RTCP:n toiminta perustuu tietyin aikavälein kaikille osapuolille lähetettäviin paketteihin. RTCP:n mahdollistamien tietojen perusteella ylemmän OSI-kerroksen ohjelmat voivat muokata toimintaansa voimassaolevalle yhteydelle sopivaksi. (RFC 3550… 2003: 18-19.)

3.2.6 RUDP

RUDP on muunnelma UDP protokollasta. Se lisää liikennöinnin luotettavuutta tavalliseen UDP protokollaan verrattuna lähettämällä samoja paketteja useita kertoja peräkkäin. Vastaanottajan tehtävä on hylätä toistuvat paketit. Tällä tavalla saadaan saapumistodennäköisyyttä kasvatettua, koska todennäköisemmin ainakin yksi samanlaisista paketeista saavuttaa vastaanottajan. Haittapuolena tästä seuraa huomattavasti suurempi kaistan käyttö. (Davidson & Peters 2002: 171.)

4 VoIP

Tietoverkoissa on perinteisesti totuttu siirtämään tietoa, joka ei ole herkkä viiveelle eikä sen vaihteluille. Uudehkoina tulokkaina tietoverkkoihin ovat vakiintumassa reaaliaikaiset toteutukset, kuten äänipuhelut, videoneuvottelut sekä streaming-sovellukset. Esimerkiksi Rapon (2006: 15) mukaan vuoden 2006 loppupuolella Yhdysvalloissa jo yli 60 % yritysten puheluista tehtiin IP-pohjaisena, mikä on kaksinkertainen määrä kahden vuoden takaiseen lukuun verrattuna. Salovuori (2006: 15) puolestaan toteaa, että Suomessa kasvu on vasta alkamassa ja IP-puhelinvaihteisiin ollaan siirtymässä enenevässä määrin.

Kaikille reaaliaikaisille sovelluksille on yhteistä pieni sietokyky verkossa esiintyville viiveille. Ääniliikenne vaatii nykyisiltä verkoilta uuden tekniikan käyttöönottoa, pientä viiveen tasoa, pientä värinän tasoa ja luetettavaa pakettien perille menoa. Näitä vaatimuksia voi joiltakin osin yleistää myös muihin reaaliaikaisiin sovelluksiin.

VoIP-verkkoa rakennettaessa verkon rakenne ja verkkolaitteet yhdessä esivalintaisten toimenpiteiden, kuten sopivan koodekin valinta, vaikuttavat ratkaisevasti laitteiden konfigurointitarpeisiin. Pelkästään varaamalla riittävästi kaistaa kaikelle mahdolliselle verkkoliikenteelle vältytään monilta ongelmilta. Kaistan suhteeton ylivaraaminen, jonka tarkoituksena on tasata verkon ruuhkahuippuja, on monesti resurssien tuhlausta. Taloudellisempi ratkaisu on taata riittävä palvelun laatu aivan keskeisimmille palveluille verkon ruuhkahuippuina.

Ääniliikennettä siirretään pääasiassa IP/UDP/RTP-paketilla. Vaikka TCP tarjoaa luotettavuutta ja se pystyy lähettämään kadonneen paketin uudelleen, eivät sen ominaisuudet tuo parannusta ääniliikenteeseen. Uudelleen lähetetty paketti saapuu joka tapauksessa liian myöhään, ja palvelun laadun heikkeneminen on jo päässyt tapahtumaan.

4.1 Standardit

Tärkeimmät telealan ja VoIP-tekniikan standardoinnista vastaavat järjestöt ovat IETF (The Internet Engineering Task Force), ITU-T (International Telecommunication Union – Telecommunication standardization sector), ETSI (European Telecommunications Standards Institute) ja SFS (Suomen Standardoimisliitto). Ne luovat yleisiä suosituksia ja standardeja, jotka pyrkivät yhtenäistämään alan toimintaa. Vaikka standardeja suunnitellaan jatkuvasti, eivät ne monesti ole uusimpien innovaatioiden tasolla. VoIP-tekniikka on ollut hyvin pitkään yhteensopiva vain saman laitevalmistajan laitteiden kanssa, mutta uusien standardien kehittymisen ja käyttöönoton myötä, nykyään on jo mahdollista rakentaa heterogeenisiä VoIP-verkkoja. Standardien tärkeyden takia haluan tuoda niistä tärkeimpiä esille ja selventää hiukan niiden alkuperää.

4.1.1 IETF

IETF on avoin kansainvälinen yhteisö, jonka tarkoituksena on tukea Internetin arkkitehtuuria ja sen sulavaa toimintaa. Yhteisön jäseneksi voi pyrkiä kuka tahansa. Yhteisön jäsenet on jaettu aihekokonaisuuksien mukaisesti omiksi työryhmiksi. Työryhmät luokitellaan edelleen omiin aluekokonaisuuksiin, joilla jokaisella on oma johtajansa. Pääasiallinen toiminta ja uusien suositusten tuottaminen tapahtuu sähköpostilistojen avulla, sekä muutamalla yhteisellä kokoontumisella vuoden aikana. Yhteisön oma toiminta ja sen tarkoitus on kuvattu IETF:n omissa dokumenteissa RFC 3935, RFC 3978, RFC 4748 ja RFC 3979. (Swale 2001: 105-110.)

IETF:n julkaisemat dokumentit ovat I-D (Internet-Draft) ja RFC (Request for Comments). I-D-dokumentteja voi julkaista kuka tahansa, jos vain lähettää oikean formaatin omaavan dokumentin IETF:n sihteerille. Dokumentit ovat monesti RFC-dokumenttien työstövaiheen julkaisuja. (Swale 2001: 105-110.)

Itse RFC-dokumentit ovat IETF:n julkaisuja, ja ne voivat sijoittua yhteen viidestä kategoriasta. Kategorioita ovat Standards Track, Best Current Practice, Informational, Experimental ja Historic. RFC-dokumentti voi siirtyä yhdestä kategoriasta toiseen. Standards Track -kategoriassa olevat RFC:n julkaisut ovat sellaisenaan yleisiä standardeja. Standardiksi pääseminen vaatii Proposed standard ja Draft standard -välivaiheen läpäisyä. Näiden kahden vaiheen jälkeen standardista tulee Internet Standard, ja vasta silloin sitä pidetään yleisenä hyväksyttynä standardina. Best Current Practise -kategorian dokumentit ovat IETF:n näkemyksiä jostakin aiheesta, mutta se ei tee niistä vielä Internetin laajuista standardia. Loput kategoriat ovat niitä dokumentteja varten, jotka ovat kokeiluluontoisia tai tutkimustietoa omaavia. (IETF n.d.)

4.1.2 ITU-T

ITU (The International Telecommunication Union) on kansainvälinen organisaatio, joka toimii YK:n alaisuudessa. ITU:n yksi kolmesta toiminnallisesta sektorista on telestandardointisektori nimeltään ITU-T. Se tutkii ja tekee suosituksia televiestintään liittyen. ITU-T:n suositukset ovat standardin omaisia, ja niitä noudatetaan maailmanlaajuisesti. Suomea järjestössä edustavat Liikenne- ja viestintäministeriö yhdessä Viestintäviraston kanssa. (Viestintävirasto – ITU-T 2006.)

4.1.3 ETSI

ETSI on voittoa tuottamaton Euroopassa toimiva telealan standardoimisjärjestö. Sen jäseniksi voivat liittyä ainoastaan eurooppalaiset telealan operaattorit, laitevalmistajat, telepalveluiden käyttäjäjärjestöt, telepalveluiden tarjoajat, tutkimuslaitokset ja konsultointiyritykset. ETSI:n dokumentit voidaan jakaa EN-standardeihin, teknisiin TR-raportteihin, teknisiin TS-specifikaatioihin, EG-ohjeisiin ja ES-standardeihin. ETSIn kotisivut löytyvät osoitteesta http://www.etsi.org, josta on myös mahdollista nähdä ilmaiseksi kaikki julkaistut dokumentit. (Viestintävirasto – ETSI 2006.)

4.1.4 SFS

SFS on riippumaton voittoa tavoittelematon yhdistys, jonka tehtävä on kansallisten standardien ohjaaminen, koordinointi ja vahvistaminen. Sen jäsenet muodostuvat elinkeinoelämän järjestöistä ja Suomen valtiosta. Itse yhdistys on jäsenenä ISOssa ja eurooppalaisessa standardisoimisjärjestössä CEN:ssä (European Committee for Standardization). (Suomen Standardisoimisliitto SFS n.d.) SFS:n julkaisemat standardit liittyen ääniliikenteeseen ovat pääasiassa televerkon standardeja perinteiseen puhelinverkkoon liittyen.

4.2 Tekniikka

Jotta VoIP-liikenteen on mahdollista siirtyä verkossa, tarvitaan siihen erilaisia teknisiä laitteita ja tiedonsiirtämiseen sopivat protokollat. Ensinnäkin tarvitaan laite, joka käsittelee puhetta ja siirtää sen verkkoon. Tähän voidaan käyttää itsenäisiä IP-puhelimia, tai samat toiminnot voidaan toteuttaa tietokoneen avulla. Erillinen IP-puhelin on helppokäyttöinen eikä vaadi itsensä lisäksi mitään muuta toimiakseen. Tietokoneen avulla voidaan IP-puheluita soittaa Softphone ohjelmistolla. Se edellyttää toimiakseen äänikortin lisäksi joko USB-liitäntäisen IP-puhelimen tai kaiuttimet ja mikrofonin.

Itse äänen siirtämiseen tietoverkoissa tarvitaan jokin yhteydenantoprotokolla. Yleisimpiä ja laajimmin käytössä olevia protokollia ovat SIP (Session Initiation Protocol) ja H.323. Lisäksi IP-puhelujen soittamista helpottavia ohjelmistoja on lukuisia. Näistä merkittävin lienee IP-puhelinvaihteen käyttäminen. Se mahdollistaa VoIP-liikenteen ohjaamisen tietoverkoissa sekä soittajaprofiilien ylläpitämisen.

VoIP-liikenteessä yhteyden muodostaminen ja ääniliikenne on eroteltu toisistaan erillisiksi datavirroiksi. Tämä mahdollistaa näiden kahden liikenteen reitityksen eriyttämisen ja antaa IP-puheluiden hallinnoinnille lisää mahdollisuuksia.

IP-puhelu voidaan muodostaa suoraan kahden soittajan välille. Tällöin yhteydenmuodostus tapahtuu suoraan molempien osapuolien välillä, kuten myös äänidatan siirto. On kuitenkin tavanomaista, että soittajien välissä käytetään palvelinta, joka ohjaa ja hallitsee yhteydenmuodostamista. Itse äänidata siirtyy edelleen suoraan soittajalta soittajalle. Palvelimen avulla voidaan mm. hallita tilanteita, joissa vastaanottaja ei ole tavoitettavissa. (Swale 2001: 16-17.)

4.2.1 IP-puhelimet

IP-puhelimia on olemassa hyvin monenlaisia lähtien erillisistä puhelimista aina PC-tietokoneisiin integroituihin ohjelmallisiin puhelimiin. IP-puhelimen mallista ja toteutustavasta riippuen se on rakennettu toimimaan joidenkin VoIP-protokollien kanssa, ja sen toiminnallinen kuva on monesti laitteistovalmistajan omien verkkotopologiamääreiden mukainen. Jo jonkin aikaa IP-puhelimet on rakennettu toimimaan saman valmistajan laitteilla, mutta standardoitujen protokollien yleistyessä, kuten SIP, ne toimivat yhä laajemmin myös muissa verkoissa. IP-puhelimilla on omat erityisvaatimuksensa tavallisiin lankaverkonpuhelimiin verrattuna. Näihin vaatimuksiin kuuluvat IP-osoitehallinta, mediayhdyskäytävään rekisteröityminen, käytettävän VoIP-protokollan hallinta ja sähköverkkoliitäntä. (Ellis, Pursell & Rahman 2003: 119.)

IP-softapuhelin tekee samat toimenpiteet kuin tavallinen IP-puhelin. Se asennetaan johonkin valmiiseen laitteistoon, kuten PC-tietokoneeseen, kannettavaan tietokoneeseen tai PDA (Personal Data Assistant) -laitteeseen. Laitteistosta täytyy löytyä äänikortin lisäksi mikrofoni ja kaiuttimet tai kuulokemikrofoniyhdistelmä. Yleistä on myös käyttää USB (Universal Serial Bus) -liitäntään liitettävää IP-puhelinta yhdessä IP-puhelinsovelluksen kanssa. Tämä tuo tavallisen puhelimen helppokäyttöisyyden tietokoneen avulla soitettaviin puheluihin.

4.2.2 IP-puhelinvaihde

IP-puhelinvaihteen tarkoitus on hallita puhelujen muodostumista. Yksi vaihtoehto puhelinvaihderatkaisuksi on IP-PBX (IP Private Branch Exchange) -järjestelmä. IP-PBX on tavallisen PC-tietokoneeseen asennettava puhelinkeskusohjelmisto. IP-BPX koostuu puhelupalvelimesta, ääniyhdyskäytävästä, asiakaspäätteistä ja lisäarvo-ohjelmistoista. Jokainen näistä elementeistä tarvitsee yhteyden muihin elementteihin IP-verkon välityksellä. (Swale 2001: 78-82.) IP-PBX:n tarkoitus ei ole reitittää itse ääniliikennettä, vaan huolehtia ääniyhteyksien muodostamisesta. Ääniliikenteen reitittämisestä huolehtivat IP-verkon laitteet ja protokollat.

4.2.3 VoIP gateway

VoIP gateway on laite, joka mahdollistaa puheliikenteen reitittämisen PSTN (public switched telephone network) ja IP-verkon välillä. Siihen on mahdollista integroida myös muita toimintoja liittyen esim. puhelujen reititykseen ja äänen pakkaamiseen.

4.2.4 SIP

SIP on määritelty RFC 3261 -dokumentissa. Se on sovelluskerroksen protokolla, joka voi muodostaa, muuttaa ja sulkea multimediayhteyksiä tai -puheluja. Se kykenee kutsumaan henkilöitä ja palveluja unicast- ja multicast-istuntoon. Kutsujan ei tarvitse itse olla osallisena istunnossa. (Ellis ym. 2003: 199.)

SIP:n käyttämä osoitteistustapa, jolla se yksilöi soittajaosapuolet, on nimeltään SIP URL (Universal Resource Locator). SIP URL:n syntaksi on muotoa *sip*:*password@host*. Syntaksin eri osat tarkoittavat seuraavaa:

sip	määrittelee käyttäjän SIP-numeron, joka voi muodostua kirjaimista ja/tai numeroista
password	määrittelee käyttäjän henkilökohtaisen salasanan, jonka avulla käyttäjä pystytään identifioimaan
host	määrittelee käyttäjän IP-osoitteen tai toimialuenimen ja mahdollisesti :-merkin jälkeen tarvitsee vielä käytettävän porttinumerotiedon

Vaikka SIP käyttääkin omaa tapaa osoitteistuksessa, voidaan se liittää tavalliseen puhelinverkkoon. Tämän jälkeen puheluja voidaan soittaa siellä oleviin puhelinnumeroihin. (Ellis ym. 2003: 199-201.)

SIP:n ominaisuudet mahdollistavat nimikäännökset, puhelun uudelleen ohjauksen ja muiden yhteydenmuodostusprotokollien yhteenliittymän (esim. H.323:n kanssa). SIP:llä yhteys voidaan muodostaa suoraan kahden osapuolen välillä tai hoitaa erillisen serverin välityksellä.

SIP tukee viittä eri toimintoa liittyen multimediayhteyksien aloittamiseen ja lopettamiseen. Toiminnot ovat:

käyttäjän sijainti:	kommunikointiin käytettävän järjestelmän määrittely
käyttäjän saavutettavuus:	määritys soitettavan kohteen halukkuudesta ottaa puhelu vastaan
käyttäjän ominaisuudet:	käytettävien mediaominaisuuksien määritys

yhteyden muodostus:	yhteyden muodostamiseen liittyvät toiminnot kuten soittoääni
yhteyden hallinta:	liikenteen siirtäminen, yhteyksien päättäminen, yhteyden parametrien muokkaus, palveluiden aktivoiminen

(IETF 3261… 2002.)

4.2.5 H.323

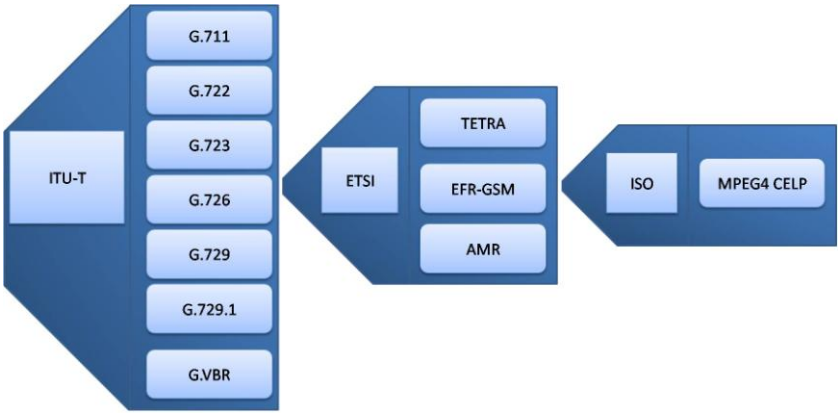
H.323-protokollaperhe määrittelee puhelun merkinannon, median ohjauksen, käytettävän ääni- ja videokoodekin, datan jakamisen ja median kuljetustavan. Se on ITU-T:n suositus siitä, miten ääntä ja videota lähetetään Internetin ja intranetin ylitse IP:n avulla. H.323:en kuuluvat protokollat ovat lueteltu taulukossa 1.

Taulukko 1: H.323-protokollaperheen protokollat (Davidson & Peters 2002: 231)

Piirre	Protokolla
Puhelun merkinanto	H.225
Median ohjaus	H.245
Äänikoodekit	G.711, G.722, G.723, G.728, G.729
Videokoodekit	H.261, H.263
Datan jakaminen	T.120
Median kuljetus	RTP/RTCP

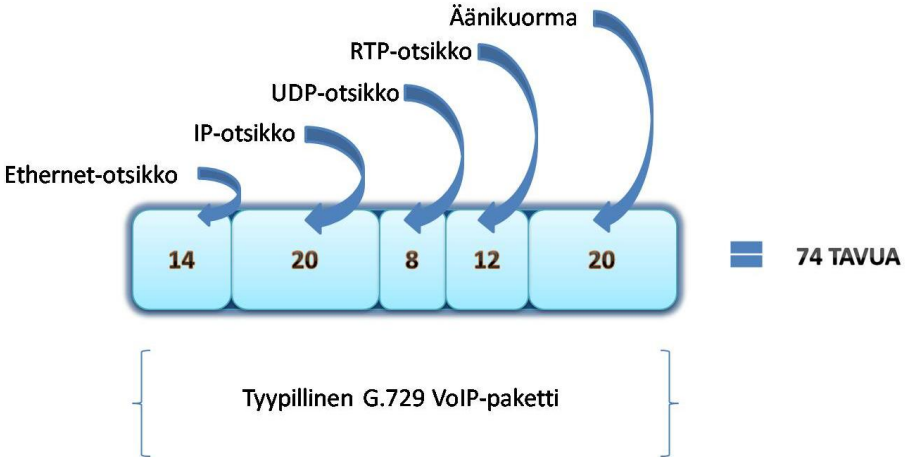
4.2.6 Koodekki

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. Kuvassa 5 on lueteltu tunnetuimpia ja käytetyinpiä koodekkeja VoIP-liikenteessä.



Kuva 5: Yleisesti tunnetut ja käytössä olevat koodekit

Kuvasta 6 voidaan nähdä tyypillisen G.729-koodekin muodostaman paketin rakenne. OSI:n 2-kerroksen muodostaman otsikon koko määräytyy käytössä olevasta 2-kerroksen tekniikasta.



Kuva 6: G.729 VoIP-paketin rakenne

4.3 Vaatimukset verkolle

VoIP-tekniikka asettaa omat vaatimuksensa tietoverkoille. Suurimpia haasteita aiheuttaa ääniliikenteen reaaliaikaisuus. Lisäksi on huomioitava, että reaaliaikaisuuden asettamien vaatimuksien laiminlyöminen näkyy suoraan loppukäyttäjillä. Ääniliikennettä implementoidessa verkkoon huomio tulee kiinnittää ainakin viiveeseen, värinään, pakettien katoamiseen, kaikuun ja puheen taukojen poistoon.

4.3.1 Viive

Viiveellä (latency) tarkoitetaan sitä aikaa, joka kuluu äänen lähtiessä puhujan suusta ja päätyessä kuulijan korvaan (Davidson & Peters 2002: 167). Viivettä lisäävät kaikki osatekijät, jotka ovat äänen matkanvarrella

sen siirtyessä lähteestä kohteeseensa. Nostan niistä viisi mielestäni merkitsevintä esille. Ne ovat levitys-, käsittely-, sarjoitus-, jonotus- ja sovellusviive. Näistä kolmea ensimmäistä esiintyy kaikissa puhelinverkoissa. Jonotusviive on ominaista nimenomaan pakettipohjaisille verkoille, ja sovellusviivettä esiintyy lähinnä ohjelmallisissa IP-puhelimissa.

Levitysviivettä muodostuu kaikissa nykyisissä verkoissa bittien siirtyessä laitteesta toiseen. Laitteiden välillä olevat kaapelit ovat pääasiassa joko kupari- tai kuitukaapeleita. Niiden siirtokyky määrittelee aiheutetun levitysviiveen suuruuden. Luonnollisesti välimatkojen kasvaessa levitysviive kasvaa, ja sen osuus kokonaisviiveestä nousee.

IP-pakettien kulkiessa verkkolaitteiden lävitse jokainen laite joutuu käsittelemään pakettia jollakin tavalla. Tästä aiheutuu *käsittelyviivettä*. Käsittelyviiveeksi määritellään myös puhenäytteiden koosta ja määrästä aiheutuvat viiveet. Puhenäytteellä tarkoitetaan puheesta otettavaa näytettä. Puhenäytteen koko riippuu käytettävästä koodekista. Kokonaisviive kasvaa, kun verkkolaitteiden ja liikenteeseen kohdistuvien toimenpiteiden määrä kasvaa. On olemassa myös *sarjoitusviivettä*, joka johtuu bitin tai tavun viemisestä rajapinnalle, mutta sen osuus on todella pieni kokonaisviiveestä.

Pakettiliikenteelle on ominaista, että laitteelle saapuneet paketit asetetaan tulostusjonoon ja näin muodostetaan verkkoon *jonotusviivettä*. Tulostusjonon tarkoitus on säilyttää paketti siihen asti, kunnes rajapinta, jolle pakettia ollaan asettamassa, on vapaana. Sen pääasiallinen tarkoitus on palvella ruuhkatilanteiden käsittelyä. Ruuhkainen verkko lisää jonojen pituutta, koska mitä kauemmin paketti on jonossa, sitä enemmän viivettä jonottamisesta muodostuu. (Davidson & Peters 2002: 168-169.)

Sovellusviivettä esiintyy täysin ohjelmallisesti toteutetussa IP-puhelimessa. Tällaisesta ohjelmasta käytetään yleisesti nimitystä Softphone. Softphone on tavallinen ohjelmisto, joka toimii jonkin käyttöjärjestelmän päällä ja on yhteydessä tämän kautta äänikortin toimintoihin. Äänikortin ja IP-puhelinohjelmiston välille voi muodostua viivettä, koska käyttöjärjestelmän toimintaan kuuluvat erilaiset välimuistitus- ja keskeytyspyyntökomennot. Nämä voivat yhdessä lisätä end-to-end-viivettä Windows ympäristössä ajurista riippuen jopa 60 ms. Tämäkin tulee huomioida laskettaessa kokonaisviivettä. (Hersent, Petit & Gurle 2005: 101.)

End-to-end-viiveen kasvaessa äänenlaatu heikkenee samassa suhteessa. ITU-T:n G.114 (ITU-T G.114… 2003) suosituksen mukaan yhteen suuntaan kohdistuva end-to-end-viive ei saa ylittää raja-arvoa 150 ms. Raja-arvon alla pysyttelevä kokonaisviive takaa äänen korkean laadun. Jos esimerkiksi viive kasvaa yli 250 ms, voi äänipuhelussa aiheutua toisen puheen päälle puhumista (talk-over). Suuresta viiveestä voi siis seurata tilanteita, joissa molemmat osapuolet puhuvat päällekkäin, koska vastapuoli aloittaa puhumisen, vaikka toinen osapuoli onkin jo aloittanut kes-

kustelun. Tilanteessa ensimmäisenä puheen aloittaneen ääni ei ole yksinkertaisesti vielä saavuttanut toista osapuolta, ja tästä johtuen vastapuoli luulee aloittavansa itse keskustelun. (Ellis ym. 2003: 83.)

4.3.2 Värinä

Värinällä (jitter) tarkoitetaan sitä ajallista vaihtelua, joka eri pakettien saapumisajankohdissa esiintyy. Voidaan myös sanoa, että se on paketin saapumisajankohdan ja oletetun saapumisajankohdan välinen erotus. Värinää esiintyy pakettikytkentäisissä verkoissa, koska jokainen paketti kulkee erillään toisista paketeista. Näin ollen eri paketit voivat hidastua eri syistä ja matkata saman matkan eri nopeudella. Yhteen lähetyssuuntaan kohdistuvan värinän tason tulee olla alle 30 ms (Szigeti & Hattingh 2005: 33).

Värinä itse aiheuttaa äänen laadun heikkenemistä ja tätä kompensoimaan onkin kehitetty erilaisia värinäpuskureita. Niiden tarkoitus on vähentää pakettien välistä aikaeroa puskuroimalla liikennettä. Toteutukset tästä vaihtelevat staattisista puskureista dynaamisiin puskureihin. Ciscon ratkaisu on dynaaminen puskuri, joka suurenee ja pienenee sen mukaan, mitä viiveiden vaihtelun perusteella on ennustettavissa. (Davidson & Peters 2002: 171). Jos värinää yritetään estää puskuroimalla, aiheutuu siitä sivutuotteena viivettä, koska osa liikenteestä joutuu odottamaan puskurissa.

4.3.3 Pakettien katoaminen

Pakettien katoamisella (packet loss) tarkoitetaan tilannetta, jossa paketti lähetetään kohti vastaanottajaa, mutta paketti ei koskaan saavu perille. Ääniliikenteen kannalta jokainen pudonnut paketti tarkoittaa, että vastaanottaja ei kuule osaa lähetyksestä. Ihmisen korva antaa jonkin verran anteeksi, kunhan putoamiset tapahtuvat satunnaisesti. Peräkkäiset pakettien putoamiset puolestaan aiheuttavat kuultavia katkoja. Pakettien häviämistä voidaan olennaisesti vähentää verkonsuunnittelulla ja palvelun laadun hallinnalla. Yhden paketin häviämisen vaikutus äänenlaatuun riippuu siitä, kuinka paljon itse äänipaketti sisälsi äänitietoa. Tähän vaikuttaa mm. käytetty koodekki ja erityisesti sen käyttämä näytteen koko. Näytteen koko ilmoitetaan millisekunteina, ja se sisältää ilmoittamansa määrän ääntä. Esim. 10 ms ääninäyte tarkoittaa 10 ms puhetta IP-puheliikenteessä.

Pakettien katoaminen on ominaista pakettikytkentäisille verkoille. Syyt voivat olla hyvinkin moninaiset. Riittämätön kaistanleveys on yleisimpiä tekijöitä, joista aiheutuu ruuhkatilanteita, joissa verkkolaitteet joutuvat pudottamaan osan liikenteestä pois. Virheitä pakettien sisältöön aiheuttavat erityisesti langattomat verkkotekniikat, mutta niitä esiintyy myös kupari ja kuituverkoissa. (Ellis ym. 2003: 156.)

4.3.4 Kaiku

Kaiulla (echo) tarkoitetaan ilmiötä, jossa ihminen kuulee puhelun aikana oman puheensa uudestaan hieman sen jälkeen kun on puhunut. Kaiku voi muodostua verkossa olevien eri siirtomedioiden risteyksissä, kuten lähiverkosta PSTN:n siirtyessä tai neljästä johdosta siirryttäessä kaksijohtoiseen mediaan. Pienessä määrin kaiku ei haittaa puhujaa, mutta kaiun viiveen ja voimakkuuden kasvaessa myös sen häiritsevyys kasvaa. Ilmiötä pyritään pienentämään verkon varrella olevilla kaiunkumoajilla. Niiden tehtävä on verrata niiden läpi kulkevia ääninäytteitä ja kumota saman kuvioinen vastakkaiseen suuntaan liikkuva liikenne. (Ellis ym. 2003: 85-86.)

4.3.5 Puheen taukojen poisto

Kun ihminen puhuu toiselle ihmiselle, on hyvin normaalia, että vain toinen osapuoli puhuu kerrallaan. Tästä voidaan päätellä, että silloin yli puolet puheliikenteestä ja puhenäytteiden otosta ei ole relevanttia keskustelun kannalta. Tämän liikenteen poistaminen vähentää huomattavasti kaistankäyttöä.

Tätä varten tarvitaan äänentunnistus mekanismi eli VAD (voice activity detection). Jos VAD aktivoituu liian aikaisin tai liian myöhään, voi osa puheen alusta tai lopusta leikkautua pois. Tästä syystä VAD:n toimintaa ei saa asettaa toimimaan liian aggressiivisesti. VAD:n erotellessa, mikä on puhetta ja mikä ei, pitää puheettomat aukot paikata jollakin. Ilman tyhjien aukkojen paikkaamista yhteys tuntuu katkeavan täydellisen mykistymisen myötä. Tätä aukkojen täyttämiseen käytettävää ääntä kutsutaan comfort noise -ääneksi. Sen avulla kuulija ei erehdy luulemaan, että linja olisi katkennut. (Swale 2001: 34.)

4.4 Äänenlaadun optimointi

Ellis, Pursell ja Rahman (2003: 248-250) listaavat äänenlaatuun vaikuttavia tekijöitä, joita verkonsuunnittelijan tulee ottaa huomioon, jotta äänenlaatu saadaan optimoitua parhaalle mahdolliselle tasolle. Seuraavassa luettelossa kuvaan ja esittelen niitä tärkeimmiltä osiltaan.

- *G.711 koodekin käyttö*
  Oikean koodekin valinta vaikuttaa ratkaisevasti äänenlaatuun ruuhkaisessa verkossa. Käyttämällä G.711 koodekkia ääntä ei pakata lainkaan ja äänenlaatu pysyy alkuperäisenä. Samainen koodekki sietää myös eniten kadonneita paketteja. Mikäli kaistaa on niukasti käytettävissä, voidaan käyttää jotakin ääntä pakkaavaa koodekkia kuten G.729 tai G.723.

- *Pieni ääninäytteiden pituus ja määrä per paketti*
  Jos paketti katoaa, riippuu sen aiheuttama haitta paketin sisältämän äänitiedon määrästä. Sopiva määrä ääntä yhdessä paketissa on 20 ms. Pienet paketit kuitenkin lisäävät kaistankulutusta, koska jokaisen erillisen paketin otsikkokentät lisäävät kokonaiskaistan kulutusta.
- *Monen perättäisen paketin katoaminen*
  Peräkkäisten pakettien katoaminen aiheuttaa suurimmat äänikatkokset puheluissa. Niiden välttäminen on erittäin tärkeää.
- *Paketin katoamisen salaaminen*
  Satunnaisen paketin katoaminen voidaan peittää tähän tarkoitukseen kehitetyllä tekniikalla. Tällöin edellisen hyvän paketin tietojen avulla verhotaan seuraavan paketin puuttumista.
- *Yhdensuuntainen viive alle 150 ms*
  Kaikki viiveen muodostumistavat huomioiden kokonaisviiveen täytyy pysytellä alle 150 ms per yksi liikennesuunta.
- *Hitaiden yhteyksien välttäminen*
  Hitaat sarjayhteydet ovat suurimpia ongelmia VoIP-liikenteelle. Niiden kaistanleveyttä tulee lisätä, jotta VoIP- ja dataliikenne voisivat yhdessä käyttää yhteyttä. Niitä varten on olemassa omia QoS-työkaluja.
- *Pakettien otsikkotietojen pakkaaminen hitaissa yhteyksissä*
  Jos viivettä ei esiinny liikaa verkossa, voidaan kaistanleveyttä vapauttaa pakkaamalla RTP-otsikkokenttiä. CRTP:n avulla voidaan otsikoiden viemä kaista pienentää kymmenesosaan alkuperäisestä. CRTP tulee kuitenkin käyttää vain alle 500 kbps yhteyksissä.
- *Suurten pakettien paloittelu ja väliin kiilaamisen salliminen hitaissa yhteyksissä*
  Suuret paketit tukkivat hitaita yhteyksiä, koska niiden asettaminen linkkiin vie kohtuuttoman kauan. Tämän takia ne tulee pilkkoa ja mahdollistaa pienempien pakettien lähettäminen näiden palasten väliin.
- *Suurin sallittu yhtäaikaisten puheluiden olemassaolo*
  On hyvin tärkeää tietää, montako yhtäaikaista puhelua verkko pystyy käsittelemään. Tämän rajan ylityttyä uusien puhelujen muodostaminen tulisi estää.
- *Prioriteettiaikataulutuksen käyttäminen ääniliikenteelle*
  QoS-toimet tulee asettaa eriyttämään liikennettä toisistaan ja priorisoimaan VoIP-liikennettä muun liikenteen edelle.
- *Verkon päivitys VoIP:in vaatimusten tasolle*
  VoIP-vaatimusten edellyttämien toimien testaaminen on järkevää, ennen kuin varsinaisesti VoIP-liikenne tuodaan osaksi tietoverkkoa. Tätä työtä helpottavat erilaiset mittaus ja analysointi työkalut, joilla voidaan simuloida VoIP-liikennettä. Myöhempää VoIP-palvelun implementointia helpottavat ennakoivat testaukset ja asetusten optimoinnit.

Edellisten lisäksi on huomioitava äänettömyyden poistamiseen käytetyn VAD (voice activity detection) -toiminta.

5 QoS

QoS:lla tarkoitetaan verkkopalvelun kokemaa palvelun laatua. Tietyn palvelun tarvitsema palvelun laatu riippuu aina itse palvelusta ja varsinkin siitä, minkälaisia vaatimuksia loppukäyttäjä sille asettaa. Jos kyseessä on esimerkiksi tiedostonsiirto, loppukäyttäjälle olennaisinta on tiedoston siirron nopeus ja tiedoston eheys.

Loppukäyttäjän näkökulmasta äänipuhelun palvelun laatu on vanhan kokemuksen mukaisen äänenlaadun vertaamista vallitsevaan äänenlaatuun. Loppukäyttäjä ei ole kiinnostunut puhelun siirron vaiheista eikä mistään muustakaan asiasta, joka ei suoranaisesti ilmene loppukäyttäjälle. (Szigeti & Hattingh 2005: 9.)

Jotta palvelun laatuun pystytään vaikuttamaan, täytyy eri liikennetyypit eriyttää toisistaan. Perinteisen liikennevirtoihin perustuvan liikenteen erittelyn lisäksi on mahdollista eriyttää liikennettä mm. ToS (Type of Service)- ja CoS (Class of Service) -luokittelua käyttämällä. Palvelun laadun varmistus on aina ajateltava koko verkon alue huomioiden.

QoS-toimia on olemassa kaistantehokkaaseen käyttöön, ruuhkien ennaltaehkäisemiseen ja ruuhkatilanteiden hallintaan. Niistä tässä opinnäytetyössä käsittelyyn on otettu niitä ominaisuuksia, joita on mahdollista toteuttaa Ciscon laitteilla.

5.1 End-to-end QoS

Palvelun laatu täytyy varmistaa tietoverkossa pakettien muodostumispisteestä aina sinne kohteeseen minne paketti on menossa. Jos matkalla on yksikin verkkolaite, joka ei huomioi palvelunlaatua, voi se tehdä hyödyttömäksi palvelun laadun varmistamisen myös kaikkien muiden laitteiden osalta. Palvelunlaadulla halutaan nimenomaan varmistaa se, että keskenään epätasa-arvoinen liikenne käsitellään myös verkkolaitteissa eriarvoisesti. Arvokkaaksi liikenteeksi luokitellaan usein sellainen liikenne, joka kärsii hidasteluista ja pakettien putoamisista suhteellisesti eniten. Arvotontakin liikennettä on mahdollista eriyttää muusta verkkoliikenteestä, ja antaa sille erityinen heikon palvelun leima (Scavenger class). (Szigeti & Hattingh 2005: 10-12.)

Jotta saavutetaan end-to-end-palvelunlaatu, täytyy liikenne olla eroteltavissa koko verkon matkalta. Paketti voi kulkea puhtaasti OSI:n 2-kerroksella LAN (Local Area Network) -ympäristössä ja käyttää 802.1p/Q-merkintöjä. Siirryttäessä reititettyyn ympäristöön paketissa täytyy olla 3-kerroksen merkintä. Se voidaan toteuttaa mm. IP-Precedence- tai DSCP (Differentiated Services Code Point) -merkinnän avulla. Edelleen paketin kulkiessa palveluntarjoajan verkkoon saattaa se kulkea jo jonkin muun tekniikan turvin kuten ATM:n (Asynchronous Transfer

Mode) päällä. Tästä päästäänkin siihen, että merkitsemällä paketit IP-kentän luokittelubittien avulla tai käyttämällä sopivia muuntotaulukoita 2-kerroksen ja 3-kerroksen välissä voidaan saavuttaa end-to-end-palvelunlaatua. (Vegesna 2001: 15.)

5.2 Kaistan tehokas käyttö

Ongelmia kaistankäytössä aiheutuu, jos se on riittämätön kuljettamaan tarvittavaa määrää liikennettä. Käytettävissä oleva kaista on usein ennalta määrätty, ja sen optimaalinen käyttöaste yhdessä onnistuneen end-to-end suunnittelun kanssa mahdollistavat tehokkaimman kaistankäytön. Kaistan kulutusta voidaan pienentää eri verkkokerroksien lisäämien otsikkotietojen tiivistämisellä sekä liikenteen uudelleen järjestelyllä.

5.2.1 Tiedon tiivistys

Sovelluskerroksella äänidatan tiivistystä voidaan tehdä koodekin avulla, mutta verkkolaitteillakin voidaan toteuttaa kehysotsikoiden pakkaamista. Pakkaamiseen voidaan käyttää mm. cTCP (compressed TCP)- ja cRTP (compressed RTP) -pakkausmekanismeja.

CTCP on pakkausmekanismi, jolla TCP/IP-otsikoiden kokoa voidaan pienentää. Huomioitavaa on kuitenkin, että TCP-otsikot tulee pakata, jos käytössä on cRTP-otsikoiden pakkaus. CRTP on puolestaan pakkausmekanismi, jonka avulla RTP-paketin otsikkokentät pakataan pienempään tilaan. Pakkauksen hyödyt nousevat esille vasta hitaissa yhteyksissä, koska niissä otsikkokenttien prosentuaalinen osuus suhteessa hyötykuormaan nousee merkitsevän suureksi. Pakkaus aiheuttaa otsikkokenttien muutoksia, joten pakettien reitittämistä varten pitää pakkaus purkaa. Tämä myös asettaa vaatimuksen, että linkit ovat point-to-point-yhteyksiä eivätkä esim. ethernet-verkkoja. On huomioitava, että jatkuva pakkaaminen ja purkaminen kuormittavat prosessoria, joten laitteella on oltava tarpeelliset resurssit lisäkuorman käsittelemiseksi. (Szigeti & Hattingh 2005: 171-172.)

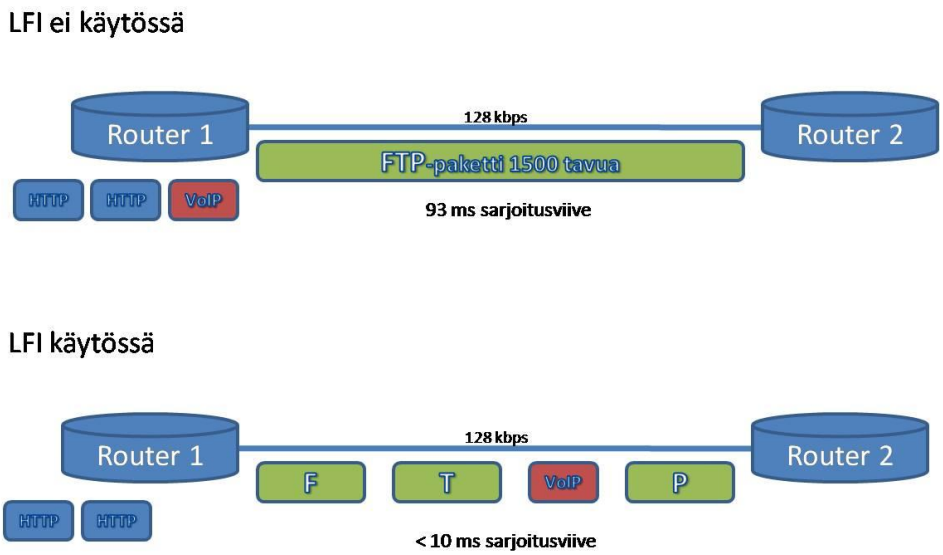
5.2.2 Liikenteen uudelleen järjestely

LFI (Link Fragmentation and Interleaving) on tekniikka, joka nimensä mukaisesti paloittelee liikennettä ja järjestää nämä palaset uudelleen. Sen käyttökohde on nimenomaan hitaissa sarjayhteyksissä.

Hitaissa yhteyksissä suuret paketit voivat lisätä sarjoitusviivettä sillä, että niiden kokonaan vieminen rajapintaan vaatii hyvin pitkän ajan. Samaan aikaan muut paketit odottavat omaa vuoroaan jonossa. Äänipaketeille tämä ei kuitenkaan sovi lainkaan ja tähän voidaankin käyttää kahta eri ta-

paa paloitella ja uudelleenjärjestellä paketteja hitaan yhteyden ylitse. PPP-yhteyksissä voidaan käyttää MLP-LFI (Multilink PPP Link-Fragmentation and Interleaving) -ominaisuutta ja Frame Relay -yhteydessä FRF.12:ta (Frame Relay Fragmentation and Interleaving). (Szigeti & Hattingh 2005: 181-182.)

Alun perin multilink PPP suunniteltiin yhdistämään monta loogista tai fyysistä linkkiä yhdeksi virtuaaliseksi linkiksi. Suuren paketin paloittelun keskeyttäminen ja väliin kiireellisten pakettien lähettäminen on ominaisuus, joka hyödyttää ääniliikenteen kulkua. (Hersent & Petit & Gurle 2005: 177.) Kuva 7 osoittaa kuinka ääniliikenteelle haitallista viivettä saadaan pienennettyä LFI-tekniikan käyttöönotolla.



Kuva 7: LFI:n toiminta

On hyvä huomata, että paloittelu tapahtuu reitittimessä OSI:n 2-kerroksella vasta mahdollisten jonotuskäsittelyiden jälkeen. LLQ- ja PQ-jonoja käytettäessä niihin sijoitettua liikennettä ei paloitella. Tämän takia reaaliaikaisen ääni- ja videoliikenteen lähettäminen prioriteettijonon kautta hitaan linkin lävitse ei ole suositeltavaa. Näiden jonojen merkitys selvitetään luvussa 5.7, joka käsittelee ruuhkan hallintaa. Yleisen ohjeen mukaisesti yhden hypyn sarjoitusviive ei saa ylittää 10 ms. Tästä seuraa, että vain alle 768 kbps kykeneviin linkkeihin on tarpeellista asettaa LFI aktiiviseksi. Seuraavassa on esitetty kaava, jolla voidaan sopiva paloitteluväli määritellä. (Szigeti & Hattingh 2005: 181-182.)

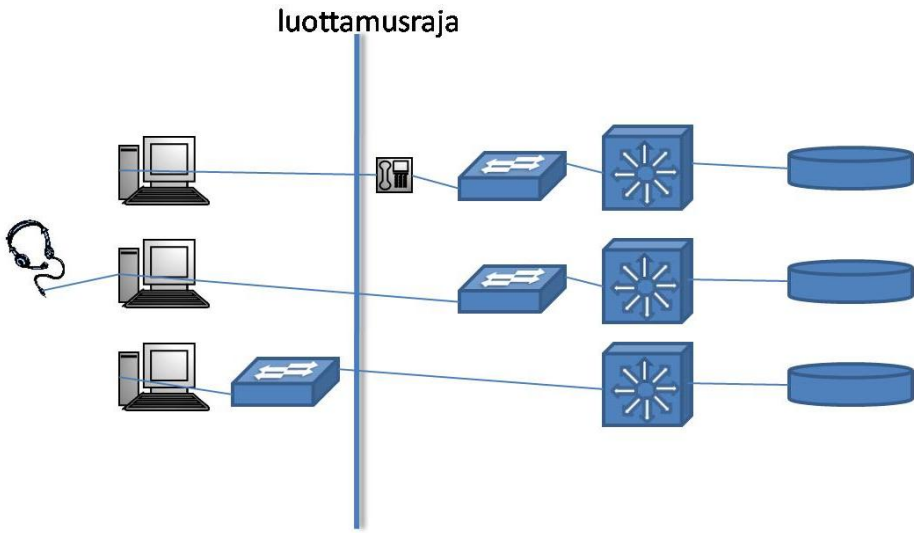
fragment = (suurin sallittu värinä[jitter] millisekuntteina [norm. 10 ms]) * (linkin nopeus) / 8

5.3 Liikenteen luokittelu

Liikennettä voidaan luokitella OSI:n 2- tai 3-kerroksella. Ciscon laitteilla luokittelua voidaan toteuttaa IEEE (Institute of Electrical and Electronics Engineers) 802.1p/Q mukaisesti ethernet-kehykseen OSI:n 2-kerroksella tai 3-kerroksella IP-paketin ToS-tavuun. IP-paketin ToS-tavu mahdollistaa liikenteen luokittelun IP Precedence-, IntServ (Integrated Services)- tai DSCP-arvojen avulla. IntServ ja IP Precedence ovat väistymässä pois DiffServ-arkkitehtuurin alta, joka käyttää luokitteluun DSCP-merkintöjä, mutta niiden yhdistäminen DiffServ-arkkitehtuurin kanssa on myös mahdollista.

5.3.1 Luottamusraja

Luottamusrajalla (trust boundaries) tarkoitetaan kuvitteellista pistettä, jonka jälkeen liikenteessä esiintyvä luokittelu on hyväksyttävää. Luottamusrajan avulla voidaan hahmottaa verkon reuna-alueet, missä luokitteluun kykenevät laitteet luokittelevat liikenteen asianmukaisesti. Kuva 8 havainnollistaa luottamusrajaa. Liikenteen kulkiessa luottamusrajan ylitse, ensimmäinen liikenteen vastaanottava laite kykenee luokittelemaan liikenteen. Suositeltavaa on, että luottamusraja on mahdollisimman lähellä liikenteen muodostumispistettä.



Kuva 8: Luottamusraja

5.3.2 DiffServ

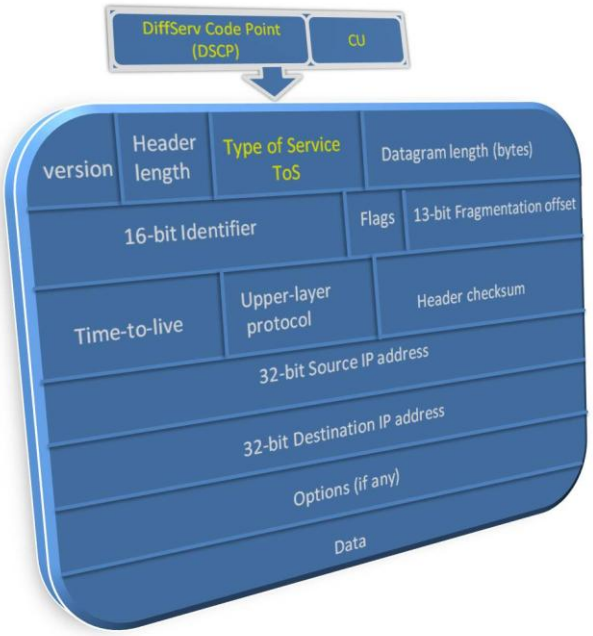
DiffServ-arkkitehtuuri antaa viitekehyksen palvelun laadun varmistamiselle. Sen avulla liikennettä luokitellaan ja saadaan eri liikennetyypit eroteltua toisistaan. Luokittelu pyritään tekemään verkon reunoilla, jolloin pakettien käsittely on sisäverkon laitteilla kevyempää. RFC 2475:n (RFC 2475… 1998) mukaan DiffServ pyrkii olemaan skaalautuva tekniikka ilman, että se on riippuvainen liikennevirtojen tiloista tai niiden signaloinnista jokaisen verkkoyhteyden kohdalla.

Luokittelun jälkeen liikennettä voidaan ohjailla PHB (per-hop behavior) -menettelyn avulla. PHB on toimintamalli, joka määritellään jokaiselle palveluluokalle erikseen. Tämän jälkeen se on toteutettava jokaiselle samassa DiffServ-toimialueessa toimivalle verkkolaitteelle. DiffServ-toimialueeksi kutsutaan loogisesti yhtenäistä IP-aluetta, jossa jokaisella verkon reitittävällä laitteella on oma PHB:nsa (Vegesna 2001: 22). Voidaankin sanoa, että DiffServ tarjoaa liikenteelle luokittelun ja PHB määrittelee tämän jälkeen, kuinka eri luokkien liikennettä ohjataan ja käsitellään yksittäisessä verkkolaitteessa.

PHB-käsittelytapoja on määritelty RFC-dokumenteissa, mutta on kuitenkin huomioitava, että niiden varsinainen toteutus on jätetty avoimeksi. Yleisesti käytössä olevia PHB-käsittelytapoja ovat EF (Expedited Forwarding) RFC 3246 määrittelemänä, AF (Assured Forwarding) RFC 2597 määrittelemänä ja luokallisiin Class Selector -luokkiin pohjautuva määrittely RFC 2474:ssä. (Szigeti & Hattingh 2005: 16-17.) EF:llä tarkoitetaan niitä toimia, joilla voidaan minimoida viivettä, värinää ja pakettien katoamista sekä pyritään antamaan yhtä nopeaa palvelua, kuin lähetysnopeus vain sallii. AF määrittelee neljä eri palveluluokkaa, joiden sisällä tapahtuu lisäksi kolmen tasoista liikenteen arvostusta. (Vegesna 2001: 27-28.) On olemassa myös BE (Best Effort) liikennettä, joka takaa nimensä mukaisesti vain parhaan mahdollisen liikenteen käsittelyn ilman mitään jaottelua liikenteen tärkeyden perusteella. On myös hyvin yleistä käyttää Class Selector -luokkia, koska ne ovat yhteensopivia IP Precedence -arvojen kanssa.

DiffServ mahdollistaa liikenteen luokittelun IP-kehyksessä sijaitsevan ToS-tavun avulla. ToS-kentässä sijaitseva DSCP-arvo määrittelee paketille palveluluokan. Tätä hyväksikäyttämällä liikennettä voidaan ohjailla paketti paketilta. (Vegesna 2001: 22.) IPv6:lla on oma Traffic Class -otsikkokenttä liikenteenluokittelulle varattuna.

Kuvan 9 avulla voidaan nähdä, missä kohtaa IP-paketissa sijaitsee DSCP-kenttä, ja kuva 10 selittää eri kenttien tarkoituksen. DSCP on kuuden bitin mittainen kenttä IP-paketin ToS-tavussa. Sen avulla voidaan määritellä 64 eri palveluluokkaa. ToS-tavussa on DSCP-bittien lisäksi kaksi bittiä, jotka on varattu tulevaisuuden tarpeisiin, eli ovat käyttämättömiä kirjoitushetkellä. (Vegesna 2001: 25.)



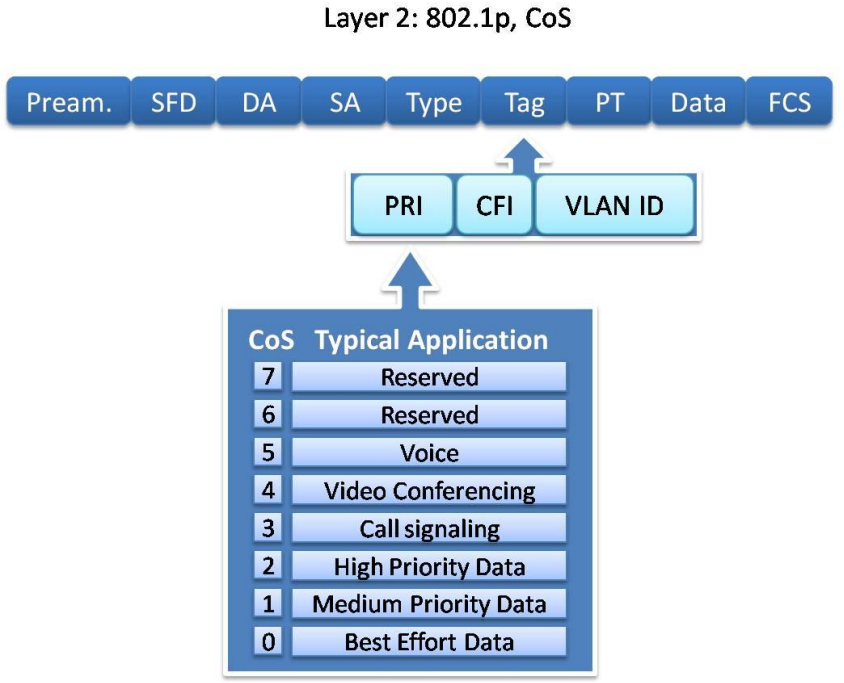
Kuva 9: DSCP-kentän sijainti IP-paketissa

Kuva 10: IP-paketin sisältämien kenttien selitykset

5.3.3 IEEE 802.1 p/Q

Liikennettä voidaan luokitella kahdeksaan eri luokkaan OSI:n 2-kerroksella. Tähän soveltuu IEEE:n määrittelemä 802.1Q-standardi, joka määrittelee VLAN (virtual LAN) -merkintätavan. Se muodostuu kahdesta tavusta ja käyttää itse niistä 12 bittiä. Jäljelle jääneistä biteistä IEEE 802.1p -standardi käyttää kolme bittiä merkitäkseen paketit. Kuva 11 osoittaa luokittelubittien sijainnin ja niiden mahdollistamat luokat. Tarkkaan ottaen luokittelubitit sijaitsevat ethernet-kehyksen Tag-kentän (lippu-kenttä) PRI-osassa (priority). Tag-kentässä sijaitsee myös CFI (Canonical Format Indicator) -kenttä, jota käytetään tunnistamaan Token Ring -kehykset ja VLAN ID -kenttä, joka määrittelee mihin VLAN:iin kehys kuuluu. (Ellis ym. 2003: 91.) Käytän läpi työn 2-kerroksen kehykseen tehtävästä merkintätavasta selkeyden vuoksi ainoastaan nimitystä CoS.

Jos halutaan tehdä luokittelua 802.1p mukaisesti 2-kerroksella, on silloin pakko käyttää verkossa VLAN:eja. VLAN-merkintä täytyy myös olla aina paketissa olemassa tai muuten luokittelumerkintää ei voida tehdä. Niin kutsuttu natiivinen VLAN ei voi olla käytössä, koska sen kehyksessä ei ole VLAN-kenttää, eikä tällöin ole myöskään mahdollista tehdä luokittelumerkintää.



Kuva 11: CoS-luokittelubitit

5.4 Ruuhkautumisen esto

Ruuhkautumisen estotoimilla yritetään estää tilanteita, joissa laitteiden jonot täyttyvät ja kaikki jonoihin pyrkivä liikenne joudutaan hylkäämään. Jonojen täyttyminen ja tästä johtuva pakettien hallitsematon pudottaminen johtaa väistämättä myös tärkeiden pakettien hylkäämiseen. Ääniliikenne on kuitenkin hyvin herkkä pakettien putoamiselle, ja sitä tulee välttää, koska äänenlaatu kärsii tästä huomattavan paljon. Verkon ruuhkautuessa täytyy paketteja hylätä, koska ne eivät yksinkertaisesti mahdu kaikki siirtymään siellä. Niiden pudottaminen tulee kuitenkin olla hallittua ja kohdistua liikenteeseen, joka kärsii tästä kaikista vähiten. Jos pakettien pudottamiset kohdistuvat TCP-liikenteeseen, pystyy se mukautumaan tilanteeseen ja pudottamaan liikennöintinopeuttaan.

5.4.1 Tail Drop

Tail Drop on hyvin yksinkertainen toimintatavaltaan. Se yksinkertaisesti pudottaa käsittelyssä olevan paketin, jos se ei mahdu jonoon, johon sitä ollaan asettamassa.

5.4.2 WTD

WTD (Weighted Tail Drop) on kehittyneempi versio perinteisestä Tail Drop -algoritmista. Sen hyödyntäminen vaatii liikenteen luokittelua. WTD toimii yksittäisessä jonossa niin, että se ryhtyy pudottamaan liikennettä jo ennen jonon täyttymistä. Pakettien satunnainen pudottaminen aloitetaan pienemmän luokitteluarvon omaavasta liikenteestä. Jos tämä ei riitä, edetään pudottamaan aina seuraavan luokan liikennettä. Lopulta, jos pudottamisesta ei ollut tarpeeksi apua, jono täyttyy ja kaikki liikenne joudutaan pudottamaan. WTD vaatii toimiakseen raja-arvoja, joiden perusteella se määrittelee, koska liikenteen pudottaminen aloitetaan. (Cisco Systems – Catalyst 3560… 2005.)

5.4.3 RED & WRED

RED:in (Random Early Detect) toiminta perustuu TCP:n ominaisuuteen säädellä lähetysnopeuttaan. TCP nopeuttaa ja hidastaa lähetystään pakettien putoamistiheyden perusteella. RED:in ideana on pudottaa paketteja TCP-lähetyksistä jonojen koon mukaisesti jo ennen kuin itse jono saavuttaa täyttymyspisteensä. Normaalissa TCP-liikenteessä paketteja putoaa vasta, kun jonot ovat täynnä ja Tail Drop aktivoituu. RED pudottaa ennakoivasti paketteja jo silloin, kun jonot alkavat täyttyä. Näin ollen TCP alkaa reagoida jonojen täyttymiseen tarpeeksi ajoissa, eivätkä jonot pääse täyttymään kokonaan niin nopeasti.

RED:ille annetaan kaksi arvoa, joiden perusteella se pudottaa paketteja. Minimum ja maximum raja-arvot määrittelevät sen pisteen, jonka jälkeen RED alkaa enenevässä määrin pudottaa paketteja TCP-liikenteestä, sekä sen pisteen, jonka jälkeen kaikki paketit pudotetaan ko. liikenteestä. (Vegesna 2001: 130-131.)

WRED on Ciscon kehittelemä versio RED:stä. Se lisää vaikutusmahdollisuuksia RED:n sattumanvaraiseen pakettien pudottamiseen. WRED käyttää IP-Precedence arvoja painottamaan heikomman arvon omaavan liikenteen pudotustodennäköisyyttä. On huomattava, että Ciscon laitteissa on pakko käyttää WRED:iä, koska niihin ei ole implementoitu RED:iä lainkaan. WRED:iä on myös edelleen kehitetty hyödyntämään DSCP-merkintöjä. Kehitettyä versiota kutsutaan DSCP-Based WRED:ksi. (Szigeti & Hattingh 2005: 161-162.)

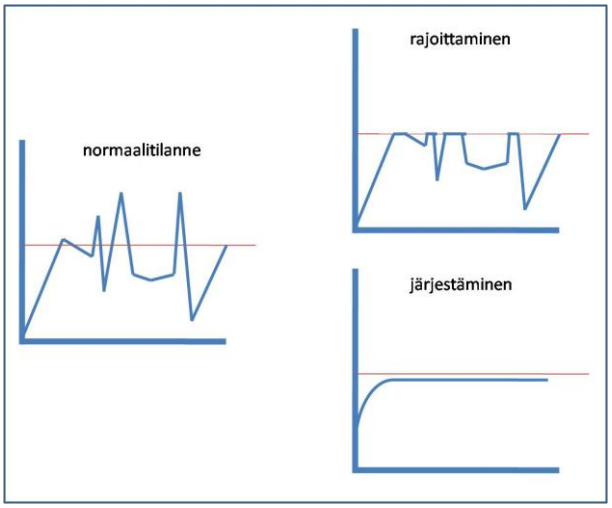
RED ja WRED ovat molemmat ruuhkanestomenetelmiä, jotka pohjautuvat TCP-protokollan toimintaan. Ääniliikenne on kuitenkin monesti sidottu UDP-protokollaan, eikä se osaa mukauttaa liikennettä, niin kuin TCP-protokolla pystyy. Tästä johtuen RED ja WRED ovat käyttökelvottomia muussa kuin TCP-liikenteen käsittelyssä.

5.4.4 WRED ECN

ECN (Explicit Congestion Notification) on IP-paketissa esiintyvän käyttämättömän kentän hyödyntämistä tavalla, jossa lähettävä ja vastaanottava osapuoli pystyy informoimaan toisilleen verkossa esiintyvästä ruuhkasta. WRED ECN toimii niin, että verkon ruuhkautuessa IP-paketit merkitään ECN-merkinnällä, ja näin lähettävä osapuoli voi pudottaa lähetysnopeuttaan huomatessaan merkinnän. Tämän toiminnon avulla voidaan pudotettavien pakettien määrää vähentää. (Szigeti & Hattingh 2005: 163-164.) Kuvassa 9 olevan CU (currently unused) -kentän bittejä käytetään ECN-merkinnän tekemiseen.

5.5 Liikenteen säännöstely ja rajoittaminen

Vaikka liikennettä voidaan hallita ruuhkatilanteissa ruuhkankäsittelytoimenpiteillä, voidaan sen käyttämää kaistanleveyttä säännöstellä ja rajoittaa liikennepolitiikan avulla. Näitä toimia voidaan toteuttaa nopeuden rajoitus- ja järjestelytyökaluilla. Ne voidaan aktivoida toimimaan yksinään tai yhdessä. *Rajoitustyökalujen* toiminta perustuu liikenteen pudottamiseen. Ne ovat monesti palveluntarjoajien käytössä, koska niillä voidaan varmistaa, että tilaaja käyttää vain sopimuksen mukaista kaistanleveyttä. *Järjestystyökalut* puolestaan turvautuvat liikenteen puskurointiin, ja niiden käyttö keskittyy yleensä asiakkaiden omiin verkkoihin. Kuvasta 12 nähdään näiden kahden työkalun vaikutus liikennevirtaan. (Davidson & Peters 2002: 208-209.)



Kuva 12: Liikennepolitiikan vaikutus liikennevirtaan

5.6 Kaistan varaaminen

Kaistan varaaminen eroaa DiffServ-arkkitehtuuriin pohjautuvasta palvelun laadun varmistamisesta, koska se varaa tietylle palvelulle tai virralle omaa varattua kaistaa. Tätä varten on olemassa oma protokolla *RSVP (Resource Reservation Protocol)*.

Normaalit QoS-toimenpiteet perustuvat ennalta määriteltyihin QoS-asetuksiin ja liikenteen erotteluun. Näiden tietojen avulla jokainen verkkolaite takaa jokaiselle erotellulle liikenteelle niiden tarvitseman palvelun laadun. RSVP on protokolla, joka varaa yhteyskohtaisesti, ennen yhteyden muodostamista, kunkin palvelun tarvitseman palvelun laadun tason jokaiselta lähettäjän ja vastaanottajan välissä olevalta kytkimeltä ja reitittimeltä.

RSVP toimii IP-paketin päällä. Se käyttää UDP-kapselointia ja toimii portissa 46. Yhteyden muodostus aloitetaan lähettämällä RSVP-viesti lähettäjältä vastaanottajalle. Tässä viestissä ilmoitetaan, että lähettäjä on halukas lähettämään tietoa vastaanottajalle. Vastaanottaja tekee tämän jälkeen palvelutasopyynnön lähetyksen tarvitsemasta palvelun laadusta, ja lähettää pyynnön jokaiselle lähetyksen matkan varrella olevalle laitteelle. Koska palvelutason varaus tapahtuu vastaanottajan toimesta, mahdollistaa tämä multicast-ominaisuuksien hyödyntämisen. (Ellis ym. 2003: 261-263.)

RSVP:llä on omat heikkoutensa. Ensinnäkin, koska se joutuu hoitamaan jokaisen yhteyden varauspyynnöt, lisää se huomattavasti runkoreitittimien kuormaa. Kaistanvaraustoimet puolestaan lisäävät yhteydenaloitukseen kuluvaa aikaa. Itse RSVP:n skaalautuvuudessa on olemassa monenlaisia rajoittuvuuksia, jotka estävät protokollan tehokasta käyttöä. (Davidson & Peters 2002: 206-207.)

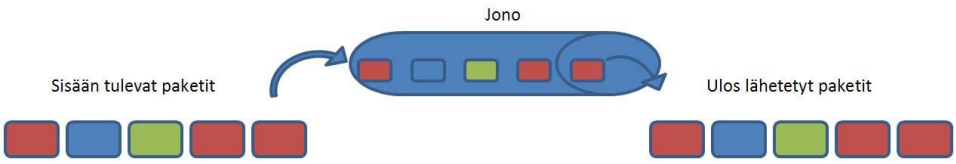
5.7 Ruuhkan hallinta

Kun liikenne ruuhkautuu verkossa, joutuvat siinä liikennöivät paketit johonkin siellä esiintyvistä jonoista, tai ne pudotetaan kokonaan pois liikenteestä. Paketti voi olla jonossa verkkolaitteen sisääntuloportissa tai uloslähtevän liikenteen portissa. Verkkolaitteen ollessa ylikuormitettuna sen sisääntuloporttien jonot alkavat täyttyä paketeista. Tämä johtuu siitä, että sisääntuloliitännät eivät voi asettaa paketteja laitteen käsiteltäväksi sitä mukaa, kun niitä saapuu laitteelle. Ulostuloliitännän jonot muodostuvat puolestaan siitä, että liitäntä ei voi lähettää prosessoituja paketteja ulos liitännästä, koska liitännän takana olevan median siirtokyky ei siihen riitä.

Mahdollisuuksia hallita ruuhkatilanteita on monia. Näistä osaa pystytään käyttämään Cisco Systemsin kytkimillä ja osaa reitittimillä. Ilman mitään QoS-asetuksia kytkimet palvelevat liikennettä tasapuolisesti parhaalla mahdollisella tavalla. Tällöin mitään liikennettä ei erotella toisistaan ja kaikkea liikennettä palvellaan samanarvoisesti. Kytkinten QoS-ominaisuuksien jäädessä yhden tai kahden algoritmin varaan, esiintyy reitittimissä huomattava määrä eri konfigurointimahdollisuuksia.

5.7.1 FIFO

FIFO (First-In First-Out) on yksinkertainen ruuhkanhallintamenetelmä. Se asettaa sisääntulevan liikenteen yhteen jonoon ja purkaa jonoa toisesta päästä. Kuvasta 13 nähdään kuinka jonoa puretaan siinä järjestyksessä, kun siihen on paketit asetettu. Ruuhkatilanteessa jono kasvaa ja lopulta täyttyy. Tämän jälkeen kaikki jonoon mahtumattomat paketit pudotetaan automaattisesti pois.



Kuva 13: FiFo

Menetelmä on hyvin helppo toteuttaa ja on laajasti käytössä sen yksinkertaisuuden takia. Sen toimintatapa ei kuitenkaan ole millään tavalla oikeudenmukainen, koska se ei erottele eri liikennevirtoja toisistaan. Tällöin suurella lähetysnopeudella tai suuria paketteja käyttävä liikenne saa vallattua enemmän kaistaa. Varsinkin, jos kaistaa käyttää TCP:n tavoin kaistansiirtokykyyn mukautuva protokolla, jää se muun liikenteen varjoon. (Vegesna 2001: 69.)

FIFO ei sovellu ääniliikenteen ruuhkanhallintatilanteisiin, koska se ei erottele sitä mitenkään muusta liikenteestä, eikä näin ollen voi luokitella sitä muun liikenteen edelle. FIFO:n yksittäinen ja välillä pitkäksi muodostuva jono lisää myös äänipaketin läpikulkuaikaa, jolloin äänenlaatu alkaa heikkenemään viiveen lisääntyessä.

5.7.2 Round-robin

Round-robin on algoritmi, joka purkaa verkkolaitteiden jonoja. Sen toiminnan kannalta on olennaista, että käytössä on useampi kuin yksi jono. Toimintaperiaatteena sillä on purkaa jonoja vuoron perään kustakin jonosta samanarvoisesti. Jos käytössä on yksi jono, on sen toiminta identtinen FiFo-menettelyn kanssa.

5.7.3 WRR

WRR (Weighted round-robin) on algoritmi, joka purkaa verkkolaitteen jonoja. Perinteinen round-robin algoritmi purkaa jokaista jonoa vuoronperään siirtyen aina jonosta toiseen. Viimeisen jonon jälkeen se aloittaa jälleen jonojen purkamisen alusta. WRR on kehittyneempi versio perinteisestä round-robin jonon purkutavasta. Se lisää mahdollisuuden antaa eri painoarvo jokaiselle jonolle. Näin ollen voidaan joitakin jonoja purkaa hieman nopeammin kuin toisia ja saada tärkeää liikennettä sisältävät jonot purettua nopeammin kuin vähemmän tärkeätä liikennettä sisältävät jonot. (Cisco Systems – Catalyst 3550… 2003.)

5.7.4 SRR

SRR (Shaped/Shared round-robin) on jonojen purkamiseen käytetty algoritmi. Sen toiminta perustuu usean jonon käyttöön ja niiden purkamiseen ennalta asetettujen painoarvojen mukaisesti. SRR on kehittynyt versio perinteisestä round-robin-menetelmästä.

SRR voidaan asettaa toimimaan kahdessa eri tilassa Catalyst 2960/3560-kytkimillä. Nämä tilat ovat share ja shape. *Shape*-tilassa jokaiselle jonolle annetaan prosentuaalinen osuus taattua kaistaa, joka rajaa ne tähän lukemaan. Kaistan käyttö ei voi koskaan nousta asetetun arvon yläpuolelle, vaikka linkki olisi muilta osin käyttämätön. Tämän avulla voidaan tasata purskeista liikennettä ja tasoittaa liikenteen kulkua pitemmällä aikavälillä. *Shared*-tilassa kaista jaetaan jonojen kesken määriteltyjen arvojen perusteella. Kaista on taattua arvojen mukaisesti, mutta se ei estä käyttämästä kaistaa enemmän, jos jonkin muun luokan kaistavaraus jää käyttämättömäksi. (Cisco Systems – Catalyst 3560… 2005.)

5.7.5 WFQ

WFQ (Weighted Fair Queue) jaottelee liikennettä liikennevirtojen perusteella ja asettaa jokaisen niistä eri jonoon. Jokaiselle jonolle se jakaa yhtä suuren määrän kaistaa käytettäväksi. Näin ollen pienet datavirrat saavat suhteellisesti enemmän kaistaa käyttöönsä kuin suuremmat datamäärät. Suuret datamäärät joutuvat mukautumaan pienempään kaistaansa, eivätkä ne kuluta kaikkea käytettävissä olevaa kaistaa omaan käyttöönsä. WFQ toimii dynaamisesti niin, että datavirtojen lukumäärän muuttuessa kaista jaetaan aina jäljellä olevien kesken. (Davidson & Peters 2002: 195-197.)

WFQ erottelee liikennevirrat toisistaan lähdeosoitteen, kohdeosoitteen, IP protokollan, TCP/UDP-porttinumeron ja ToS-tavun viiden viimeisen bitin avulla. WFQ:ta verrattaessa FIFO:n voidaan todeta, että se kohdistaa pakettien pudottamisen suurempiin datavirtoihin, jolloin pienet ja monesti tärkeämmät datavirrat jäävät yleensä koskemattomiksi. Jonoja voi oletuksena muodostua 256 erilaista, mutta tämäkin arvo on muutettavissa. (Vegesna 2001: 79-80.)

Ääniliikenteen kannalta WFQ tuo parannusta FIFO:n verrattuna, koska se vähentää verkossa esiintyvää värinää tasoittamalla liikennevirtojen kulkua. WFQ:n käyttöä ei suositella enää yli 2 mbps yhteyksiin. (Davidson & Peters 2002: 195-197.)

5.7.6 PQ

PQ (Priority Queuing) -menettely pohjautuu neljän jonon olemassaoloon. Se määrittelee jonot high-, medium-, normal- ja low-luokkiin. Jonojen purkaminen tapahtuu korkea-arvoisimmasta jonosta lähtien niin, että aina ylemmän jonon ollessa tyhjä aloitetaan seuraavan jonon tyhjentäminen. Tämä tarkoittaa siis sitä, että alaluokan tyhjentäminen vaatii, että kaikki sen yläpuolella olevat jonot ovat tyhjiä. Menettely mahdollistaa ääniliikenteen etuoikeutetun kohtelun, mutta saattaa johtaa tilanteisiin, joissa vähemmän tärkeä liikenne lopettaa toimintansa kokonaan kaistan olemattomuuden takia. (Vegesna 2001: 91-92.)

5.7.7 CQ

CQ (Custom Queuing) eroaa PQ:sta siten, että se ei varmista tärkeänliikenteen toimintaa vähemmän tärkeän liikenteen kustannuksella. Sen toiminta perustuu tärkeälle liikenteelle määritellystä kaistanleveydestä ja vähimmäiskaistanleveyden varmistamisesta jokaiselle jonolle. CQ:n toiminta muistuttaa painotettua round-robin menettelytapaa sekä CBWFQ (Class Based Weighted Fair Queue) -menettelyä. Käytettävissä on 16 eri jonoa sekä eristetty jono 0, jonka tarkoitus on palvella verkkolaitteiden välistä liikennöintiä. (Vegesna 2001: 94.)

CQ:n konfigurointi vaatii tietoutta verkossa liikennöivän liikenteen portti- ja liikennetyypeistä. Koska konfigurointi perustuu näihin ominaisuuksiin, kasvavat sekä menetelmän käyttöönoton vaikeusaste että siihen käytetty työpanos. (Davidson & Peters 2002: 198.)

5.7.8 CBWFQ

CBWFQ on WFQ:n muunnelma, jonka perusidea on sama kuin WFQ:ssa, mutta liikenteen jaottelu eri jonoihin tapahtuu liikennevirtojen sijasta luokittelun avulla. Luokittelun myötä liikennevirtoja voidaan niputtaa samoihin jonoihin, eikä kaikille liikennevirroille tarvitse muodostaa omaa jonoaan. Eri jonojen kaistanleveys määräytyy normaalissa WFQ:ssa liikennevirtojen lukumäärän mukaisesti, mutta CBWFQ:ssa on mahdollista allokoida haluttu kaistanleveys tietyn luokan liikenteelle. Näiden kahden tekniikan yhdistäminen on mahdollista, koska CBWFQ:ssa on olemassa oletusluokka, johon kaikki muu luokittelematon liikenne ohjautuu. Tähän oletusluokkaan on mahdollista aktivoida liikennevirtoihin perustuva liikenteen jonotuskäsittely. (Vegesna 2001: 85-86.)

Luokittelu voi perustua mm. DSCP-arvoihin, sisääntuloportin perusteella tai vaikkapa protokollatietoihin. (Vegesna 2001: 280.) Ääniliikenteen priorisoinnissa DSCP-arvojen mukainen luokittelu on hyvin loogista, koska nykyisin liikenteen luokittelu tapahtuu usein suoraan IP-pakettiin. Tällöin luokittelu on verkon reunalaitteiden tekemän työn jälkeen kevyttä, ja paketit pystyvät säilyttämään samanarvoisen palvelunlaadun verkon päästä päähän.

5.7.9 LLQ

LLQ (Low-Latency Queuing) eli alkuperäiseltä nimeltään PQ-CBWFQ (Class Based Weighted Fair Queue with Priority Queuing) yhdistää PQ-, CQ- ja WFQ-algoritmien parhaimpia ominaisuuksia. Sen toiminta jakautuu kahteen osioon. Ensinnäkin se mahdollistaa prioriteettijonon luomisen ja tälle tietyn kaistanleveyden varaamisen. Prioriteettijonon purkaminen tapahtuu aina PQ-algoritmin tavoin, etuoikeutetusti ennen muita jonoja. Prioriteettijonon lisäksi muut jonot toteutetaan CBWFQ:n tavoin luokitteluperiaatteella ja kaistanvarauksella. Näin saavutetaan reaaliaikaisille sovelluksille niiden vaatimusten mukaiset käsittelytavat ja dataliikenteelle optimoidut luokkakohtaiset käsittelytavat. (Szigeti & Hattingh 2005: 140-141.)

6 Ciscon laitteiden QoS-ominaisuudet

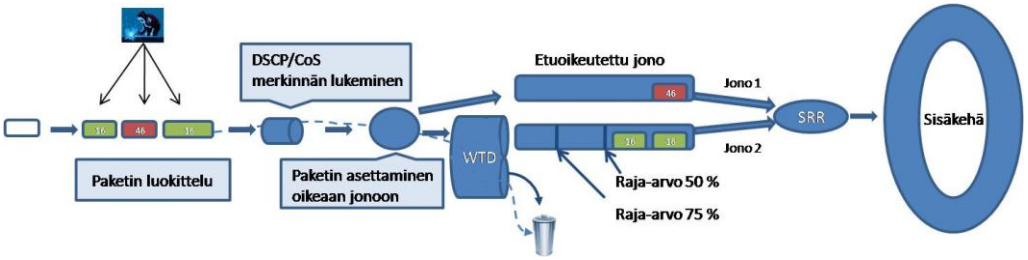
Palvelun laadun varmistamiseksi on kehitelty monia tekniikoita, mutta niiden käytössä tulee huomioida, että ne ovat aina laitteistoriippuvaisia. Harjoitustehtäviin valitut laitteet ovat Ciscon Catalyst 2960 -kytkin, Catalyst 3560 -reitittävä kytkin ja 2620-reititin. Näiden laitteiden ominaisuudet rajoittavat hyvin pitkälti, mitä QoS-ominaisuuksia voidaan käyttää tarvittavien PHB-kriteerien saavuttamiseksi. Catalyst 2960 ja 3560 -kytkimet ovat QoS-ominaisuuksiltaan aivan identtiset. Niiden ominaisuudet poikkeavat kuitenkin hyvin paljon edellisestä mallista. Reitittimissä ja kytkimissä Cisco käyttää eri ruuhkanesto- ja ruuhkanhallintatoimenpiteitä. Lisäksi reitittimissä voidaan käyttää liikenteen säännöstely- ja rajoittamistoimenpiteitä.

6.1 Catalyst 2960 -kytkin ja Catalyst 3560 -reitittävä kytkin

Tässä alaluvussa käsitellään 2960 ja 3560 -kytkinten QoS-prosessi keskeisimmiltä osilta. QoS-prosessin osat koostuvat luokittelusta, ennaltaehkäisevästä ruuhkanhallinnasta, jonotuksesta ja jonojen purkamisesta. Käsittelemättä jätetään luokitteluarvon muuttaminen ja alentaminen. Käytössä olevissa Catalyst 2960 -kytkimissä on IOS versio 12.2(25)SEE2 ja Catalyst 3560 -reitittävissä kytkimissä IOS versio 12.2(25)SEB4.

Catalyst 2960 -kytkin on kehittynyt sitten version 2950, jossa jonojen purku tapahtui WRR-algoritmin avulla ja liikennettä pystyttiin luokittelemaan vain CoS-arvojen perusteella. Lisäksi WRR:ä voitiin käyttää vain ulostuloportissa. Catalyst 2960 -kytkin käyttää kehittyneempää SRR-algoritmia jonojen purkamiseen ja mahdollistaa ruuhkia ennaltaehkäisevän WTD-algoritmin käytön. Uutuutena on myös mahdollisuus hyödyntää näitä QoS-tekniikoita joiltakin osin myös sisääntuloportissa.

Kuva 14 havainnollistaa paketin käymää QoS-prosessia laitteen sisääntuloportissa. Paketin saapuessa kytkimelle suoritetaan ensimmäisenä paketin luokittelu, jos luottamusrajan mukaisesti laitteen kuuluu se tehdä. Liikennettä voidaan luokitella CoS- tai DSCP-merkintöjen avulla. Luokittelun jälkeen seuraa luokittelun lukeminen. Tämän jälkeen paketti ohjataan luokittelun mukaiseen jonoon. Jonoja voi olla yksi tai kaksi kappaletta jokaista sisääntuloporttia kohden. Ennen jonoon asettamista joutuu paketti vielä Tail Drop- tai WTD-käsittelyyn riippuen siitä, kumpi niistä on asetettu aktiiviseksi. Jonoja tyhjennetään SRR-algoritmin avulla. SRR lähettää QoS-prosessin viimeisenä osana paketit kytkimen sisäkehälle (internal ring), jossa varsinaiset kytkentään vaikuttavat toiminnot suoritetaan. Sisäkehältä paketti siirretään johonkin ulostuloporteista, jossa se käy vielä uuden QoS-prosessin läpi. (Cisco Systems – Catalyst 2960… 2006.)



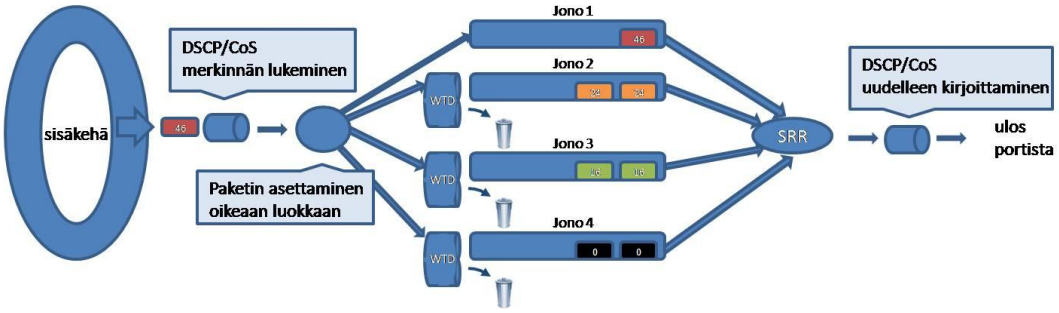
Kuva 14: Catalyst 2960 -kytkimen sisääntuloliitännän QoS-prosessi

Jos sisääntuloporttiin on asetettu Tail Drop aktiiviseksi, katsotaan ennen jonoon asettamista, onko tämä jono täynnä. Jos jono on täynnä, paketti pudotetaan. WTD-algoritmi voidaan asettaa jonoihin aktiiviseksi, jolloin niihin kohdistuvasta liikenteestä tarkistetaan, mahtuvatko ne ennalta asetettujen raja-arvojen sisälle. Jos jokin raja-arvo ylittyy tai jono on täynnä, paketti pudotetaan. WTD-algoritmia ei voi käyttää etuoikeutetussa jonossa. (Cisco Systems – Catalyst 2960… 2006.)

Kuvaan 14 on sisällytetty esimerkki WTD:n toiminnasta. Siinä nähdään, kuinka jonolle 2 on asetettu kaksi eri raja-arvoa. Seuraava paketti, joka on käsiteltävänä, kuuluu alimmaiseen jonoon ja on raja-arvon 50 % alainen. Jäljellä oleva vapaa tila jonossa ennen raja-arvoa on kuitenkin pienempi kuin paketin koko, joten WTD tulee pudottamaan paketin. Kuvassa paketin kulku on kuvattu sinisellä katkoviivalla.

Asetukset, joita kytkimelle täytyy tehdä, liittyvät luokitteluun, WTD- ja SRR-algoritmien toimintaan ja jonojen eli välimuistin koon määrittelyyn. Luokittelussa kiinnostava liikenne erotellaan ACL:n tai liitännän avulla muusta liikenteestä ja asetetaan sille haluttu luokitteluarvo. CoS-luokittelussa ei voida käyttää ACL:iä hyväksi, joten siinä on tyydyttävä liitäntäkohtaiseen luokitteluun. Tämä tarkoittaa käytännössä sitä, että yhdestä liitännästä tuleva liikenne luokitellaan aina yhteen luokkaan. Tämä ei mahdollista eri liikennetyyppien erottelua eikä näin kunnollista liikenteen luokittelua. DSCP-arvoja käytettäessä päästään ACL:ien avulla samasta portista saapuvia eri liikennetyyppejä luokittelemaan eri luokkiin. (Cisco Systems – Catalyst 2960… 2006.)

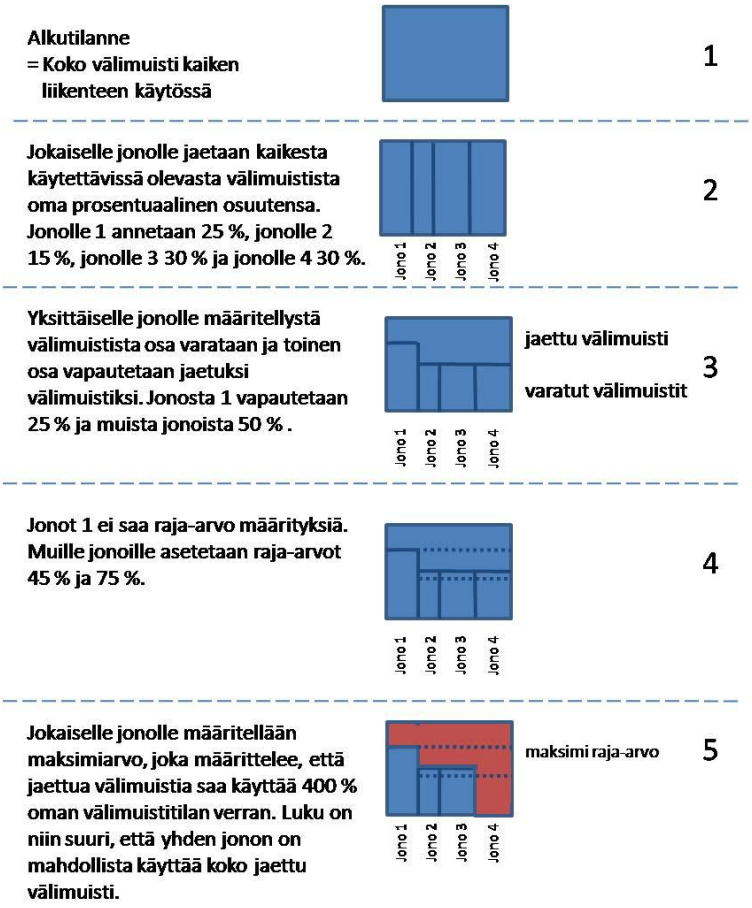
Sisäkehältä paketti jatkaa matkaa johonkin ulostuloporttiin. Ulostuloportin QoS-prosessi on kuvattu kuvassa 15. Ulostuloportilla luetaan paketin DSCP/CoS-merkintä. Tämän perusteella katsotaan, mihin luokkaan paketti kuuluu ja kuuluuko se Tail Drop:n tai WTD:n piiriin. Jos paketti ylittää jonkin raja-arvon tai jono on täynnä, pudotetaan paketti. Muussa tapauksessa paketti asetetaan jonoon. WTD:tä ei ole mahdollista asettaa aktiiviseksi prioriteettijonoon. Jonoja on ulostuloporteissa mahdollista olla neljä kappaletta sisääntuloportin kahden sijasta. Jonojen purku tapahtuu SRR:n mukaisesti samalla tavalla kuin sisääntuloportissakin. Lopussa pakettiin on vielä mahdollista tehdä muutoksia DSCP/CoS-kenttään, ennen kuin se lähetetään portista siirtomediaan. (Cisco Systems – Catalyst 2960… 2006.)



Kuva 15: Catalyst 2960 -kytkimen ulostuloliitännän QoS-prosessi

Jonot

QoS-prosessissa olevien jonojen konfigurointi tapahtuu viidessä eri vaiheessa. Kuvassa 16 käydään läpi esimerkin avulla, kuinka konfigurointi tapahtuu. Jonojen konfigurointi aloitetaan välimuistin jakamisella jonojen kesken. Tämän jälkeen halutuista jonoista osa voidaan vapauttaa kaikkien jonojen yleiseen käyttöön. Jos halutaan käyttää WTD-algoritmia, määritellään neljännessä kohdassa jokaiselle jonolle sen tarvitsemat raja-arvot. Viimeisenä toimena määritellään jokaiselle jonolle maksimiarvo, johon jono saa kasvaa, mikäli yleisessä käytössä olevaa muistia on vapaana.



Kuva 16: Välimuistin allokointi Catalyst 2960 ja 3560 -kytkimissä

SRR:n konfiguroinnissa on mahdollista määritellä prioriteettijono ja eri jonojen purkamiseen käytetyt painoarvot. Liitteessä 1 on käyty tarkemmin lävitse konfigurointiasetuksia ja kuinka niitä käytetään.

6.2 2620-reititin

Reitittimien QoS-ominaisuudet ovat huomattavasti monipuolisemmat kuin kytkinten. Kytkimissä on yleensä yksi ratkaisumalli palvelun laadun takaamiseksi, mutta reitittimissä ominaisuuksia on todella runsaasti. Reitittimissä QoS-ominaisuudet, joita on mahdollista käyttää, riippuvat käytettävistä yhteystyypeistä. Reititin pystyy käyttämään lähestulkoon kaikkia niitä palvelun laadun varmistamisen keinoja, joita tässä opinnäytetyössä on käsitelty.

Käytettävissä on mm. seuraavia ominaisuuksia:

- cRTP
- CAR (Committed Access Rate)
- IP Precedence
- PBR (Policy Based Routing)
- BGP (Border Gateway Protocol) Propagation
- WFQ
- CQ & PQ
- FIFO
- VIP-Distributed WFQ
- CBWFQ
- IP RTP Priority
- Frame Relay RTP Priority
- LLQ
- WRED
- DWRED (distributed WRED)
- Flow-based WRED
- GTS (Generic Traffic Shaping)
- FRTS (Frame Relay Traffic Shaping)
- CAR Rate limiting
- RSVP
- CRTP
- IP to ATM (Asynchronous Transfer Mode) CoS.

(Cisco Systems – Cisco IOS… 2006.)

Käytössä olevissa reitittimissä on IOS versio 12.2(13b).

7 Käytännön harjoittelukokonaisuus

Käyn harjoitustehtävien tekemiseen liittyneen prosessin läpi viidessä vaiheessa. Ensin pohdin ja rajaan harjoitustehtävien sisältöä. Tämän jälkeen suunnittelen harjoitusten tuottamista. Itse harjoitustehtävät käyn läpi yksitellen toteutukseen paneutuvassa aliluvussa. Tuon myös esiin ongelmakohtia, joita esiintyi harjoitusten tekovaiheessa. Lopuksi kuvaan, kuinka testasin harjoitusten toimivuutta. Harjoitusten ja oppituntien onnistumista pohdin luvussa 8.

7.1 Sisältö ja sen rajaus

Työ koostuu sarjasta harjoituksia, jotka on ajallisesti määrä tehdä yhden kokonaisen opiskelupäivän puitteissa eli noin 8 tunnin aikana. Tähän aikarajaan kuuluu tämän työn tuloksena muodostuvien harjoitustöiden tekeminen ja niiden tekoa edeltävä lyhyt luento. Tuntien aikana käydään myös pienryhmäkeskusteluja. Aiheen teoriatiedon opiskeleminen ei kuulu aikarajaan. Teoriatietoa opiskelijat lukevat ennakkoon kurssin materiaaleista. Harjoitustehtävien jälkeen opiskelijat voivat laajentaa tehtävissä opittujen taitojen teoria pohjaa lukemalla tämä opinnäytetyö, tai he voivat tutkia harjoitusmateriaalissa mainittuja verkkolähteitä. Harjoitusmateriaalin tarkoitus ei ole suoranaisesti selittää kaikkea mahdollista teoriatietoa, vaan pikemminkin kertoa vain välttämättömin. Tiettyjä faktoja tehtävämateriaalissa on pakko käydä läpi, koska tehtävissä esiintyy täysin uusia ja ennalta tuntemattomia tekniikoita.

Itse harjoitukset ovat sisällöltään ääniliikenteen palvelun laadun varmistamista. Ääniliikenne tuo omat vaatimuksensa tietoverkoille, ja näitä vaatimuksia vastaan pyritään varmistamaan ääniliikenteen häiriötön kulku. Suurin huomio harjoituksissa kiinnitetään verkon hitaiden linkkien ja verkossa esiintyvien ruuhkahuippujen käsittelemiseen. Tärkein yksittäinen opittava asia on liikenteen luokitteleminen.

Harjoitusten tekeminen on rajattu Ciscon Catalyst 2960 ja 3560 -kytkimille sekä 2620-reitittimille. Harjoituksen tekeminen ei onnistu muunlaisilla laitteilla. Koska käytössä ei ole Ciscon IP-puhelimia, täytyy tehtävät suorittaa ilmaisilla Softphone-puhelimilla. Verkon ruuhkautuminen täytyy luoda keinotekoisesti joko tähän tarkoitukseen suunnitellulla ohjelmalla tai käyttämällä jotakin paljon kaistaa kuluttavaa tiedostonsiirtoa. Linkkien nopeuden pudottaminen mahdollisimman alhaiseksi helpottaa ruuhkauttamista.

Tehtävissä haluan käydä läpi kytkinten QoS-prosessin keskeisimmiltä osiltaan kuitenkin niin, että yksinkertaistan prosessia jonkin verran. Jätän siitä käsittelemättä luokitteluun liittyvät CoS-DSCP muunnostaulukot, DSCP-CoS mutation map -käsittelyn ja luokittelumuutosten tekemisen.

7.2 Suunnitelma

Aikomuksenani on tehdä työharjoituksia opiskelijoille liittyen palvelun laadun varmistamiseen verkossa, johon on implementoitu VoIP-tekniikkaa. Ääniliikenne on hyvin herkkää erilaisille tietoverkoissa esiintyville ominaisuuksille, kuten värinälle ja viiveelle, joten se tulee erotella ja priorisoida muuhun liikenteeseen verrattuna. Harjoituksieni avulla opiskelijoiden tulisi saavuttaa kokonaiskuva verkkoliikenteen luokittelusta ja sen hyödyntämisestä. Pääpaino harjoituksissa on ääniliikenteen luokittelulla ja sen priorisoinnilla muun verkkoliikenteen edelle. Tällä tavalla ääniliikenteelle varmistetaan riittävä palvelun laatu, mikä riittää laadukkaisiin VoIP-puheluihin.

Harjoituksista on tarkoitus saada opiskelijoille mahdollisimman mielenkiintoisia ja muihin kurssin harjoituksiin verrattuna erilaisia. Haapakankaan (6.11.2006, haastattelu) mukaan harjoituksissa tehtävät toimet olisi hyvä olla mahdollisimman suoraviivaisia. Hänen mielestään tilanteisiin tulisi näyttää vain yksi ratkaisumahdollisuus, jotta tehtävät eivät muodostu liian sekaviksi. Opiskelijoiden onkin tärkeää ymmärtää tekemänsä ja saada käsiteltävästä aiheesta hyvin selkeä kuva. Olisi myös hienoa, jos opiskelijat saisivat aiheeseen innostuksen ja haluaisivat asiasta lisää tietoa. Syventävää tietoa aiheesta saa jo lukemalla tämän opinnäytetyön.

Harjoituksia suunnittelen tekeväni kolme kappaletta. Ajan tehokasta käyttöä tukee, jos verkon topologia ei suuresti muutu harjoituksesta toiseen. Tämä myös yhtenäistää harjoituskokonaisuutta.

Ensimmäisen harjoituksen tulee sisällöltään käsitellä liikenteen luokittelua, koska tehokkaiden QoS-ominaisuuksien käyttäminen vaatii sitä. Luokittelu on mahdollista todentaa liikenteenkaappausohjelmalla. Toinen harjoitustehtävä voidaan aloittaa soittamalla IP-puhelu verkon läpi ja toteamalla VoIP-puhelun hyvä toiminta. Tämän jälkeen verkko ruuhkautetaan streamingmedia-sovelluksella ja todetaan puhelulaadun heikkeneminen. Kun tiedostetaan, että verkkoon täytyy tehdä jotakin toimenpiteitä äänenlaadun säilyttämiseksi, aloitetaan äänipuheluita tukevat toimenpiteet. QoS-toimiin kuuluu liikenteen luokittelu, ennaltaehkäisevät ruuhkanhallinta toimet ja ruuhkatilanteiden hallinta. Lopussa VoIP-puhelun uudelleen soittaminen todentaa, kuinka tehdyt toimenpiteet vaikuttavat verkon toimintaa parantavasti. Kolmanteen harjoitustehtävään voisi sisällyttää SIP-puhelinvaihteen käytön ja WAN (PPP) -yhteydessä käytettävän LFI-toiminnon todentamista.

Ensimmäisen ja toisen harjoituksen konfigurointia tehdessä käytän apuna Cisco Systemsin laitekohtaisia konfigurointioppaita (Cisco Systems – Catalyst 2960… 2006.; Cisco Systems – Catalyst 3560… 2005). PPP-yhteyden ja LFI-toiminnon konfiguroinnissa käytän apuna Cisco Systemsin aihetta käsittelevää dokumenttia (Cisco Systems – VoIP over PPP… 2003).

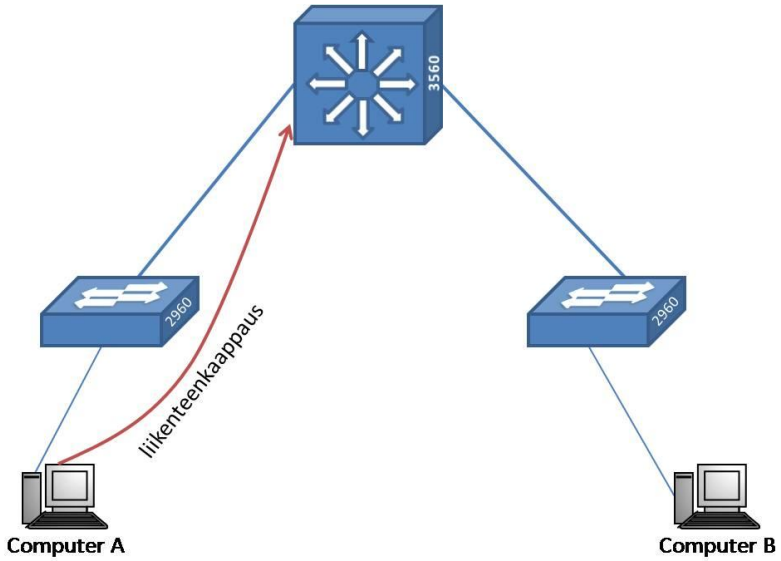
Harjoituksissa toivottiin käytettävän uusimpia koulussa olevia laitteita (Haapakangas 6.11.2006, haastattelu; Hakonen 31.10.2006, haastattelu). Uusia laitteita on rajoitetummin käytössä kuin vanhempia. Yhdelle opiskelijaryhmälle riittää käyttöön kaksi Catalyst 2960 -kytkintä, yksi Catalyst 3560 -kytkin ja kaksi 2620-reititintä. Reitittimistä on saapunut myös uudempia 2800-sarjan malleja, mutta näistä ei kuitenkaan riittäisi kuin yksi laite kullekin ryhmälle. Kolmannessa harjoituksessa tarvitaan joka tapauksessa kaksi reititintä, joten niiden käyttö ei ole mahdollista.

7.3 Toteutus

Harjoitustehtävä 1

Harjoitukset pohjautuvat DiffServ-arkkitehtuurin määrittelemään liikenteen luokittelemiseen ja näiden luokkien palvelun laadun takaamiseen. Ensimmäinen harjoitus käy läpi luokittelua OSI:n 2- ja 3-kerroksella ja todentaa luokittelubittien muutokset liikenteenkaappauksen avulla.

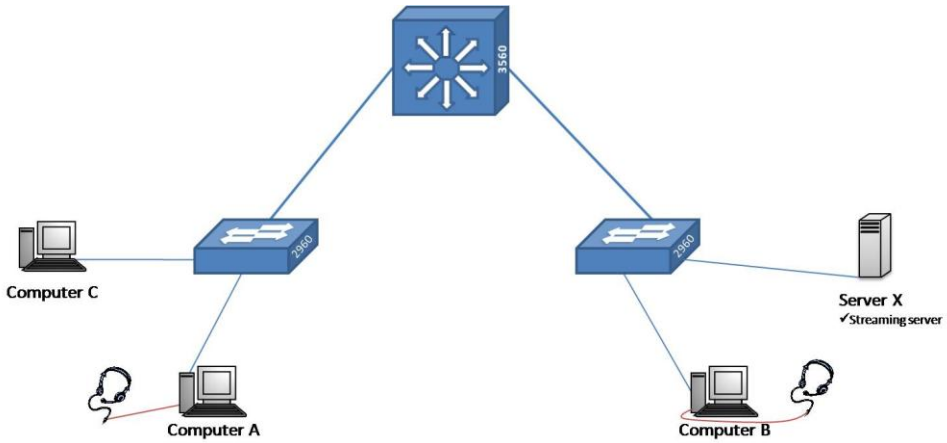
Harjoitustehtävä 1 jakautuu seitsemään eri osa-alueeseen. Kuvassa 17 on kuvattu harjoituksen topologia. Harjoitus löytyy kokonaisuudessaan liitteestä 1. Ensimmäisessä harjoituksessa opiskelija omaksuu teoriaa DiffServ-arkkitehtuurista. Tämän jälkeen rakennetaan verkko, jonka avulla voidaan harjoitella DiffServ-arkkitehtuurin mukaista liikenteen luokittelua. Verkko tulee toimimaan pohjana myös tuleville harjoituksille. Seuraavat neljä kohtaa opettavat opiskelijat luokittelemaan liikennettä DSCP- ja CoS-merkinnän avulla OSI:n 2- ja 3-kerroksella. Luokittelun toteuttamisen jälkeen seuraa aina sen todentaminen. Lopuksi harjoituksessa palautetaan verkko toimivaan lähtötilanteeseen, jolloin siitä pystytään jatkamaan suoraan harjoitustehtävä 2:en.



Kuva 17: Harjoitustehtävä 1:n topologia

Harjoitustehtävä 2

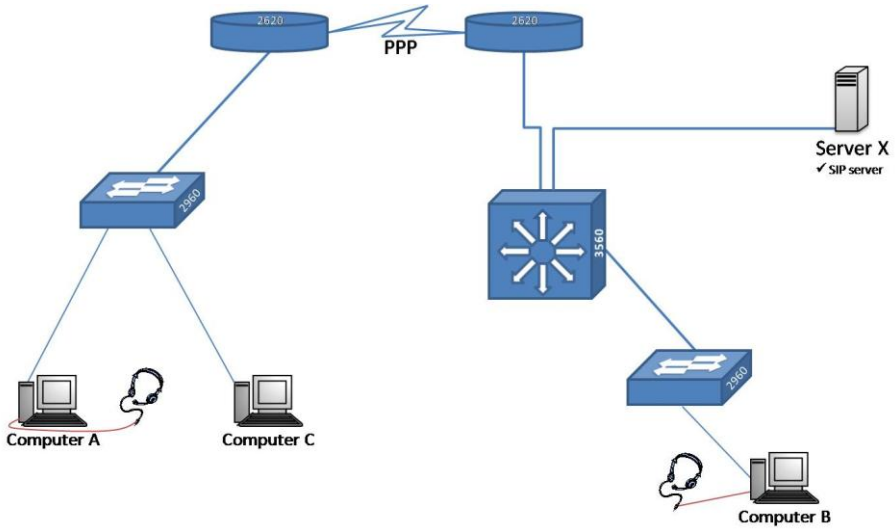
Harjoituksista haastavin on harjoitustehtävä 2. Se paneutuu käytössä olevien kytkinten konfiguroimiseen WRR- ja SRR-algoritmien osalta sekä välimuistin jakamiseen. Harjoituksen topologia esitellään kuvassa 18. Edellisessä harjoituksessa opittu liikenteen luokittelu otetaan harjoituksessa käyttöön, käytetään SoftPhone-sovellusta, ja opitaan streamaamaan mediaa verkkoon. Tämän jälkeen opetellaan konfiguroimaan kytkimiin tarvittavat QoS-toimet. Harjoituksessa todennetaan QoS-asetuksien toiminta seuraavasti. Tehtävän alussa soitetaan VoIP-puhelu ja todetaan sen häiriötön toiminta. Tämän jälkeen verkkoon lisätään streamingmedia-sovelluksella videoliikennettä ja soitetaan puhelu uudestaan. Puhelu muuttuu sietämättömäksi, mutta videokuvassa ei esiinny minkäänlaista häiriötä. QoS-asetuksien asettamisen jälkeen soitetaan jälleen VoIP-puhelu, kun verkossa on samanaikaisesti videostreamingiä. Puhelu kulkee asetusten myötä häiriöttä, mutta videossa esiintyy rakeisuutta. Tästä voidaan huomata, kuinka ääniliikenne saa osan videoliikenteen kaistasta käyttöönsä, sekä todennetaan QoS-asetuksien vaikutusta verkon toimintaan.



Kuva 18: Harjoitustehtävä 2:n topologia

Harjoitustehtävä 3

Tehtävän päätarkoitus on opettaa ja todentaa LFI-tekniikan toiminta. Siinä käytetään LFI-tekniikan kanssa LLQ-ruuhkanhallintaa. Tehtävässä käydään läpi myös SIP-palvelimen käyttöä VoIP-puheluliikenteen ohjaamisessa. LFI:n toiminnan merkitys todennetaan lähettämällä ping-pyyntöjä PPP-linkin ylitse, jossa samanaikaisesti siirretään FTP-liikennettä. Ennen LFI:n aktivoimista ping-pyyntöjen vastausajoissa on huomattavissa suuria vaihteluita, jotka johtuvat siitä, että ping-paketteja jää suurien FTP-pakettien taakse jonottamaan. Aktivoinnin jälkeen vastausajat pysyvät tasaisina. Harjoituksen topologia on esitetty kuvassa 19.



Kuva 19: Harjoitustehtävä 3:n topologia

7.4 Ongelmakohdat

Ensimmäinen ongelma tuli esille katsottaessa ethernet-kehyksen bittejä Wireshark-ohjelmalla. Ohjelma ei aluksi näyttänyt ollenkaan 802.1p/Q-kehystä. Ratkaisuna selvisi, että jotkin verkkokortit sisältävät asetuksissaan valinnaisen option, joka päällä ollessaan poistaa VLAN-kehyksen paketin saapuessa verkkokortille. Näin verkkokortin jälkeen paketin vastaanottava käyttöjärjestelmä ja siinä olevat ohjelmat eivät näe VLAN-kehystä ollenkaan.

Koska ideana oli tehdä rakenteeltaan yksinkertaisia harjoituksia, minun tuli löytää tarvittavat ohjelmat, joiden käyttöliittymä ja toiminta olisivat suhteellisen pelkistettyjä. Lisäksi näiden ohjelmien tuli olla vapaasti käytettävissä olevia eli käytännössä open source- tai freeware-ohjelmia. Streaming media server -sovellus nimeltään VLC media player löytyi nopeasti ja samoin Wireshark-liikenteenkaappausohjelma. Softphone-ohjelmaksi kokeilin TalkByPC-, SJphone- ja Iaxcomm-ohjelmia. Ne eivät kuitenkaan soveltuneet kaikilta osin tarkoituksiini. Lopulta pitkän etsinnän ja kokeilun tuloksena löysin Express Talk -ohjelman, jonka perusversio on täysin ilmainen. Kolmanteen harjoitukseen SIP-palvelimeksi valitsin Express Talk -ohjelman ja tekijöiden toisen ohjelmiston Axon Virtual PBX -puhelinvaihdesovelluksen, joka on myös ilmainen.

Vaikeutta harjoituksen 2 tekemisessä tuotti Ciscon laitteiden suorituskyky ethernet-yhteydessä. Minun nimittäin täytyi saada laskettua ethernet-liitännän nopeutta tarpeeksi alas, jotta verkko saadaan ruuhkautettua helpommin. Sinänsä harvinainen vaatimus, mutta tässä tapauksessa se on välttämätöntä. Nopeuden laskeminen onnistui 100 Mb full duplex -tilasta 10 Mb half duplex -tilaan helposti, mutta tästä alaspäin nopeuden lasku onnistuu vain QoS-asetuksien kautta. Tämä kuitenkin aiheuttaisi harjoi-

tusten rakenteeseen liiallista monimutkaisuutta, joten ensin mainitulla nopeudenpudotuksella täytyy tulla toimeen.

Suuria ponnisteluja toisessa harjoitustehtävässä tuotti QoS-asetuksien tekeminen niin, että videolähetyksen kaistankäyttö pieneni niin paljon, että äänipuhelun toiminta oli täysin häiriötöntä. Huomioitavaa oli, että mikäli rajoitin videolähetyksen kaistankäyttöä liikaa, katkesi lähetys kokonaan.

Viimeisessä harjoituksessa jouduin luopumaan VoIP-puhelun ja videostreamingin avulla tehtävästä todentamisesta, koska niiden kaistankäyttö oli liian suurta käytössä olleeseen PPP-linkkiin. LFI:n toiminnan todennus onnistui lopulta ping-pakettien vastausaikavertailulla.

7.5 Testaus

Suunniteltuani yhden harjoituksen sisällön, testasin sen toimivuuden käytössäni olleessa harjoitusympäristössä. Harjoitusympäristössäni oli käytettävissä samat laitteet, joita opiskelijoillakin tulee olemaan käytössään. Saatuani suunnitellun harjoituksen sisällön toimimaan, esittelen sen sisällön opettajille, joiden käyttöön työ lopulta tulee. Tämän jälkeen tein työhön vielä tarvittavia muutoksia ja parannuksia. Muutoksien jälkeen testasin niiden toiminnan vielä kertaalleen. Otin laitteilta konfigurointiasetukset talteen tehtävän jokaisen vaiheen jälkeen. Näin on mahdollista palata tarpeen tullen nopeasti johonkin vaiheeseen harjoitusta. Lisäksi tarvitsin kuvaruutukaappauksia eri ohjelmien käytöstä ja asetuksista havainnollistamaan opiskelijoille niiden käyttöä.

Tehtyäni harjoitukset valmiiksi testautin ne eräällä opiskelijalla. Hän ehti testaamaan ensimmäisen harjoitustehtävän kokonaan, jonka jälkeen loput harjoitukset käytiin läpi vain keskeisimmiltä osilta. Testauksessa onnistuttiin löytämään muutama konfigurointivirhe ja muita pieniä tekstivirheitä. Kokonaisuudessaan harjoituksista ei löydetty mitään poikkeavaa tai toimimatonta.

7.6 Opetuspäivät

Materiaalin tuottamiseen liittyi opetuspäivien pitäminen, jossa opiskelijat tekivät tekemäni harjoitusmateriaalin. Opetuspäivät pidin sovitusti ajallaan, ja ne olivat mielestäni onnistuneet. Aamun aiheeseen perehdyttävän luennon aloitin klo 08.30, ja se kesti molempina päivinä n. 45 minuuttia. Erityisesti jälkimmäisen ryhmän kuulijakunta kehui esityksen helppoa ymmärrettävyyttä ja kiinnostavuutta. Kyseltyäni opiskelijoilta harjoituksista jälkeenpäin, he kertoivat niiden olleen selkeitä, sisällöltään sopivia, erittäin havainnollisia ja positiivisesti erilaisia kurssin muihin harjoituksiin nähden. Yhteensä kuudesta ryhmästä kaksi ennätti tekemään kaikki harjoitukset, kolme pääsi puoliväliin viimeistä harjoitusta ja yksi ryhmä

ei aloittanut viimeistä harjoitusta ollenkaan. Ryhmät poistuivat tunneilta klo 15.15–16.00 aikoihin. Ne ryhmät, jotka ehtivät tehdä kaikki harjoitukset, pitivät harjoitusten sisältöä sopivana, mutta muut ryhmät olisivat voineet jättää kolmannen harjoituksen tekemisen toiselle päivälle. Opiskelijat kokivat yleisesti, että ohjaajan, eli minun, läsnäolo oli lähes välttämätöntä harjoituksia tehtäessä. Mielestäni asia olisi voinut olla toisin, mikäli he olisivat lukeneet tunnille ennakkolukemiseksi määritellyn materiaalin. Kysymysteni valossa juuri kukaan opiskelijoista ei ollut lukenut ennakkomateriaalia kunnolla.

Mielestäni suurimmat hidasteet opiskelijoilla johtuivat huolimattomasta ohjeiden lukemisesta ja heidän tekemistään pienistä konfigurointivirheistä. Opastustani he tarvitsivat uusien asioiden soveltamista vaativissa tilanteissa. Uskon, että harjoitukset on mahdollista tehdä ilman ohjausta, mikäli ne tehdään huolella ja asiaan paneutuen. Tällöin ehdottoman tärkeää olisi, että asiaan olisi perehdytty etukäteen kurssin materiaalin avulla.

Toisessa harjoituksessa käytetyn videostreaming-lähetyksen tarkoituksena oli tukkia käytettävissä oleva kaista ja aiheuttaa häiriötä linkissä kulkevalle äänipuhelulle. Häiriötä ei kuitenkaan esiintynyt neljällä ryhmällä, vaan heidän tapauksessaan jouduttiin käyttämään kahta videotreaming-lähetystä. Tämä aiheutti ongelmia harjoituksen myöhemmässä vaiheessa, koska harjoitukseen suunnittelemani QoS-asetukset olivat riittämättömät varmistamaan ääniliikenteen häiriöttömän kulun linkissä, jossa nyt kulki kaksi videostreaming-lähetystä. Vaikka ääniliikenne ei asetusten myötä parantunut täysin häiriöttömälle tasolle, se parani kuitenkin siedettäväksi. Tämä riitti lopulta tekemään harjoituksen idean selväksi, eli todistamaan, että QoS-asetuksilla päästään parantamaan äänipuheluiden kulkua ruuhkaisessa verkossa. Ryhmillä, joilla riitti yksi videostreming-lähetys tukkimaan kaistan, ei harjoituksessa ilmennyt minkäänlaisia ongelmia. Syytä tähän ongelmaan ei löydetty.

8 Pohdintaa

Ennen opinnäytetyön tekemistä ei minulla ollut minkäänlaista tietoa VoIP-tekniikasta, en ollut koskaan käyttänyt Catalyst 2960 ja 3560 -kytkimiä ja DiffServ-arkkitehtuuri oli minulle täysin tuntematon. Toisaalta minulla oli vankka kokemus QoS:sta, Ciscon laitteista ja Ciscon laitteiden konfiguroimisesta. Lisäksi verkkotekniikka oli minulla erinomaisesti hallussa. Näistä lähtökohdista lähdin työstämään toimeksiantoa ja opinnäytetyötä. Lopputulos, jonka lopulta saavutin, ylitti omat sekä toimeksiantajani odotukset. Toimeksiantajan positiivinen palaute yhdessä opiskelijoiden palautteiden kanssa sai minut uskomaan, että olen saavuttanut jotakin hyvin hyödyllistä, josta kaikki osapuolet hyötyvät.

Työn tavoitteena olleet harjoitustehtävät valmistuivat ajallaan samoin kuin opetuspäivät. Harjoitustehtävät ja opetuspäivät pitivät olla valmiit hyvin tiukkojen aikarajojen sisällä, koska ne sopivat sisällöltään juuri tiettyyn kohtaan kurssia. Kokonaisuudessaan opinnäytetyö valmistui ennen asettamaani viimeistä takarajaa. Harjoitustehtävien tuottamiseen kului suunniteltua enemmän aikaa, koska työn alkuvaiheessa ei sen haastavuudesta ollut vielä kunnollista kokonaiskuvaa. En usko, että ylimääräinen aika ja ponnistelut olivat turhia, koska ilman kunnollista paneutumista aiheeseen ei lopputulos olisi ollut näin onnistunut.

Työhön liittynyt teoria oli mielestäni hyvin vaativaa ja se käsitteli VoIP-tekniikkaa ja QoS-ominaisuuksia hyvin syvällisesti. Tästä huolimatta onnistuin kokoamaan siitä kohtuullisen tiivistetyn tietosisällön sekä harjoitustehtäviin että opinnäytetyöhön. Aiheeseen liittyvää kirjallisuutta oli hyvin vähän saatavilla kirjastoissa, joten päädyin tilaamaan muutaman teoksen ulkomailta asti.

Kehitysideat

Harjoituksia olisi mahdollista parantaa selkeyttämällä aiheen teoriaosuuksia ja eriyttämällä selkeämmin suoritettavien tehtävien osuudet. Vaikka harjoitukset pyrkivät olemaan yksinkertaisia tehdä, oli niiden tuottaminen hyvin monimutkaista, joten joitakin pieniä virheitä olisi saatu karsittua paremmalla testaamisella. Parempi testaus olisi kuitenkin vaatinut lisää resursseja käyttöön.

Opetuspäivien läpivientiä olisi helpottanut, jos opiskelijoita olisi motivoitu paremmin ennakkomateriaalin lukemiseen. Aiheen vaativuustaso tuntui olevan korkea joillekin opiskelijoille, joten harjoitusten välissä olisi voinut hieman kerrata joitakin teoriasisällön osa-alueita. Kolmas harjoitus jäi kesken osalla ryhmistä, joten sen tekeminen olisi voitu jättää opiskelijoille tuntien ulkopuolella tehtäväksi. Vapautunut aika olisi voitu käyttää syventämään kahden ensimmäisen harjoituksen oppimista. Toisaalta kolmannen tehtävän sai osa suoritettua, eivätkä he valittaneet sen tekemisestä lainkaan. Tämä viittaa siihen, että nimenomaan parempi ennakkomateriaalin lukeminen olisi nopeuttanut harjoitusten tekemistä.

Jos harjoituksia lähdetään tuottamaan lisää tähän harjoitussarjaan, olisi videoliikenteen ja VoIP-liikenteen yhdistäminen looginen jatke, koska tarve tilausvideoihin ja videoneuvotteluihin on lisääntynyt. Harjoituksissa on jo valmiiksi videostreaming-lähetys, ja tämän lähetyksen muuttaminen unicast-lähetyksestä multicast-lähetykseksi onnistuu käytössä olevalla VLC Media Player -sovelluksella. Tarvittavat laitteet ja ominaisuudet löytyvät siis jo harjoitusympäristöstä. Jotta multicast-ominaisuutta voidaan hyödyntää, täytyy kaikki verkon laitteet konfiguroida tukemaan multicast-ominaisuutta. Todennus olisi mahdollista tehdä lähettämällä videostreaming-lähetys multicastina kahdelle koneelle verkon päästä päähän ilman verkkolaitteiden multicast-asetuksia. Tällöin liikenne kulkisi todella huonosti hitaimman linkin lävitse ja VoIP-liikenne kärsisi tilanteesta. Tämän jälkeen multicast-asetukset tehtäisiin ja lähetys lähetettäisiin uudestaan, minkä jälkeen lähetys kulkisi yhtenä lähetyksenä verkon läpi ja ongelmat saataisiin karsittua pois. Verkossa täytyisi olla vähintään yksi linkki, jossa yksi videostreaming-lähetys voisi kulkea häiriöittä, mutta kaksi lähetystä aiheuttaisi häiriötä lähetyksiin. Liittämällä tämä kaikki harjoituksessa olevaan VoIP-verkkoon saataisiin aikaan tilanne, josta nähtäisiin VoIP-liikenteen ja videoliikenteen toiminta samassa verkossa.

Loppusanat

Onnistuin mielestäni rakentamaan harjoituksiin tiiviin ja tietosisällöltään rikkaan kokonaisuuden. Pyrin aktivoimaan opiskelijoita välikysymyksillä ja käyttämällä harjoitusten edetessä työvaiheita, jotka pohjautuvat aiemmin harjoituksissa opittujen asioiden omatoimiseen soveltamiseen. Mielestäni parhaita kohtia harjoituksissa ovat asetusten toiminnan todentamiseen käytettyjen käytännönläheisten keinojen käyttö, kuten oikeiden VoIP-puhelujen soittaminen ja videoliikenteessä näkyvien muutosten tulkinta. Ne tuovat selkeästi esille harjoitusten pääidean.

Kun opiskelijat olivat tehneet harjoitustehtävät ja olin tehnyt oman analyysin harjoitusten onnistumisesta, tein harjoitustehtäviin vielä pieniä muutoksia. Tämän työn liitteeksi (liite 1) liitin korjatun version. Harjoituksista jäi opiskelijoille paperiversio, sekä kurssin kotisivuille jätin korjatun version sähköisenä kappaleena. Kotisivuille liitin myös luennoille tekemäni PowerPoint-diat.

Lähteet

Kirjat

Davidson, Jonathan & Peters, James 2002. Voice over IP. Helsinki: Edita.

Ellis, Juanita, Pursell, Charles & Rahman, Joy 2003. Voice, Video, and Data Network Convergence: Architecture and Design, From VoIP to wireless. San Diego: Academic Press.

Hersent, Olivier, Petit, Jean-Pierre & Gurle, David 2005. Beyond VoIP Protocols: understanding voice technology and networking techniques for IP telephony. Chichester: Wiley.

Swale, Richard 2001. Voice over IP: systems and solutions. United Kingdom: BT EXACT TECHNOLOGIES.

Szigeti, Tim & Hattingh, Christina 2005. End-to-End Qos Network Design: Quality of Service in LANs, WANs, and VPNs. USA: Cisco Press.

Tanenbaum, Andrew S. 2003. Computer Networks. USA: Pearson Education, Inc.

Vegesna, Srinivas 2001. IP Quality of Service. USA: Cisco Press.

Haastattelut

Haapakangas, Ville. Tampereen ammattikorkeakoulu, lehtori. Haastattelu 6.11.2006. Tampere

Hakonen, Harri. Tampereen ammattikorkeakoulu, lehtori. Haastattelu 31.10.2006. Tampere.

Artikkelit

Rapo, Raija 2006. Voip on vakiintunut USA:ssa. Kauppalehti 19.12.2006, 15.

Salovuori, Jarno 2006. Puhe siirtyy lähiverkkoon. Kauppalehti Vip 30.10.2006, 15.

Verkkolähteet

Cisco Systems – Catalyst 2960 Switch Software Configuration Guide: Configuring QoS 2006. [online] [viitattu 8.1.2007]. http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2960/12225see/scg/swqos.htm

Cisco Systems – Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(19) EA1 2003. [online] [viitattu 10.1.2007]. http://www.cisco.com/application/pdf/en/us/guest/products/ps646/c2001/ccmigration_09186a00801cdf54.pdf

Cisco Systems – Catalyst 3560 Switch Software Configuration Guide: Configuring QoS 2005. [online] [viitattu 8.1.2007]. http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3560/1225sea/3560scg/swqos.htm

Cisco Systems – Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 2006. [online] [viitattu 19.3.2007]. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/qcfbook.pdf

Cisco Systems – VoIP over PPP Links with Quality of Service (LLQ / IP RTP Priority, LFI, cRTP) 2006. [online] [viitattu 10.12.2006]. http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.html

IETF n.d. [online] [viitattu 12.3.2007]. http://www.ietf.org/overview.html

IETF 3261 SIP: Session Initiation Protocol 2002. [online] [viitattu 19.3.2007]. http://www.ietf.org/rfc/rfc3261.txt

ITU-T G.114 One-way transmission time 2003. [online] [viitattu 6.3.2007]. http://www.itu.int/rec/T-REC-G.114/en

RFC 2475 An Architecture for Differentiated Services 1998. [online] [viitattu 19.3.2007]. http://www.ietf.org/rfc/rfc2475.txt

RFC 3550 RTP: A Transport Protocol for Real-Time Applications 2003. [online] [viitattu 6.3.2007]. http://www.rfc-editor.org/rfc/rfc3550.txt

Suomen Standardisoimisliitto SFS n.d. [online] [viitattu 12.3.2007]. http://www.sfs.fi/

Viestintävirasto – ETSI 2006. [online] [viitattu 12.3.2007]. http://www.ficora.fi/index/palvelut/standardointi/etsi.html

Viestintävirasto – ITU-T 2006. [online] [viitattu 12.3.2007]. http://www.ficora.fi/index/palvelut/standardointi/itut.html

Liitteet

Liite1: Harjoitustehtävät

TYÖHARJOITUS 1 - LIIKENTEEN LUOKITTELU

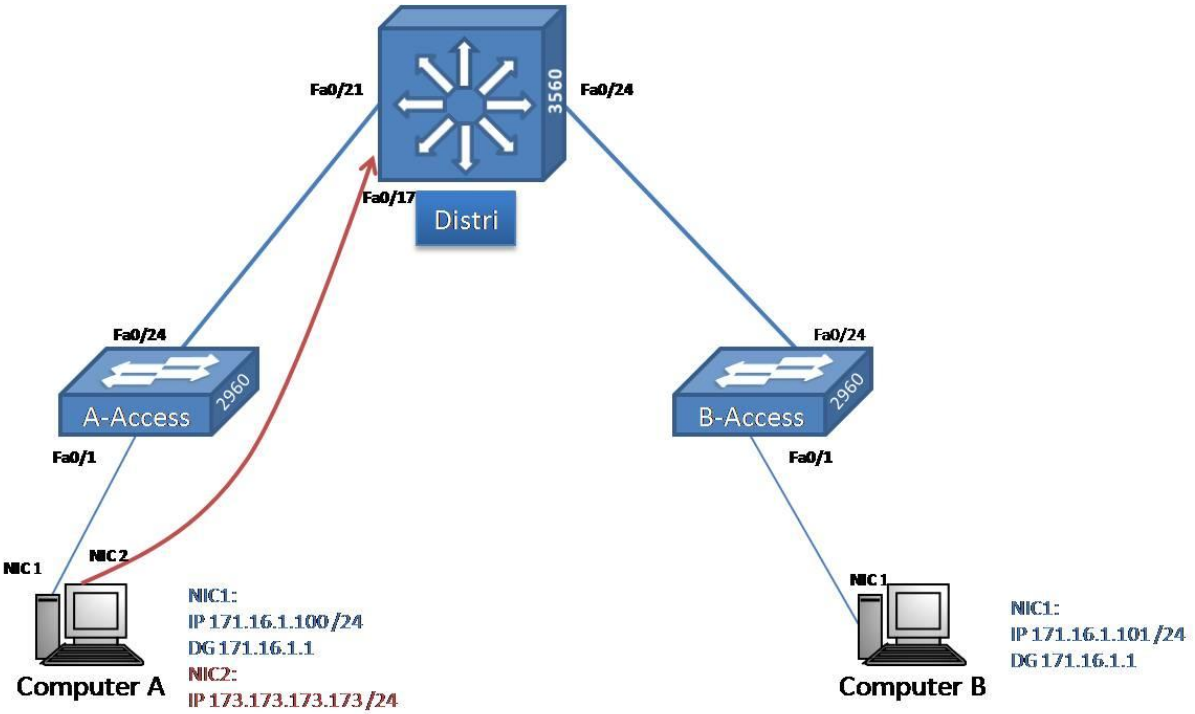
Tämä harjoitus on yksi osa kolmen harjoituksen kokonaisuudesta. Harjoituksen tarkoituksena on selvittää liikenteen luokittelua Cisco Catalyst 2960 -kytkimen avulla. Tähän on olemassa monia eri keinoja, joista harjoituksessa käydään läpi nykyisin yleisesti suositeltavan DiffServ-arkkitehtuurin määrittelemä liikenteen luokittelu.

Esivaatimukset

- ✓ 2 x Cisco Catalyst 2960
- ✓ 1 x Cisco Catalyst 3560
- ✓ 2 x PC (Windows XP)
- ✓ ohjelmat: Wireshark, www- ja ftp-siirtomahdollisuus (onnistuu XP:n avulla)
- ✓ Perus tiedot/taidot lähiverkoista ja käytettävistä laitteista

Työharjoitus jakautuu seitsemään osioon. Ensimmäinen osa tarjoaa lyhyesti teoriaa, jotta olisi mahdollista omaksua harjoitusten idea paremmin. Sen jälkeen rakennetaan kuvan 1 mukainen verkko niin, että IP-paketin olisi mahdollista kulkea verkko päästä päähän. Toimivan verkon rakentamisen jälkeen liikenne jaetaan kolmeen eri luokkaan merkitsemällä paketit toisella ja kolmannella verkkokerroksella. Lisäksi liikenteenkaappausohjelmalla todetaan, onko IP-paketit todella merkitty oikein.

HUOM! Työharjoituksessa annettavat konfigurointiohjeet ovat suuntaa antavia, eivätkä ne aina ohjeista aivan kaikkia asetuksia. Sinun on siis käytettävä omaa harkintaa laitteita konfiguroitaessa.



Kuva 1: Verkon kuva

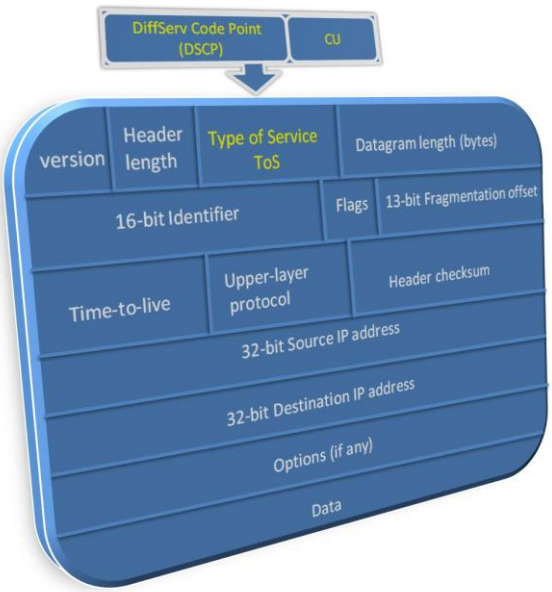
1. VAIHE - TEORIAA

Viimeistään siinä vaiheessa, kun verkossa liikkuu viiveherkkää liikennettä, kuten ääni- ja videoliikennettä, tarvitaan keinoja hallita käytettävissä olevaa kaistaa. QoS (Quality of Service) tarkoittaa palvelun laatua. Palvelun laatu voi tarkoittaa eri asioita eri tilanteissa. Reaaliaikaisessa liikenteessä se monesti kuvaa palvelun hyvää saatavuutta ja palvelun jatkuvaa ja häiriötöntä toimivuutta. QoS-toimet, joita verkkovastaavan tulisi tehdä, ovat aina tapauskohtaisia ja niitä tehdään aina verkon eri palveluiden vaatimusten mukaisesti. Palvelun laadun varmistaminen tulisi aina tehdä end-to-end ajattelutapaa käyttäen eli liikenteen kulkiessa paikasta toiseen, tulee jokaisen verkonsolmukohdan huomioida liikenteen eriarvoisuus QoS-käsittelyssä molemmat liikennesuunnat huomioiden.

DiffServ

DiffServ-arkkitehtuuri määrittelee liikenteen luokittelutavan, jolla voidaan erotella eriarvoiset liikenteet toisistaan. Sen avulla voidaan liikenne merkitä paketti paketilta. Merkintä tapahtuu jokaiseen pakettiin erikseen, ja se olisi hyvä tehdä mahdollisimman lähellä liikenteen alkupistettä. Tällöin verkon sisälaitteet voivat hyödyntää luokittelua ja samalla säästyä merkitsemisen tekemiseltä sekä siitä aiheutuvasta prosessorin kuormittumisesta. Liikenteen luokittelutapoja on tietenkin muitakin, ja osa niistä pohjautuu vuopohjaiseen liikenteen hallinnointiin.

DiffServ:in mukainen pakettien merkitseminen tapahtuu IP-kehyksessä olevaan ToS (Type of Service) -kenttään. ToS-kenttä on tavun mittainen. Ensimmäistä 6 bittiä ToS-tavussa kutsutaan DS-kentäksi ja se on varattu DSCP (Differentiated Services Code Point) -merkinnän tekemiseen. Myöhemmin sekaannuksien välttämiseksi harjoituksissa käytetään vain DSCP nimitystä. Näitä DSCP-bittejä käyttämällä on mahdollista luoda 64 eri luokkaa. Loput kaksi bittiä ovat käyttämättömiä ja varattu tulevaisuuden tarpeisiin. Kuvan 2 avulla voidaan nähdä, mihin DSCP-arvo sijoittuu IP-paketissa. Kuva 3 määrittelee IP-kehyksen kentät.



Kuva 2: IP-paketti

Kuva 3: IP-paketin kenttien merkitys

DiffServ-arkkitehtuuri on yleisesti suositeltu liikenteen luokittelumetodi, mutta sitä ennen on ollut myös muita liikenteenluokittelutapoja, kuten DiffServ:in edeltäjä IntServ (Integrated Services) sekä IP Precedence. Näistä, ja niiden yhteen liittämisestä DiffServ:in kanssa, voit lukea lisää seuraavista osoitteista:

- IntServ -> RFC 1633 www.ietf.prg/rfc/rfc1633.txt
- IP PRECEDENCE -> http://www.ietf.org/rfc/rfc1349.txt
- http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Jos halutaan säilyttää yhteensopivuus IP Precedense ja IntServ luokittelun kanssa, voidaan käyttää Ciscon laitteilla DSCP-luokkia 8,16,24,32,36,40,48,56. Nämä luokat voidaan saada suoraan toimimaan myös näiden kahden vanhemman luokitteluperiaatteen kanssa.

PHB

Luokittelun jälkeen jokaiselle luokalle määritellään PHB (Per Hop Behavior) käsittelytapa. DSCP-arvot on jaettu omiin kategorioihin, ja tietyssä kategoriassa oleva liikenne kuuluu aina tiettyyn PHB-luokkaan. PHB määrittelee minkälaisen palvelun kyseinen paketti saa verkkolaitteessa. PHB-käsittely toteutetaan koko verkossa niin, että sama käsittely toteutuu samanlaisena jokaisessa verkkolaitteessa, kun paketti matkaa verkkolaitteiden lävitse.

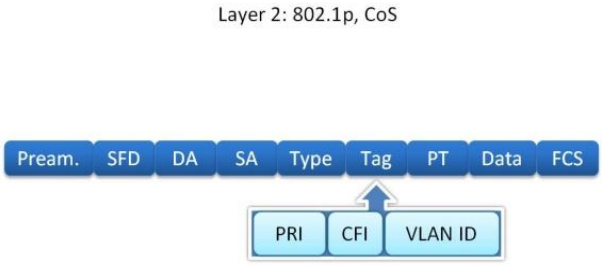
PHB-käsittelyjä on määritelty useanlaisia, mutta niistä esille nostettavia yleisesti standardoituja viitekehyksiä ovat EF (Expetited Forwarding)- ja AF (Assured Forwarding) -käsittelytavat. EF on liikenteenkäsittely tapa, jolla pyritään vähentämään verkossa esiintyvää viivettä, värinää ja pakettien putoamista, sekä se pyrkii edelleen lähettämään liikennettä niin nopeasti kuin ulostuloliitännän nopeus vain sallii. AF-käsittely puolestaan määrittelee neljä eri palveluluokkaa, joissa kussakin liikenne voi olla kolmessa eri palvelutasossa. Nämä kaksi määritelmää ovat standardeja vain käsitteidensä osalta eivätkä määrittele suoranaisesti, millä menetelmällä nämä määreet saavutetaan. DiffServ-arkkitehtuurista ja PHB-käsittelytavoista saat lisätietoa seuraavista www-osoitteista:

- Architecture for Differentiated Service RFC 2475 http://www.ietf.org/rfc/rfc2475.txt
- Definition of the Differentiated Services Field (DS field) in the Ipv4 and Ipv6 headers http://www.ietf.org/rfc/rfc2474.txt
- EF PHB http://www.ietf.org/rfc/rfc2598.txt
- AF PHB http://www.ietf.org/rfc/rfc2597

CoS

Luokittelua voidaan toki tehdä myös verkon toisella kerroksella, mutta tällöin tulee huomioida, että liikenteen siirtyessä esimerkiksi ethernet-verkosta ATM-verkkoon ei ethernet-kehyksen luokittelua ole enää olemassa ATM-verkossa. IP-pakettiin tehdyt luokittelumerkinnät puolestaan säilyvät koko verkon läpi. 2-kerroksen luokittelua voidaan kuitenkin hyväksikäyttää joissakin tilanteissa, silloin kun esimerkiksi laitteet eivät pysty hyödyntämään IP-paketin luokittelua. Huomattavaa on, että Catalyst 2950 -kytkin ei tue DSCP-merkintöihin pohjautuvaa jonotuskäsittelyä, mutta Catalyst 2960 -kytkin pystyy jo hyödyntämään sitä. Catalyst 2950 -kytkimiä käytettäessä luokittelu on toteutettava CoS (Class of Service) -bittien avulla, jos halutaan käyttää laitteen QoS-ominaisuuksia.

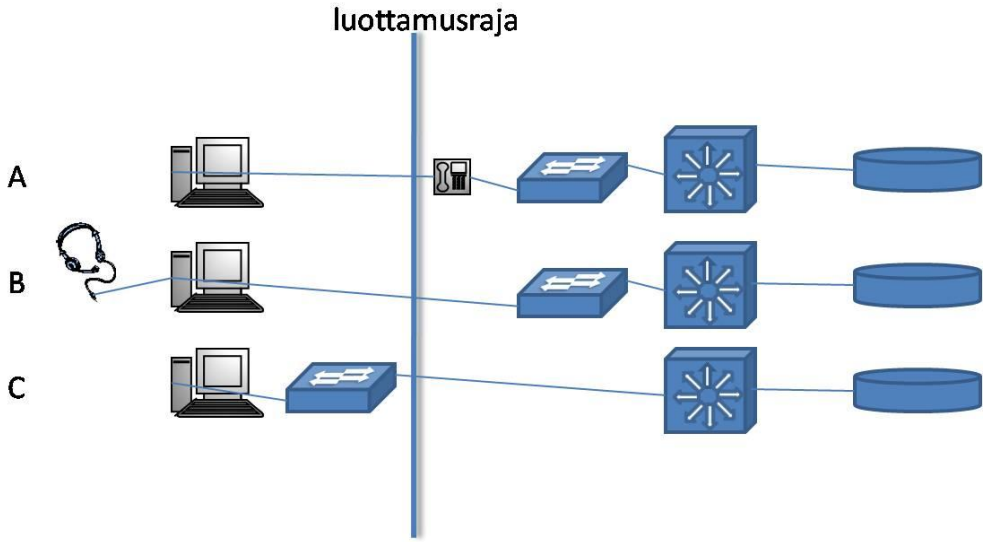
Ethernet-kehyksessä on paikka nimeltä CoS (Class of Service), joka koostuu 3 bitistä. Näitä bittejä yhdistelemällä on mahdollista saavuttaa kahdeksan eri palveluluokkaa. CoS-kenttä sijaitsee 802.1p/Q-kehyksen VLAN-kentässä, joten verkon liikenteen täytyy kulkea jossakin VLAN:ssa, jotta sitä voidaan yleensäkin luokitella. Natiivi VLAN kuljetetaan oletuksena ilman VLAN-tagia, joten siinä kulkevalla liikenteellä ei ole kehyksessä paikkaa luokittelumerkinnälle. CoS-tavun sijainti ethernet-kehyksessä näkyy kuvassa 4 osoitetun tag-kentän (lippu-kenttä) PRI-osassa (PRI = priority).



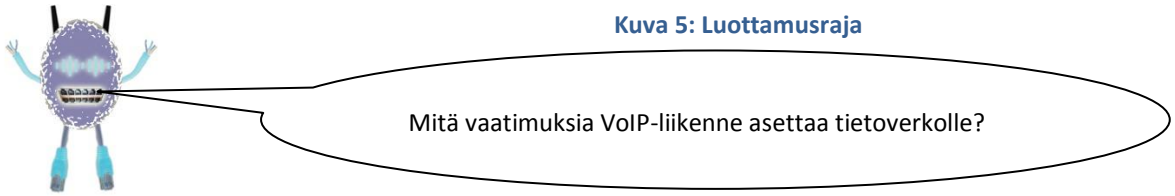
Kuva 4: CoS-bittien sijainti ethernet-kehyksessä

Luottamusraja

Luottamusraja on kuvitteellinen raja verkon reunalla, joka määrittelee, minkä verkkolaitteen jälkeen IP-paketeissa oleva luokittelu on hyväksyttävää. Kuva 5 havainnollistaa luottamusrajaa ja sen toimintaa. Kaikki laitteet viivan oikealla puolella ovat luotettuja laitteita, ja viivan vasemmalla puolella on kaikki ei luotetut laitteet. Ei-luotetut laitteet ovat yleensä kykenemättömiä luokittelemaan oikealla tavalla liikennettä. Toisin sanoen, kun paketti saapuu luottamusrajalta luotetulle laitteelle, paketin luokitteluun ei luoteta. Paketin täytyy tulla luottamusrajan sisältä, jotta paketin luokitteluun voidaan luottaa. Harjoitustehtävässä on tilanteen B kaltainen tilanne.



Kuva 5: Luottamusraja



2. VAIHE – VERKON RAKENNUS

Verkkolaitteiden tarvitsemat asetukset löytyvät alla olevasta taulukosta. Taulukon ja ohjeiden avulla verkon rakentaminen pitäisi onnistua. Aloita kuitenkin verkon kaapeloinnilla (kuva 1).

	Computer A *NIC 1*	*Computer A* *NIC 2*	*Computer B* *NIC 1*
IP-osoite	171.16.1.100	173.173.173.173	171.16.1.101
aliverkon peite	255.255.255.0	255.255.255.0	255.255.255.0
oletusyhdyskäytävä	171.16.1.1	-	171.16.1.1

A-Access-kytkin (Catalyst 2960)

- Anna nimeksi A-Access
- Luo virtuaalinen vlan 100 -liitäntä ja anna sille IP-osoite 171.16.0.2 255.255.255.0
- Aseta oletusyhdyskäytäväksi osoite 171.16.0.1
- Access-port asetukset:
    - liitännät 1 – 16 liitetään vlan 110
- Trunk-port asetukset:
    - kapselointi dot1q
    - ei neuvottelua trunk-linkistä (nonegotiate)
    - native vlan 1

B-Access-kytkin (Catalyst 2960)

- Anna nimeksi B-Access
- Luo virtuaalinen vlan 100 -liitäntä ja anna sille IP-osoite 171.16.0.3 255.255.255.0
- Aseta oletusyhdyskäytäväksi osoite 171.16.0.1
- Access-port asetukset:
    - liitännät 1 – 16 liitetään vlan 110
- Trunk-port asetukset:
    - kapselointi dot1q
    - ei neuvottelua trunk linkistä (nonegotiate)
    - native vlan 1

Distri-kytkin (Catalyst 3560)

- Anna nimeksi Distri
- Luo virtuaalinen vlan 100 -liitäntä, määrittele sen IP-osoitteeksi 171.16.0.1 ja aliverkoksi 255.255.255.0
- Aktivoi reititys
- Luo vlan 110 ja anna sille IP-osoite 171.16.1.1 255.255.255.0
- Trunk-port asetukset liitäntöihin:
    - kapselointi dot1q
    - ei neuvottelua trunk-linkissä (nonegotiate)
    - native vlan 1

Testaa verkon toiminta lähettämällä ping-paketteja Computer A:lta Computer B:lle. Verkon toimiessa voit jatkaa eteenpäin. Suositeltavaa olisi ottaa tässä vaiheessa konfiguraatio-asetukset talteen, koska niistä saattaa olla apua myöhemmissä harjoitustehtävissä.

Tarkistuslista:

- Onko liitännät nostettu ylös?
- Onko kapselointi oikein kaikissa yhteyksissä?
- Ovatko IP-osoitteet varmasti oikein?
- Näkyykö VLAN-taulukossa kaikki tarvittavat VLAN:t?

3. VAIHE – LIIKENTEEN LUOKITTELU DSCP:N AVULLA

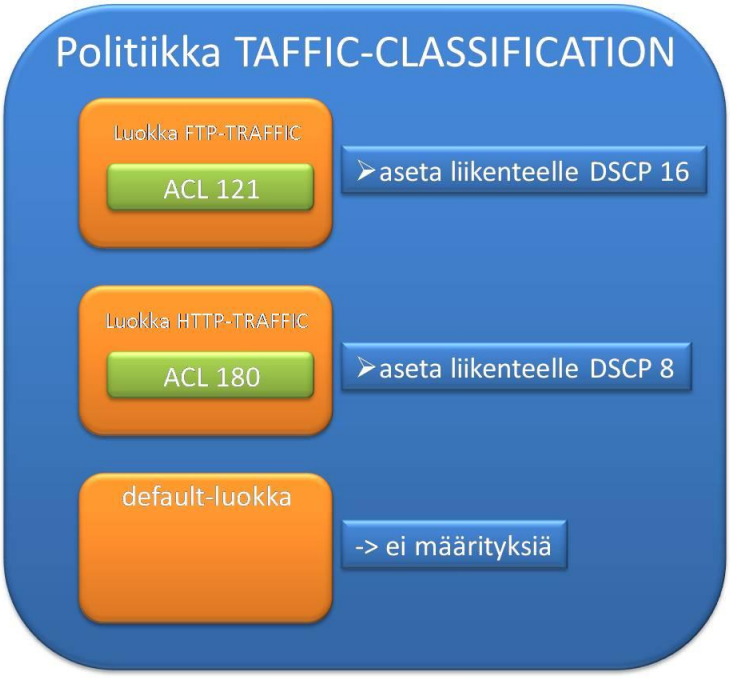
Liikenteen luokittelu tapahtuu selkeimmällä tavalla silloin, kun käytetään vain yhtä merkitsemistapaa. Aina tämä ei kuitenkaan ole mahdollista. Liikenteen luokitteluun DSCP-kentän hyödyntäminen sopii hyvin siksi, että se säilyy ja on käytettävissä IP-verkossa liikenteen kulkiessa verkon päästä päähän.

DiffServ:in mukainen liikenteenluokittelu luottaa IP-paketin DSCP-kenttään tehtyihin merkintöihin. Suositusten mukaan liikenteen luokittelun tulisi tapahtua mahdollisimman lähellä liikenteen alkupistettä, joten seuraavaksi luokittelemme liikennettä 2960-kytkimen avulla. Vaikka Ciscon Catalyst 2960 -sarjan kytkimet ovatkin toisen verkkokerroksen laitteita, ne kykenevät merkitsemään ja lukemaan IP-paketissa olevaa ToS-kenttää. Tämän vuoksi seuraavaksi harjoittelemme DSCP-merkinnän asettamista. Mikäli käytössä olisi Ciscon IP-puhelin, voitaisiin luokittelu toteuttaa sen avulla.

Liikennettä luokitellaan kolmeen luokkaan niin, että http- ja ftp-liikenne luokitellaan arvokkaampaan luokkaan kuin muu liikenne. Ftp-liikenne luokitellaan luokkaan 16, http-liikenne luokkaan 8 ja kaikki muu liikenne saa jäädä oletusluokkaan eli luokkaan 0.

Luokittelu tapahtuu luomalla ensin luokkia (class-map). Luokkiin poimitaan haluttu liikenne joko ACL:n, DSCP-merkinnän tai CoS-merkinnän avulla. Luokittelua tehtäessä poiminta tapahtuu normaalisti ACL:n avulla. Liikennepolitiikassa (policy-map) kootaan yhteen aiemmin luodut luokat ja määritellään luokkien liikenteille luokkamerkinnät eli DSCP-arvot. Lopuksi liikennepolitiikka liitetään haluttuun porttiin sisäänpäin kohdistuvaan liikenteeseen.

Seuraavaksi esitellään komennot, joiden avulla luodaan politiikka nimeltä TRAFFIC-CLASSIFICATION. Sen sisälle luodaan kaksi luokkaa, jotka ovat nimeltään FTP-TRAFFIC ja HTTP-TRAFFIC. Luokkaan FTP-TRAFFIC sidotaan ACL 121 määrittelemä liikenne. Luokka itsessään asettaa siihen kuuluvalle liikenteelle DSCP-arvon 16. Luokkaan HTTP-TRAFFIC puolestaan sidotaan ACL 180 mukainen liikenne ja luokan liikenteelle märitetään DSCP-arvo 8. Kun politiikka, siinä olevat luokat, luokkien määritykset ja ACL:t ovat valmiita, asetetaan luokka sisääntuloliitäntään aktiiviseksi. Voit yrittää hahmottaa luokittelua kuvan 6 avulla.



Kuva 6: Liikennepolitiikan rakenne

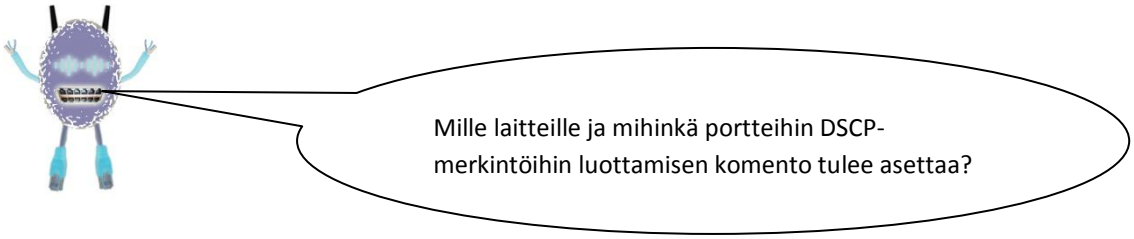
Itse liikenteen luokittelu tapahtuu seuraavien komentojen avulla molemmissa access-tason kytkimissä. Tee komennot.

komennot	**selitys**
(config)# mls qos	*liikenteen hallinnan aktivointi*
(config)# access-list 121 permit tcp any any eq ftp	*mikä tahansa ftp-liikenne mihin tahansa suunta*
(config)# access-list 121 permit tcp any any eq ftp-data	*sama ftp-data liikenteelle*
(config)# access-list 180 permit tcp any any eq www	*mikä tahansa http-liikenne mihin tahansa suuntaan*
(config)# class-map FTP-TRAFFIC	*luo luokan FTP-TRAFFIC*
(config-cmap)# match access-group 121	*liittää luokkaan ACL 121:n määrittelemän liikenteen*
(config)# class-map HTTP-TRAFFIC	*luo luokan HTTP-TRAFFIC*
(config-cmap)# match access-group 180	*liittää luokkaan ACL 180:n mukaisen liikenteen*
(config)# policy-map TRAFFIC-CLASSIFICATION	*luodaan liikennepolitiikka*
(config-pmap)# class FTP-TRAFFIC	*liittää luokan FTP-TRAFFIC politiikkaan*
(config-pmap-c)# set dscp 16	*asettaa luokan liikenteelle DSCP-arvon 16*
(config-pmap)# class HTTP-TRAFFIC	*liittää luokan HTTP-TRAFFIC politiikkaan*
(config-pmap-c)# set dscp 8	*asettaa luokan liikenteelle DSCP-arvon 8*
(config)# int range fa0/1 - 16	
(config-if-range)# service-policy input TRAFFIC-CLASSIFICATION	*asettaa politiikan TRAFFIC-CLASSIFICATION aktiiviseksi liitännästä sisään tulevalle liikenteelle*

Voit varmistaa asetuksien oikeellisuuden show komennoilla:
#show policy-map TRAFFIC-CLASSIFICATION
#show class-map FTP-TRAFFIC
#show access-list 121

Liikenne luokitellaan heti access-tasolla, jolloin distribution-tasolle tarvitsee asettaa ainoastaan luottosuhde näihin merkintöihin. Luottosuhde täytyy myös asettaa kaikille verkkolaitteille, joiden läpi liikenne kulkee matkatessaan määränpäähänsä. Mieti, millä laitteella ja missä liitännöissä pakettien luokittelumerkintöihin täytyisi luottaa. Tee tämän jälkeen luottosuhde seuraavalla komennolla valitsemiisi liitäntöihin:

(config-if)# mls qos trust dscp	*luotetaan porttiin saapuvan liikenteen DSCP-merkintöihin*



Nyt liikenne luokitellaan ja merkitään IP-kehyksen ToS-kenttään käyttäen hyväksi DSCP-merkintätapaa. Kun merkintä on kerran tehty pakettiin, siihen luotetaan jokaisella laitteella tämän jälkeen.

4. VAIHE – DSCP-LUOKITTELUN TODENNUS

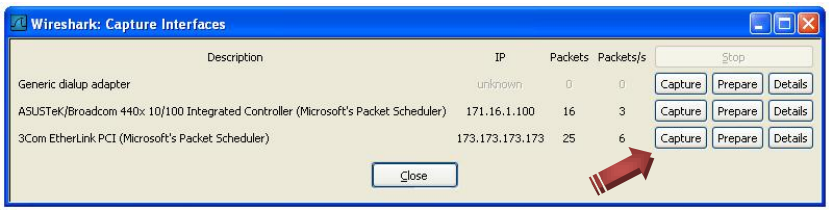
Liikenne on saatu verkossa kulkemaan ja liikenne myös luokitellaan eri luokkiin. Vai luokitellaanko? Nyt tarkastelemme hieman lähemmin IP-pakettien luokittelubittejä ja sitä, ovatko ne todella muuttuneet oletusarvosta määrätynlaisiksi. Tähän tarvitsemme liikenteenkaappausohjelman. Ilmainen ja hyvin monipuolinen liikenteenkaappausohjelma Wireshark:in voi noutaa osoitteesta http://www.wireshark.org/. Asennettuasi ohjelman tee seuraavat toimenpiteet:

- Aseta Computer A NIC 2:en verkkokortin IP-osoitteeksi 173.173.173.173 ja aliverkoksi 255.255.255.0.
- Aseta Computer B:lle IIS-toiminto päälle, jos se ei ole jo päällä. Löydät sen polusta Control Panel -> Add or Remove Programs -> Add/Remove Windows Components ->Internet Information Services (IIS) [valitse tämä] ->Details… -> Internet Information Services Snap-In [täppä] World Wide Web Services [täppä] File TransferProtocol (FTP) Service [täppä]-> OK, Next, Finish
- Luo kooltaan suuri tiedosto ja siirrä se kansioon c:\Inetpub\ftproot\
- Ennen liikenteenkaappausohjelman käynnistämistä tarvitsee Distri-kytkimeen ajaa muutama komento. Niiden päämäärä on peilata SPAN:in avulla portin Fa0/21 liikenne porttiin Fa0/17. Toiseen päähän porttia Fa/17 asetetaan Computer A kuuntelemaan liikenteenkaappausohjelman avulla siihen peilattua liikennettä.

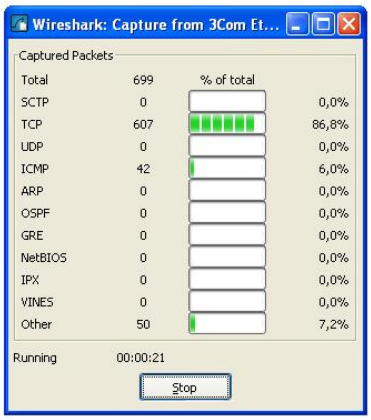
```
Distri(config)# monitor session 1 source interface Fa0/21
Distri(config)# monitor session 1 destination interface Fa0/17 encapsulation replicate
```

Ensimmäisellä komennolla määritellään SPAN session tunnistenumeroksi 1 ja kuunneltavaksi portiksi Fa0/21. Jälkimmäinen komento määrittelee, että peilattava liikenne lähetetään porttiin Fa0/17. Encapsulation replicate-komennon lopussa varmistaa, että myös pakettien 2-verkkokerroksen kapselointi peilataan alkuperäisenä.

- Käynnistä Wireshark
- Wiresharkin käynnistämisen jälkeen valitaan ikkunan yläosan valikosta Capture -> Interfaces. Kuvan 7 mukaisesta näkymästä voidaan Capture-valinnalla valita ja aloittaa halutun liitännän liikenteenkaappaus. Valitse se liitäntä, johon olet asettanut 173.173.173.173 IP-osoitteen. Kts. kuva 7

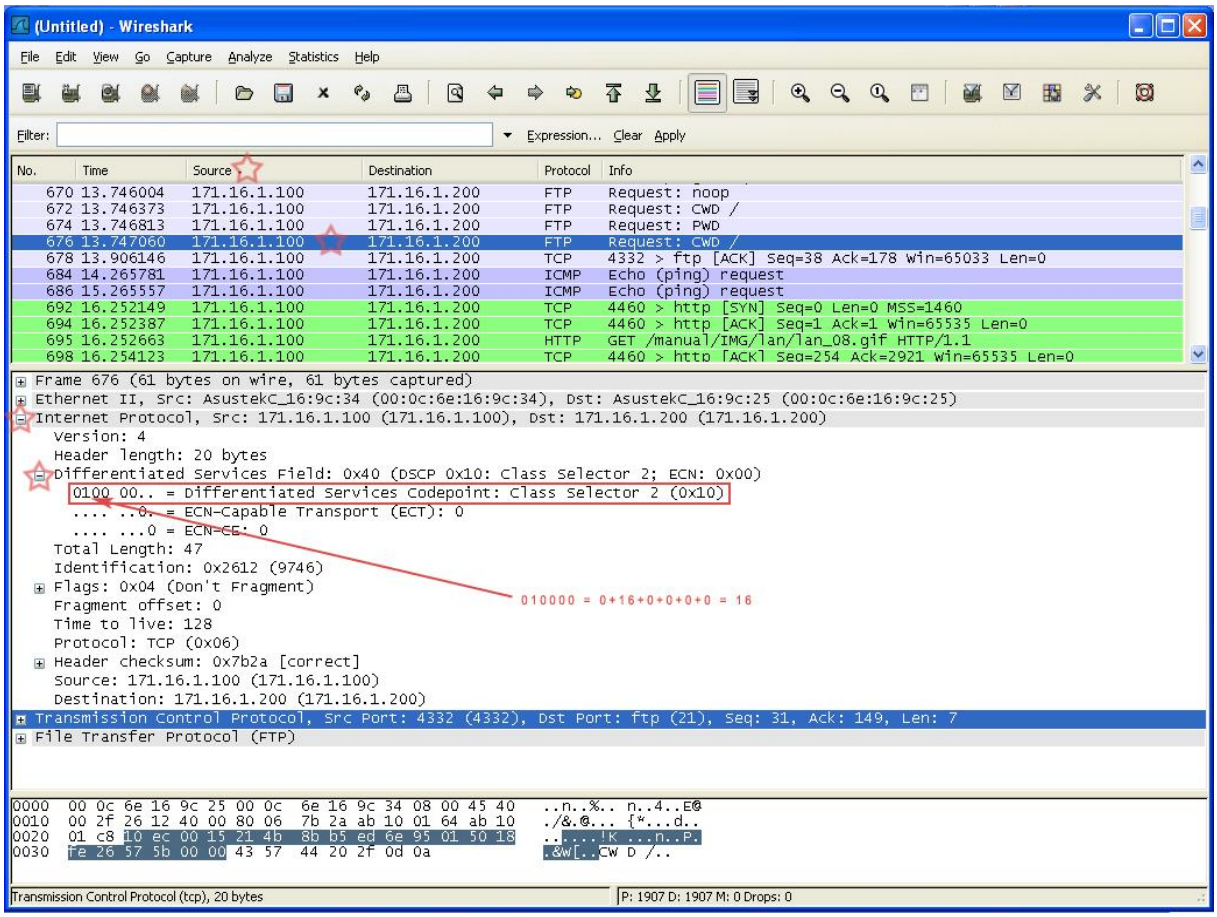


Kuva 7: Wireshark – Liitännän valitseminen



Kuva 8: Wireshark – Kaapattujen tiedostojen näkymä

Liikenteen kaappaus alkaa, ja kuvan 8 mukainen ikkuna ilmestyy ruudulle. Se kertoo mitä eri paketteja valitsemastasi verkkokortinliitännästä saapuu kaappausohjelmalle. Other-kohta kasvaa luultavasti koko ajan, koska itse verkkolaitteet lähettävät koko ajan omaa liikennettään. Lähetä nyt Computer A:lta ping-pyyntö Computer B:lle, ja ota selaimella http- ja ftp-yhteys Computer B:hen. Siirrä lisäksi luomasi tiedosto Computer B:ltä Computer A:lle. Nyt voit huomata, kuinka TCP-sarake alkaa kohota Wiresharkin-ikkunassa. Paina Stop-nappia pysäyttääksesi kaappauksen.



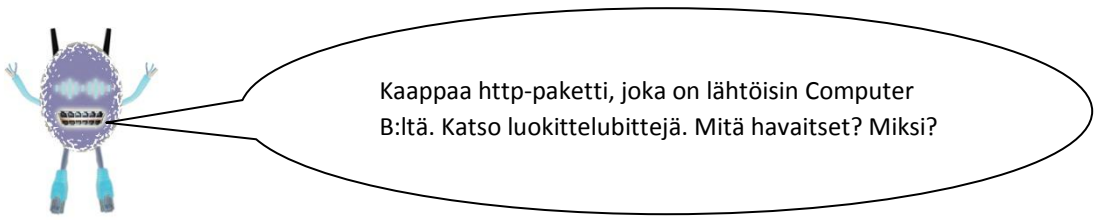
Kuva 9: Wireshark – Kaapatun liikenteen näkymä

Eteesi aukeaa kuvan 9 mukainen näkymä. Ylemmässä näkymässä on kuvattu kaikki kaapatut paketit, ja alemmassa näkymässä on nähtävillä kulloinkin valittuna olevan paketin sisältö. Painamalla ylemmän näkymän ylälaidassa olevaa Source-nappia järjestyy paketit lähdeosoitteen mukaiseen järjestykseen. Valitse luettelosta yksi ftp request -paketti, joka on lähtöisin computer A:lta. Avaa alemmassa näkymässä sijaitsevia tietokenttiä kuvan 9 mukaisesti. Näkyviisi avautuu kuvaan punaisella merkitty kenttä, joka määrittelee DSCP-bitit. Siitä voidaan huomata, että pakettiin on merkitty DSCP-arvoksi 16. Bittejä on kuusi kappaletta, kuten aiemmin on mainittu. Bittien avulla muodostetaan eri luokat. Kun DSCP-bittejä halutaan muuttaa desimaalimuotoon, onnistuu se helposti laskemalla yhteen binäärilukuja vastaavat desimaaliarvot yhteen. Vasemmalta oikealle luettuna binääri-arvojen vastineet ovat 32, 16, 8, 4, 2 ja 1. Jokainen bitti, joka on ykkönen, tulee mukaan laskuihin. Tässä tapauksessa ykkösenä on ainoastaan toinen bitti, joten laskukaavassa on yhteenlaskettavana vain luku 16. DSCP-arvo on siis 16. Avaa myös yksi http-paketti ja varmista, että sen DSCP-kentän arvo on 8. Jos puolestaan avaat ICMP paketin, voit huomata, että DSCP-arvo on oletusarvossaan eli kaikki bitit osoittavat nollaa. Alapuolella olevasta taulukosta voidaan nähdä suositellut PHB-käsittelytavat eri luokille ja bittien sijoittuminen eri DSCP-luokkiin.

HUOM! Windowsin ftp-palvelin tekee yhteysneuvottelut portissa 21, mutta itse data siirtyy jossakin muussa portissa kuin 20. Tästä johtuen harjoituksessa voitaisiin käyttää jotakin muuta ftp-palvelinta, joka käyttää näitä standardeja porttinumeroita.

PHB käsittely	DSCP luokka	DSCP-arvo	bitit	määrittely
EF	EF	46	101110	RFC 3246
AF1	AF11 AF12 AF13	10 12 14	001010 001100 001110	RFC 2597
AF2	AF21 AF22 AF23	18 20 22	010010 010100 010110	RFC 2597
AF3	AF31 AF32 AF33	26 28 30	011010 011100 011110	RFC 2597
AF4	AF41 AF42 AF43	34 36 38	100010 100100 100110	RFC 2597
IP routing	Class 6	48	110000	RFC 2474
Streaming video	Class Selector 4	32	100000	RFC 2474
Telephony signaling	Class Selector 3	24	011000	RFC 2474
Network Management	Class Selector 2	16	010000	RFC 2474
Scavenger	Class Selector 1	8	001000	Internet 2 käyttöä varten

Hienoa! Liikenne on onnistuneesti luokiteltu ja luokittelutieto siirtyy verkossa eteenpäin.



5. VAIHE – LIIKENTEEN LUOKITTELU COS:N AVULLA

Liikennettä voidaan merkitä myös OSI:n 2-kerroksella ethernet-kehyksessä sijaitsevaan CoS-kenttään. Tällöin luokittelu on voimassa ainoastaan silloin, kun liikenne matkustaa ethernet-verkossa. Heti paketin matkatessa pois sieltä häviää ethernet-kehykset ja samalla niissä esiintyvä luokittelu. On myös huomattava, että nykyisillä Ciscon 2900 -sarjan Catalyst-kytkimillä on ainoastaan yksi merkitsemistapa, jolla Co- arvo saadaan käytännössä asetettua. Se onnistuu vain porttikohtaisesti ja tällöin myös eriarvoiseksi luokiteltava liikenne täytyy tulla eri porteista. Tämä puolestaan johtuu siitä, että kytkimet eivät pysty käyttämään ACL:iä apunaan CoS-merkintöjä tehdessään. CoS-merkintöjä pystytään hyödyntämään lähinnä Ciscon omien IP-puhelimien avulla ja tällöinkin hyvin rajoittuneesti.

Seuraavaksi poistamme DSCP-lukuihin perustuvan luokittelun ja luokittelemme liikennettä CoS-arvojen avulla. Poista DSCP-arvoihin perustuva luokittelu seuraavilla komennoilla:

```
A/B-access(config)# no access-list 121
A/B-access(config)# no access-list 180
A/B-access(config)# no policy-map TAFFIC-CLASSIFICATION
A/B-access(config)# no class-map FTP-TRAFFIC
A/B-access(config)# no class-map HTTP-TRAFFIC
Distri(config-if)# no mls qos trust dscp
```

CoS-arvon merkitseminen molemmilla access-kytkimillä:

```
(config)# int range fa0/1 – 8
(config-if-range)# mls qos cos 1          määrittelee sisään tulevalle liikenteelle default-CoS -arvoksi 1

(config-if-range)# mls qos cos override   pakottaa CoS-arvon asettamisen
(config)# int range fa0/9 - 16
(config-if-range)# mls qos cos 2
(config-if-range)# mls qos cos override
```

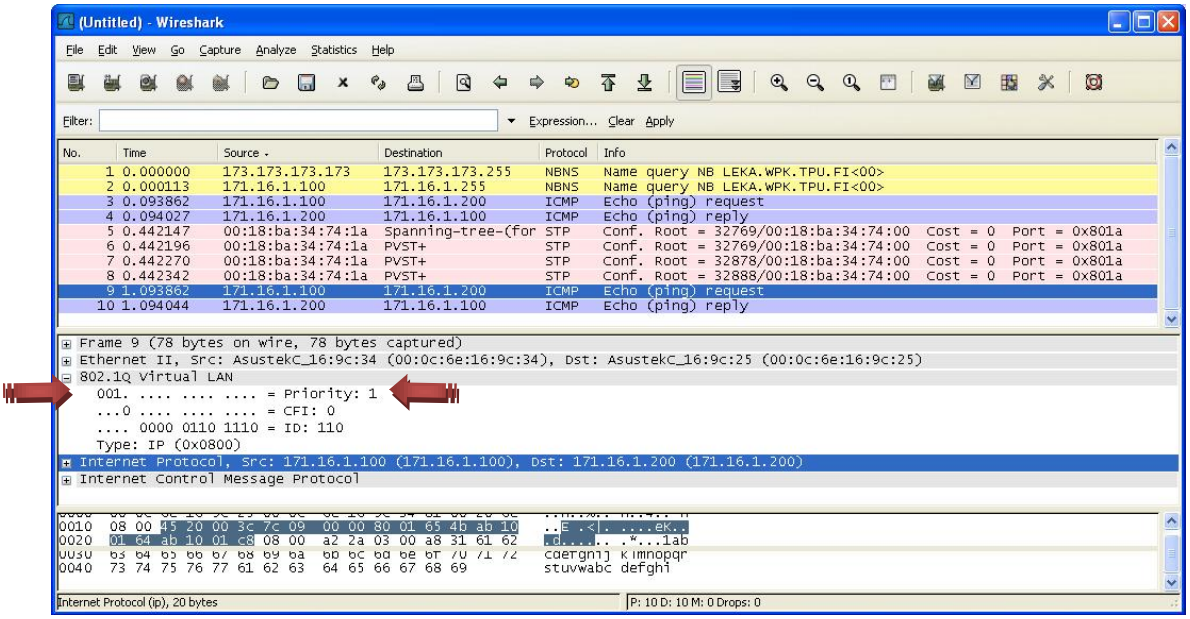
Luotetaan saapuvan liikenteen CoS-merkintöihin:

```
(config-if)# mls qos trust cos
```

6. VAIHE – COS-LUOKITTELUN TODENNUS

Liikenne on saatu verkossa kulkemaan ja liikenne myös luokitellaan eri luokkiin. Nyt tarkastelemme hieman lähemmin ethernet-kehyksen luokittelubittejä.

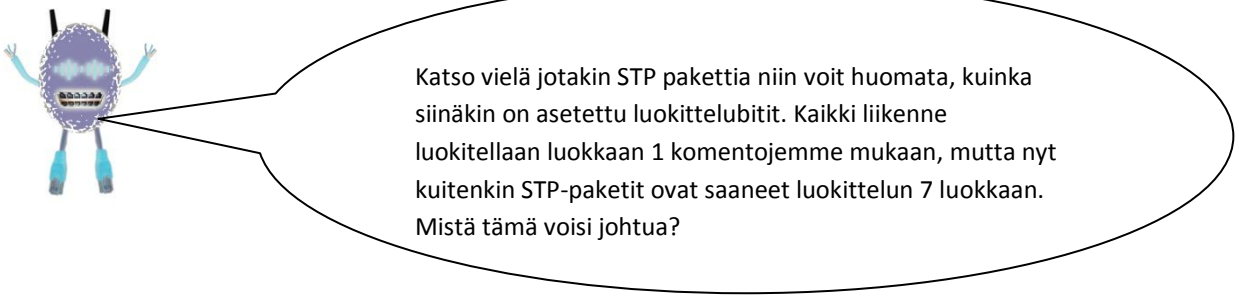
Kaappaa liikennettä vaiheessa neljä esitetyllä tavalla. Generoi liikennettä valitsemallasi tavalla. Valitse jälleen luettelosta yksi paketti. Tarkastele tämän sisältöä hieman tarkemmin avaamalla sen sisältö näkyviin. Kuva 10 osoittaa, missä CoS-luokittelubitit sijaitsevat ja mikä niiden arvo tulisi olla.



Kuva 10: CoS-bittien sijainti ethernet-kehyksessä

Alapuolella olevasta taulukosta voidaan nähdä eri arvoja, mitä CoS-kentässä voisi olla, ja mihinkä luokkaan oletuksena tällöin liikenne kuuluisi.

Luokka	bitit	tyypillinen sovellus
7	111	varattu
6	110	varattu
5	101	äänidata
4	100	videoneuvottelu
3	011	äänensignalointi
2	010	tärkeä dataliikenne
1	001	keskitasoinen dataliikenne
0	000	Best Effort



Jos ihmettelet, miksi paketteihin, joihin asetetaan CoS-arvo, ilmestyy myös DSCP-merkintä, niin sen kuuluukin ilmestyä. 2960-kytkimellä on ominaisuus, jonka myötä paketteihin tehdään automaattisesti myös IP-pakettiin DSCP-merkintä. Tällä pyritään luultavasti varmistamaan, että paketissa säilyy luokitteluarvo, vaikka se matkaisi pois ethernetistä. DSCP-arvo muodostuu kytkimen sisäisen CoS-to-DSCP map -liitoksen avulla. Tätä muutoskarttaa on mahdollista muokata tarpeiden mukaan.

Tarkistuslista, jos 802.1p/Q-tietoa ei näy paketissa:

- Verkkokortissa ei saa olla 802.1p-tuki aktiivisena. Katso polusta Control Panel -> Network Connections -> Local Area Connection [hiiren oikea] -> Properties ->General ->Configure -> Advanced -> 802.1p Support -> Disabled (3Com-verkkokorteissa)
- Muistithan käyttää SPAN:ia konfiguroidessasi asetusta encapsulation replicate
- Liikenne, jota kaappaat, ei saa kulkea native VLAN:ssa, koska silloin VLAN-kentän puuttuessa kehyksessä ei ole paikkaa, johon luokittelu merkinnän voisi tehdä.

Lisätehtävä

Vaihda Computer A ja Computer B kytkimen portista Fa0/1 porttiin Fa0/18 ja muuta niiden IP-osoitteet toiseen aliverkkoon. Katso Wiresharkilla luokittelubittejä.

A)

B)

7. LOPUKSI

Olet nyt oppinut, kuinka DiffServ-arkkitehtuurin mukaisesti liikennettä luokitellaan IP-paketin ToS-kenttään. Lisäksi tilanteisiin, joissa DSCP-merkintöjä ei voida käyttää, opit keinon, jolla merkintä tehdään ethernet-kehyksen CoS-kenttään. Näiden kahden käsitteen erottaminen toisistaan on hyvin tärkeää.

Liikenteenluokittelutapoja on monia, ja niistä sopivimman valitseminen on aina tehtävä käytettävissä olevien laitteiden ehdoilla. Tässä harjoituksessa käytettiin ohjelmallisia IP-puhelimia. Jos käytössä olisi ollut Ciscon omat IP-puhelimet, tapahtuisi luokittelu suoraan niiden avulla. Normaali tilanteessa Ciscon IP-puhelimeen kytketään tietokone kiinni ja pakettien matkatessa IP-puhelimen läpi se luokittelisi paketit CoS- ja DSCP-arvoilla.

Mikäli tarvitset lisätietoa muista liikenteenluokittelutavoista, lue lisää aiheesta:

- Vegesna, Srinivas. 2001. IP Quality of Service. USA: Cisco Press.
- Szigeti, Tim. 2005. End-to-End Qos Network Design: Quality of Service in LANs, WANs, and VPNs. USA: Cisco Press.

Jos jatkat seuraavan harjoitustehtävään, tee seuraavat toimenpiteet poistaaksesi ylimääräiset komennot kytkimiltä:

Molemmilla Access-kytkimillä:

```
A/B-access(config) no mls qos
A/B-access(config)# int range fa0/1 - 16
A/B-access(config-if-range)# no mls qos cos
A/B-access(config-if-range)# no mls qos cos override
```

Distri-kytkimellä:

```
Distri(config-if)# no mls qos
Distri(config-if)# no mls qos trust cos
```

TYÖHARJOITUS 2 – VOIP-LIIKENTEEN PRIORISOINTI ETHERNETISSÄ

Tämä harjoitus on toinen osa kolmen harjoituksen kokonaisuudesta. Harjoituksen tarkoituksena on jälleen luokitella liikennettä DiffServ-arkkitehtuurin mukaisesti. Tämän jälkeen liikenteen luokittelua hyödynnetään ruuhkankäsittelyssä ja ruuhkien ennaltaehkäisyssä. Työharjoitus 2 voidaan tehdä suoraan työharjoituksen 1 perään. Jos tämän harjoituksen tekeminen aloitetaan suoraan, on työharjoitus 1:stä tehtävä kohta 2. Harjoitus olettaa, että sitä tekevällä on omaksuttuna teoriataidot liikenteenluokittelusta ja liikenteenhallinnasta. Työn tarkoitus on liittää nämä tiedot käytännön harjoitteeseen.

Esivaatimukset

- ✓ 2 x Cisco Catalyst 2960
- ✓ 1 x Cisco Catalyst 3560
- ✓ 4 x PC (Windows XP)
- ✓ 2 x kuulokemikrofoni
- ✓ Perus tiedot/taidot lähiverkoista ja käytettävistä laitteista
- ✓ Ohjelmat: VLC media server ja Express Talk
- ✓ DiffServ-arkkitehtuurin ymmärtäminen
- ✓ Ciscon laitteiden avulla liikenteen luokitteluun vaadittavat komentorivikomennot
- ✓ Työharjoitus 1:en vaihe 2 suoritettuna

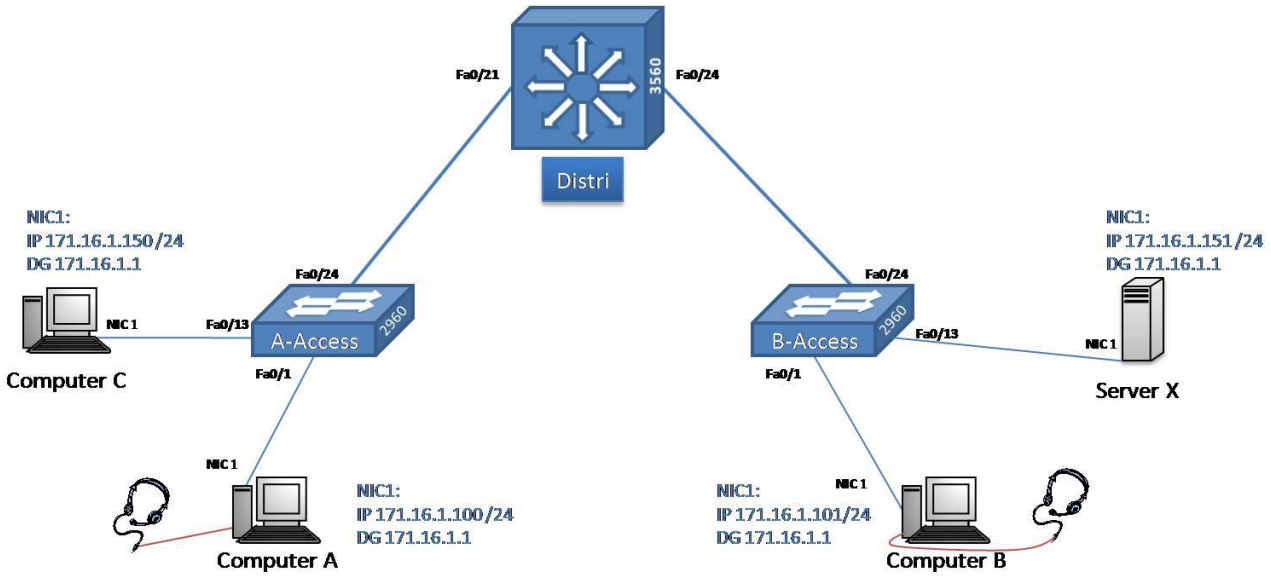
Harjoitus jakaantuu viiteen osioon. Ensimmäisessä osassa asennetaan Softphone-sovellus kahdelle tietokoneelle. Tämän sovelluksen avulla soitetaan puhelu verkon ylitse ja testataan IP-puhelun laatua. Toisessa osiossa verkko ruuhkautetaan videostreamauksen avulla. Uusi IP-puhelu soitetaan ja huomataan verkon ruuhkatilanteen vaikutus IP-puhelun laatuun. Kolmas osio on liikenteen luokittelun suunnittelua ja toteutusta harjoitusympäristöön. Neljäs osa jakaantuu A- ja B-osioon. A-osassa keskitytään QoS-toimiin Catalyst 2960 ja 3560 -kytkinten osalta sisääntuloportissa ja B-osassa samojen laitteiden ulostuloportissa. Osiot esittelevät teoreettiselta näkökannalta laitteiden QoS-ominaisuudet ja ohjaa sopivien asetuksien asettamiseen. QoS-toimissa käydään läpi välimuistin allokointia ja SRR (Shaped/Shared round-robin)- ja WTD (Weighted Tail Drop) -algoritmien toimintaa. Konfiguraatioasetusten jälkeen soitetaan uusi IP-puhelu verkonruuhkahuipulla ja yritetään huomata toimien äänenlaadulliset vaikutukset. Viimeinen osio kokoaa opitut asiat yhteen ja pohjustaa verkon seuraavaa harjoitusta varten.

Sisältö:

Muutoksia alku konfiguraatioon:

- Pudota molempien access-kytkinten ja distri-kytkimen välisten yhteyksien nopeus 10 Mbps
- Aseta nämä linkit toimimaan myös half-duplex-tilassa

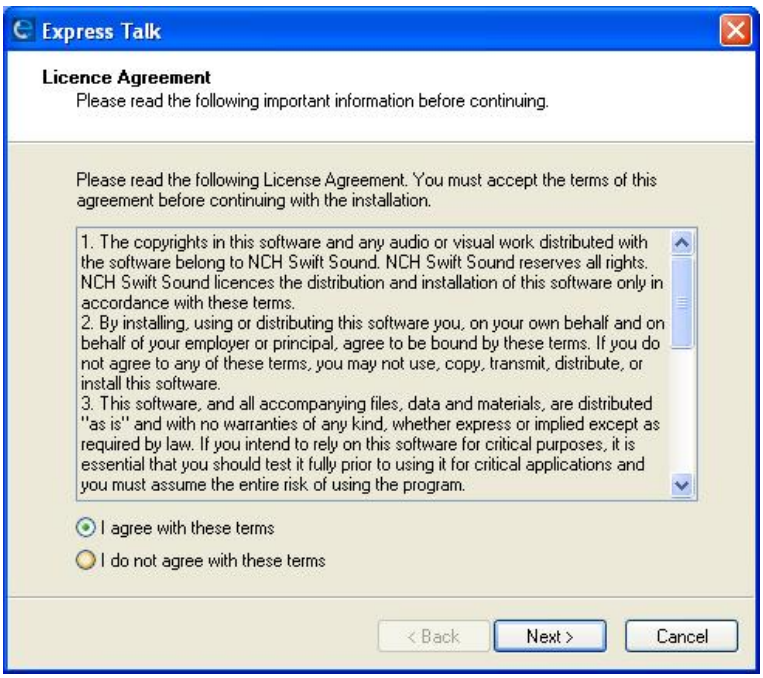
Voit helpottaa harjoituksen tekemistä noutamalla etukäteen tarvittavat työtiedostot osoitteesta https://www.wpk.tpu.fi/A4121_CCNP/tavaraa/ccnp3/. Tiedostot ovat yhdessä ZIP-tiedostossa. Pura tiedostot jokaiselle tietokoneelle.



Kuva 1: Verkon kuva

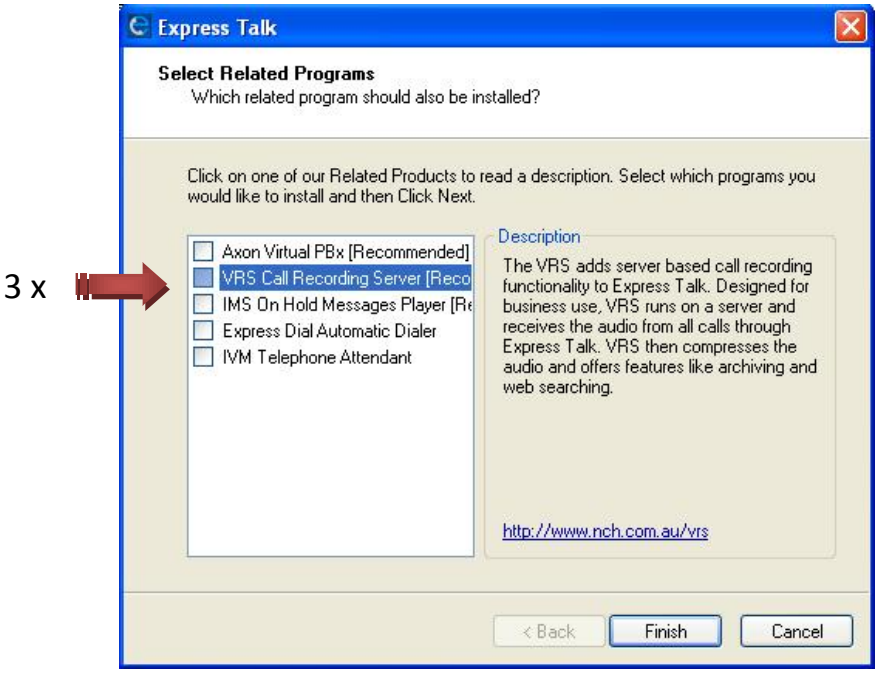
1. VOIP-PUHELUN SOITTAMINEN

Verkko on nyt siinä vaiheessa, mihin viime harjoituksessa päästiin. Tästä eteenpäin harjoituksessa käytetään oikeaa VoIP-liikennettä. VoIP-liikenne toteutetaan käyttämällä SoftPhone-puhelimia. Puhelimet asennetaan tietokoneisiin Computer A ja Computer B. IP-puheluja soitetaan suoraan tietokoneelta tietokoneelle SIP-protokollaa käyttäen. Aloitetaan siis VoIP-puhelinsovelluksen asentamisella ja käyttöön tutustumisella. Harjoitukseen sopivan sovelluksen voit noutaa osoitteesta http://www.nch.com.au/talk/index.html tai CCNP-kurssin verkkosivuilta https://www.wpk.tpu.fi/A4121_CCNP/tavaraa/ccnp3/. Ohjelman asennus sisältää monia tehtävän suorittamiseen vaikuttavia asetuksia, joten seuraavassa on näytetty yksityiskohtaisesti asennukseen liittyvät valinnat. Käynnistä ohjelman asennus Computer A:lla ja seuraa ohjeita.



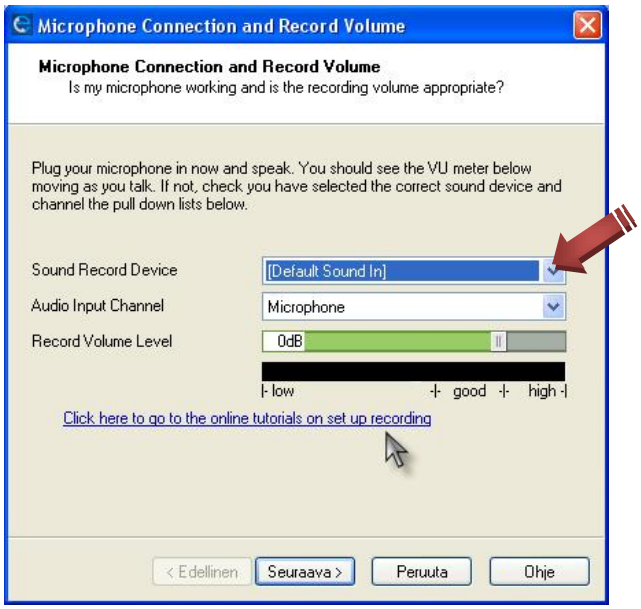
Kuva 2: Express Talk asennus – Lisenssiehdot

Ensimmäisenä asennusohjelma pyytää lukemaan ja hyväksymään lisenssiehdot. Hyväksymällä ne pääset jatkamaan asennusta.



Kuva 3: Express Talk asennus – Rinnakkaissovellukset

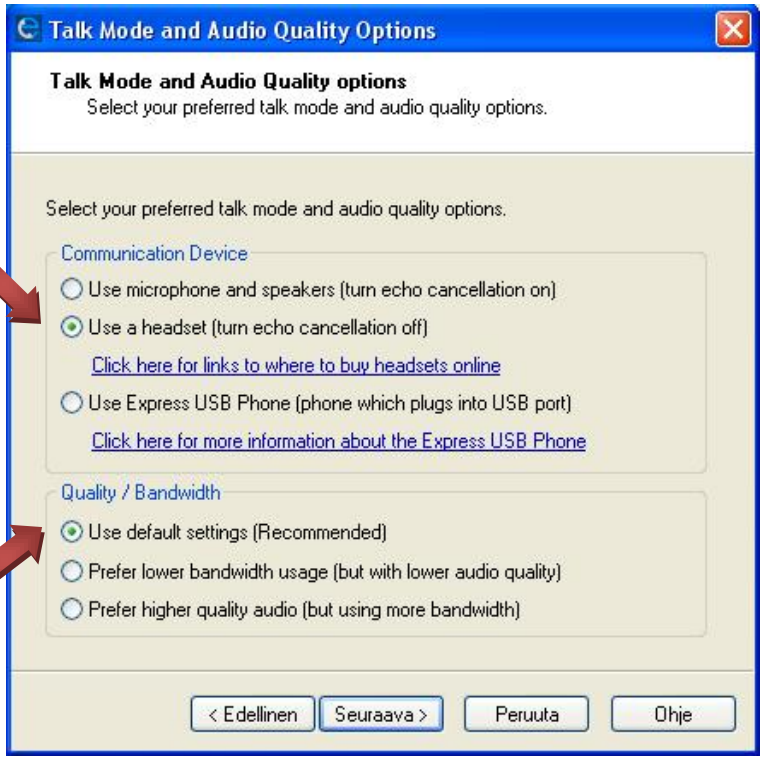
Seuraavaksi ohjelma kysyy, mitä ohjelmakomponentteja haluat asentaa puhelinsovelluksen lisäksi. Et tarvitse harjoitustehtävän suorittamiseen mitään tarjottavista lisäominaisuuksista. Poista valinta kaikista kohdista ja jatka asennusta.



Kuva 4: Express Talk asennus – Äänilähdön atetukset

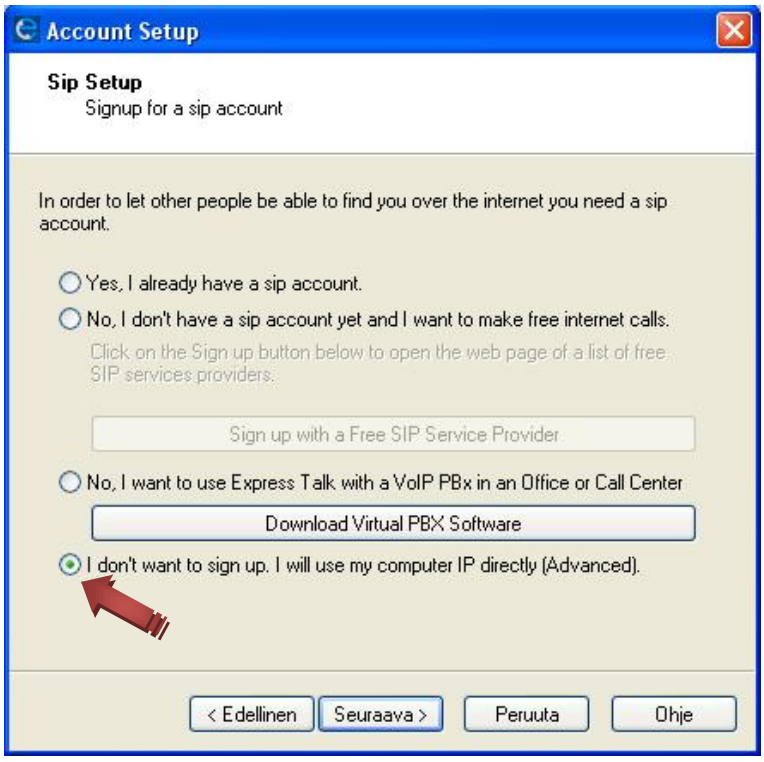
Kuva 5: Express Talk asennus – Äänentoiston asetukset

Ohjelma on nyt asennettu tietokoneelle, ja seuraavat valinnat muokkaavat ohjelman asetuksia. Äänen sisään- ja ulostuloliitännät pyydetään antamaan ja testaamaan niiden toiminta. Löydät pudotusvalikosta tietokoneeseen liitetyt laitteet. Tee ohjeiden mukaiset äänentasosäädöt.



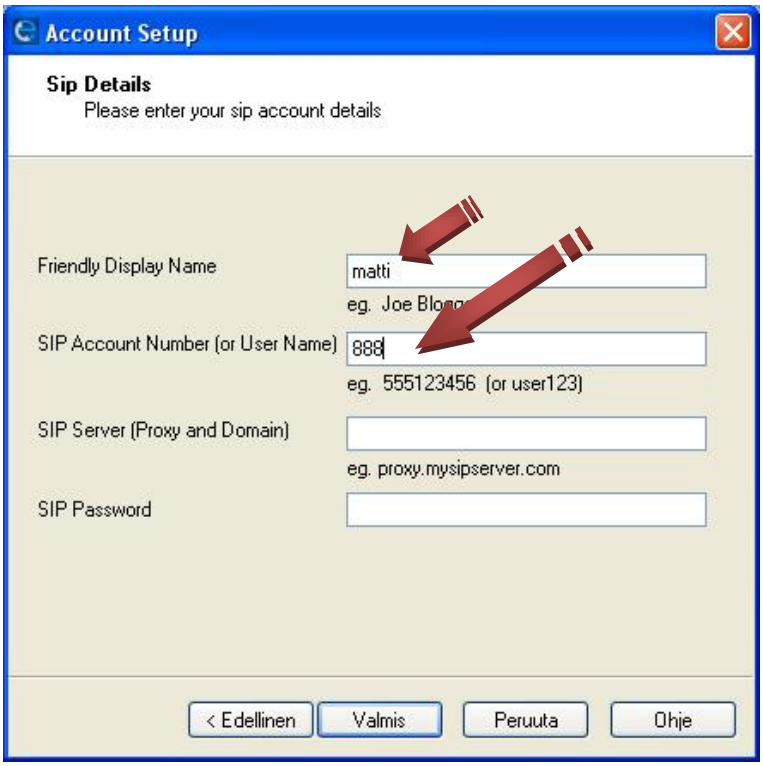
Kuva 6: Express Talk asennus – Laitteisto- ja äänenlaatuasetukset

Valitse seuraavaksi Communication Device –kohdasta, millä laitteella aiot käyttää puhelinsovellusta. Harjoitustehtävän suorituksen kannalta on suotavaa käyttää kuulokemikrofonia. Alempaan Quality / Bandwidth -kohdalla voidaan vaikuttaa haluttuun äänenlaatutasoon. Harjoitustehtävässä on suositeltavaa käyttää oletusasetuksia.



Kuva 7: Express Talk asennus – SIP-serverin käyttö

Koska ohjelma käyttää SIP-protokollaa voidaan sillä ottaa yhteys SIP-palvelimeen. SIP-palvelin on puhelinvaihde ohjelma, jolla voidaan hoitaa numerokäännöksiä ja ohjailla IP-puheluita myös valtakunnalliseen verkkoon. Tässä harjoituksessa IP-puhelut soitetaan suoraan tietokoneelta tietokoneelle omassa lähiverkossa ilman SIP-palvelinta. Valitse alin vaihtoehto ”I don’t want to sign up. I will use my computer IP directly [Advanced]”.

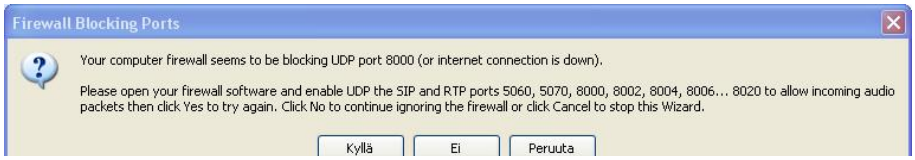


Kuva 8: Express Talk asennus – SIP-käyttäjätili

Vaikka SIP-palvelinta ei käytetä, täytyy ohjelmalle määritellä ainakin yksi käyttäjä. Käyttäjälle täytyy asettaa nimi ohjelman näyttöä varten ja SIP-numero, jota käytetään soitettaessa puheluja. Paina Valmis-painiketta

Kuva 9: Express Talk asennus – Porttien avaaminen ohjelman käyttöön

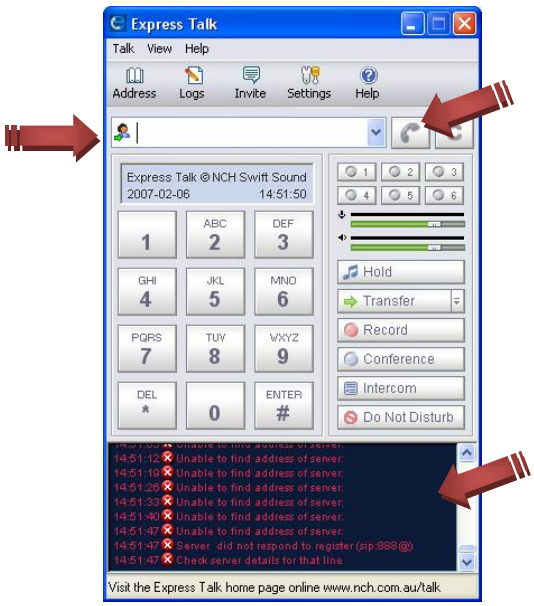
Kuva 10: Express Talk asennus – Virheilmoitus porttien avaamisesta 1/3



Kuva 11: Express Talk asennus – Virheilmoitus porttien avaamisesta 2/3

Kuva 12: Express Talk asennus – Virheilmoitus porttien avaamisesta 3/3

Seuraavaksi ohjelma yrittää aukaista palomuurista portteja, joita se käyttää toiminnoissaan. Kuvien 9-12 mukaiset ikkunat avautuvat ruudulle ja ilmoittavat ongelmista porttien avaamisessa. Jos käytössäsi on palomuuri, hyväksy porttien avaaminen. Muuten voit painaa ilmestyviin ikkunoihin Ei-valinnan. Harjoitusympäristössä ei ole suotavaa käyttää palomuuria, koska se saattaa luoda ongelmatilanteita joihinkin osiin harjoitusta.



Kuva 13: Express Talk – Ohjelman perusnäkymä

Asennus on valmis. Express Talk on käyttöliittymältään kuvan 13 mukainen. Kuvaan on myös nuolilla osoitettu rivi, jolle syötetään soitettavan henkilön soittotieto, puhelun vastausnäppäin ja logitietoruutu. Logitietoruudussa saattaa esiintyä ilmoitus, että SIP-palvelimeen ei saada yhteyttä. Tällä ei tilanteessamme ole merkitystä, koska SIP-palvelimen ei kuulu olla käytössä. Toista asennus Computer B:llä. Määrittele siellä käyttäjäksi mervi ja SIP-numeroksi 666.

Testaa IP-puhelinsovelluksen toiminta soittamalla yksi puhelu. Puhelu soitetaan syöttämällä vastaanottajan SIP-osoite kuvan 13 vasemman nuolen osoittamaan ruutuun. SIP-osoite on IP-verkon puhelinnumero ja se on muotoa SIP-numero@IP-osoite:porttinumero. Esim. 888@171.16.1.100:5070. Lopussa oleva 5070 numerosarja on Express Talkin yhteydenmuodostukseen käyttämä porttinumero. Oletusasetuksilla se on 5070. Kun puhelinyhteys toimii, varmista vielä, että puhe välittyy häiriöittä ja äänenlaatu on muutenkin hyvää tasoa. Yhteys kannattaa katkaista aina, kun sitä ei käytetä, koska ohjelman toiminta pysyy tällöin harjoitukseen sopivana.

2. STREAMING MEDIA SERVER

Pystyäksemme toteamaan, minkälainen on huono puheyhteys, ruuhkautamme verkon streamaamalla videota verkon läpi. Tämä onnistuu asettamalla streaming media server -sovellus lähettämään Server X:ltä videolähetystä Computer C:lle. Computer C vastaanottaa tämän lähetyksen ja näin käytettävissä olevasta kaistasta saadaan, median pakkaustavasta riippuen, hyvinkin suuri osa käyttöön. Lähetettävän videotiedoston tulisi olla mpeg-, avi- tai divx-muodossa, ja sen tulisi käyttää n. 8000 tavua bittivirtaa (bitrate). Osoitteesta http://www.gamershell.com/download_13714.shtml löydät sopivan videopätkän.

Tarvitaan siis sovellus, joka pystyy streamaamaan mediaa ja sovellus, joka pystyy ottamaan tällaisen lähetyksen vastaan. Tähän tarkoitukseen sopii mainiosti vapaan lähdekoodin ohjelma VLC media player. Se pystyy sekä lähettämään että vastaanottamaan streaming-lähetyksiä. Voit hakea sen osoitteesta http://www.videolan.org/vlc/ tai CCNP-kurssin verkkosivuilta https://www.wpk.tpu.fi/A4121_CCNP/tavaraa/ccnp3/. Ohjelman käyttö perustuu server-client -toimintatapaan. Tämä tarkoittaa sitä, että yksi VLC asennetaan koneeseen, joka toimii palvelimena. Palvelinkone asetetaan jakamaan videota. Muihin tietokoneisiin asennetaan myös VLC, ja ne asetetaan ottamaan vastaan palvelimen lähettämää lähetystä. Palvelin voidaan asettaa lähettämään ääntä tai videota unicast-lähetyksenä yhdelle tietylle vastaanottajalle tai multicast-lähetyksenä usealle vastaanottajalle yhtäaikaisesti. Lähetettävä lähetys voi olla DVD:n tai kiintolevyn lisäksi esim. Internetistä peräisin olevaa mediaa, jota VLC vain uudelleen lähettää eteenpäin.

Asenna VLC media player Server X:lle ja Computer C:lle. VLC:n asennus on hyvin yksinkertainen, eikä siinä pitäisi olla mitään ihmeellisyyksiä. Käynnistä ohjelma asennuksen jälkeen. Kuva 14 näyttää VLC:n perusnäkymän. Kuten huomaat, ohjelma on hyvin pelkistetty ilmeeltään ja sitä on hyvin helppo käyttää. Voit tutustua valikoista löytyviin ominaisuuksiin, mutta harjoituksessa tarvittavia toimintoja on vain muutama.

Kuva 14: VLC media player – Ohjelman perusnäkymä

Verkon läpi lähetettävän videomateriaalin olisi tarkoitus hidastaa muun verkkoliikenteen kulkua. Tämän takia valittavan videopätkän tulisi kuluttaa kaistaa huomattava määrä. Määrittäessä videokuvan käyttämää kaistanleveyttä voit käyttää apuvälineenä VLC:n näkymää, joka löytyy view-valikosta Stream and Media Info… -valinnan takaa. Siellä olevan Statistics-välilehden alta on nähtävissä videon kaistankulutus. Stream bitrate antaa osviittaa siitä, kuinka paljon kaistaa toistettava media tarvitsee. Send rate -kohta näyttää mediaa streamatessa todellisen lähetysnopeuden. Avaa siis yksi mediatiedosto ohjelmalla ja tarkastele näitä kenttiä. Valmiiksi annettu Crysis demo -videotiedosto riittää vallan mainiosti tukkeuttamaan kaistan. Itse asiassa harjoitus on rakennettu toimimaan nimenomaan kyseisellä bittivirralla olevan videotiedoston kanssa yhteensopivaksi.

Aloita Server X:ltä lähettämään Computer C:lle videokuvaa. Tämä onnistuu helpoiten tähän tarkoitukseen olevalla asennus velhon avulla. Velho löytyy valitsemalla File-valikosta Wizard… -valinnan.

Velhosta valitaan seuraavat valinnat:

- Stream to network -> Next

  Valittavana on kaksi vaihtoehtoa. Jälkimmäisellä Transcode/Save to file -toiminnolla otetaan vastaan streaming-lähetystä ja tallennetaan se omalle tietokoneelle omaksi tiedostoksi. Ensimmäisellä puolestaan streamataan mediatiedostoa verkkoon. Sillä on myös mahdollista uudelleen ohjata streamattua verkkolähetystä, kuten nettiradiota, edelleen lähiverkkoon.

- Select a stream ->Choose…

  Valitaan streamattava media. Alhaalla oleviin kenttiin voidaan myös määritellä alku- ja loppukohdat mediasta, jos halutaan lähettää vain jokin osa median sisällöstä.

- Hae haluttu äänitiedosto -> OK -> Next
- RTP Unicast -> Destination 171.16.1.150 -> Next

  Valitsee lähetystavan. Streamaus voidaan tehdä unicast-, multicast-, tai http-lähetyksenä. Yhdelle tietokoneelle lähetettäessä valitaan unicast-lähetys. Tällöin lähetys voidaan ottaa vastaa vain yhdellä tietokoneella ja vain yhteen määriteltyyn IP-osoitteeseen. Lähetettäessä useammalle tietokoneelle voidaan valita joko multicast- tai http-lähetystapa. Multicast-lähetyksessä täytyy verkon laitteiden tukea multicast-ominaisuutta ja jokaisen vastaanottajan tulee liittyä kuuntelemaan tiettyä multicast-osoitetta. Http-lähetystavassa data siirtyy http-protokollan päällä, ja lähetys vastaanotetaan selaimen avulla. Vastaanottajia voi olla useampia.

  HUOM! Http-lähetys on hyvin herkkä katkeamaan, mikäli lähetys joutuu kulkemaan ylikuormitetussa verkossa.

- MPEG TS -> Next

  Lähetykselle täytyy määritellä jokin kapselointi tyyppi.

- Ei muutoksia -> Next

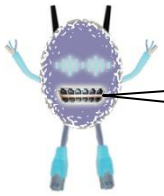
  VLC rupeaa heti lähettämään valittua lähetystä. Seuraavaksi vastaanottajien täytyy ottaa lähetys vastaan.

Kun lähetys on aloitettu, voidaan asettaa Computer C ottamaan vastaan tätä lähetystä. Lähetyksen vastaanottamiseksi mene File -> Open network stream… . Eteesi avautuu ikkuna, jonka avulla voidaan määritellä, mistä vastaanotettava liikenne on lähtöisin. Valitse UDP/RTP-valinta ja anna portiksi 1234. Porttinumero on ohjelman oletusportti, mihin se lähettää ja vastaanottaa streamattavaa unicast-lähetystä. Ok-napin painamisen jälkeen ruudulle pitäisi ilmaantua vastaanotettava lähetys.

VLC voidaan asettaa lähettämään samaa lähetystä aina uudestaan ja uudestaan. Tämä helpottaa harjoituksen suorittamista. Asetuksen voi tehdä view -> Playlist… -valikosta Repeat One -painikkeella.

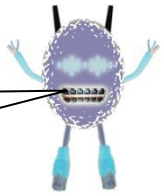
Hyvä! Sekä puhelin sovellus että Streaming media-sovellus toimii moitteetta. Asettamalla ne toimimaan yhtä aikaa päästään kokeilemaan, kuinka ääniliikenne reagoi verkon ruuhkautumiseen.

HUOM! Jos VLC joutuu ottamaan pätkivää ja huonolaatuista videokuvaa pitkään vastaan, saattaa ohjelma kaatua.



Onko IP-puhelun laadussa huomattavaa eroa aiempaan, kun verkossa on lisäksi streaming-lähetys? Jos on, niin minkälaista?

Katso vielä Wiresharkilla esiintyykö äänipaketeissa minkäänlaista luokittelua. Jos esiintyy, mistä se on peräisin?



Lisätehtävä

Lähetä VLC:n lähettämä streaming-lähetys http-protokollan päällä. Lähettäminen onnistuu Server X:llä samaisen asennus velhon avulla. Valittaessa streamaus-tapaa valitaan RTP Unicast -lähetystavan tilalle http-protokollan päällä tapahtuva lähetys. Muuta asetusmuutosta ei tarvitse tehdä. Computer B:llä otetaan lähetys vastaan osoitteesta http://171.16.1.150:8080. Tämän jälkeen lähetyksen pitäisi näkyä.

Jos säätäminen kiinnostaa, kokeile vielä seuraavaa (vain WPK-verkossa). Liitä Server X:ään toinen verkkokortti ja liitä se WPK-verkkoon. Testaa Internet-yhteyden toiminta. Aseta VLC streamaamaan lähetystä, joka on peräisin jostakin Internet lähteestä. Esim. www-osoitteesta http://217.30.180.245/listen.pls. Streamaa lähetys Computer C:lle ja ota se vastaan sillä. Esimerkissä olevasta osoitteesta tuleva KLF-radiokanavan lähetyksen pitäisi nyt kuulua Computer C:llä.

3. LUOKITTELU

Opit viime harjoituksessa luokittelemaan liikennettä CoS- ja ToS-merkintöjen avulla. Tee seuraavaksi oppimiasi taitoja hyödyntämällä suunnitelma tähän tehtävään sopivasta liikenteen luokittelusta. Kirjaa ylös tarvittavat komennot, ja selvitä itsellesi luokittelun rakenne. Jos sinulla on käytössäsi ohjaaja, kysy hänen mielipidettä suunnitelmasi toimivuudesta. Voit käyttää hyväksesi harjoitustehtävä 1:sen materiaalia sekä Ciscon konfiguraatio-opasta. Oppaan löydät osoitteesta http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2960/12225see/scg/swqos.pdf.

Ohjeet:

- Käytä Luokkia EF (DSCP 46), CS3 (DSCP 24) ja CS2 (DSCP 16)
- Luokittele ääniliikenne, äänensignalointiliikenne ja telnet-liikenne edellä mainittuihin luokkiin

4. QOS-TOIMENPITEET VERKKOLAITTEILLE

Jotta QoS-toimenpiteet osataan tehdä verkkolaitteille, on ensiarvoisen tärkeää tuntea paketin käymät QoS-prosessit sen kulkiessa laitteen lävitse. Tämä kappale kuvaa paketin kulun Ciscon Catalyst 2960 ja 3560 -kytkinten lävitse. Prosessin kuvaus painottuu jonotuksen ja aikataulutuksen selvittämiseen, koska luokittelu on käyty syvemmin läpi jo aiemmassa harjoituksessa. Kappaleessa mainitaan ainoastaan 2960-kytkin, mutta samat komennot ja ominaisuudet löytyvät myös 3560-kytkimestä. 2960-kytkin käyttää QoS-käsittelyssä SRR- ja WTD-algoritmeja. Seuraavassa pieni selvitys, mitä varten algoritmit ovat.

SRR – Jonojen purkamiseen käytetty algoritmi

SRR(Shaped/Shared round-robin) on Catalyst 2960-kytkimellä jonotuksen hallintaan käytettävissä oleva algoritmi. Se on kehittyneempi versio aiemmasta round-robin -menetelmästä. Eri verkkolaitteilla on omat liikenteenhallintavälineensä ja esimerkiksi edellisessä Catalyst-mallissa 2950 oli SRR:n tilalla WRR-jonotuskäsittely. WRR:n konfigurointi on huomattavasti yksinkertaisempaa kuin SRR:n. Kytkinmallin heikkouksiin kuuluu kuitenkin liikenteen luokittelu ainoastaan CoS-arvojen perusteella. Lisäksi WRR:ää voitiin käyttää vain ulostuloporteissa. Uutta 2960-kytkimessä on se, että näitä QoS-tekniikoita on mahdollisuus hyödyntää joiltakin osin myös sisääntuloportissa.

SRR voidaan asettaa toimimaan kahdessa eri tilassa Catalyst 2960/3560 -kytkimellä. Nämä tilat ovat sharing ja shaping. Shaped-tilassa jokaiselle jonolla annetaan prosentuaalinen osuus taattua kaistaa ja ne ovat rajoitettu tähän lukemaan. Kaistan käyttö ei voi täten nousta koskaan asetetun arvon yläpuolelle, vaikka linkki olisi muilta osin käyttämätön. Tämä mahdollistaa purskeisen liikenteen tasoittamisen pitemmällä aikavälillä. Shared-tilassa kaista jaetaan jonojen kesken määriteltyjen arvojen perusteella. Kaista on taattua arvojen mukaisesti, mutta se ei estä käyttämästä kaistaa myös enemmän, jos jonkin muun luokan kaistavaraus jää käyttämättömäksi. Catalyst 2960 -kytkin pystyy käyttämään sisääntuloportissa share-tilaa, mutta ulostuloportissa molempia tiloja. Harjoituksessa käytetään ainoastaan share-tilaa.

WTD – Ennaltaehkäisevä ruuhkanhallinta

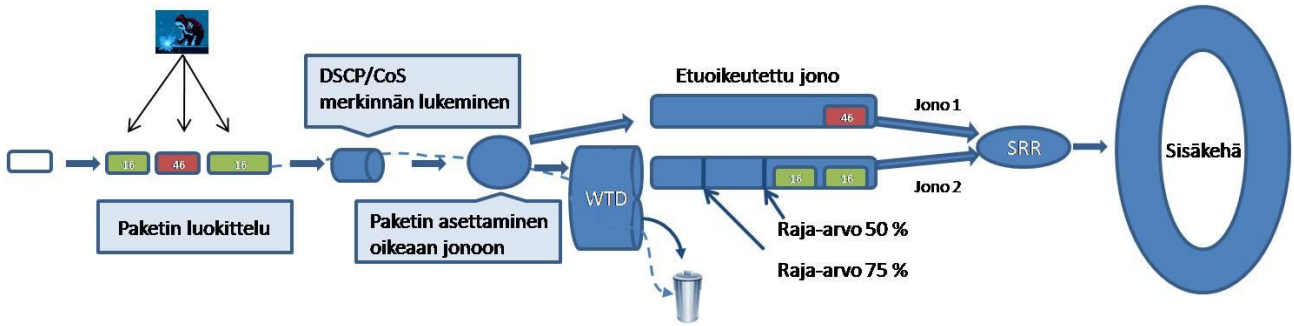
2960-kytkimessä voidaan Tail Drop -menetelmän tilalla käyttää WTD (Weighted Tail Drop) -menetelmää. Tämä mahdollistaa pakettien pudottamisen jo ennen kuin jonot täyttyvät, ja pystytään kohdistamaan pakettien pudottamiset vähemmän tärkeään liikenteeseen DSCP-merkintöjen avulla. WTD tarvitsee toimiakseen ennalta määriteltyjä raja-arvoja (threshold). Raja-arvo on prosenttimäärä jonon kokonaiskoosta. Se määrittelee pisteen, minkä jälkeen paketteja aletaan pudottaa jonosta. WTD ennaltaehkäisee jonojen täyttymistä allokoimalla jonon käyttämästä välimuistitilasta suuremman osan tärkeälle liikenteelle ja pudottamalla vähemmän tärkeää liikennettä jo ennen jonon täydellistä täyttymistä.

Kuva 15 osoittaa sinisellä katkoviivalla seuraavaksi vuorossa olevan paketin kulun. Esimerkki selventää hieman WTD:n toimintaa. Siinä nähdään kuinka jonolle 2 on asetettu kaksi eri raja-arvoa. Seuraava paketti, joka on käsiteltävänä, kuuluu alimmaiseen jonoon ja on raja-arvon 50 % alainen. Jäljellä oleva vapaa tila jonossa, ennen raja-arvoa, on kuitenkin pienempi kuin paketin koko, joten WTD tulee pudottamaan paketin. Näin jonotustilaa säästyy muulle liikenteelle. Jos kyseessä on TCP-liikennettä, voi se pudottaa liikennöintinopeuttaan.

A. INGRESS (SISÄÄNTULOPORTTI)

Sisääntuloportin ruuhkanhallintamenetelmien käyttö on perusteltua, mikäli voidaan olettaa, että laite saattaa ruuhkautua käsiteltävän datan määrästä. Tällöin laitteen sisäkehä (internal ring) ei pysty käsittelemään kaikkea sitä liikennevirtaa, mikä sen läpi täytyisi virrata.

Aloitetaan sisääntuloportin QoS-vaiheiden tutkiminen ihan alusta. Kuva 15 havainnollistaa QoS-prosessia sisääntuloportissa. Paketti saapuu kytkimelle jostakin sisääntuloportista. Ensimmäisenä paketti joutuu luokitteluprosessiin. Vaihtoehtoina on paketin luokitteluun luottaminen tai luokittelumerkinnän tekeminen riippuen siitä, onko laite luottamusrajan sisäpuolella oleva laite vai rajalla merkintöjä tekevä laite. Luokittelun jälkeen paketista luetaan sen sisältämät luokittelubitit. Näiden arvojen perusteella paketti asetetaan menemään jompaankumpaan kahdesta sisääntulojonosta. Ennen paketin asettamista jonoon, varmistetaan onko kohteena oleva jono prioriteettijono. Jonon ollessa prioriteettijono asetetaan paketti kyseiseen jonoon. Kohteena olevan jonon ollessa normaali jono, tarkistetaan, onko jonolle asetettu WTD raja-arvoja ja ylittyvätkö ne. Paketin päästyä jonoon se jää odottamaan omaa vuoroaan. Jonojen purku tapahtuu SRR-algoritmin toimesta. SRR purkaa annettujen painoarvojen mukaisesti näitä kahta jonoa ja lähettää paketteja jonosta kohti laitteen sisäkehää.

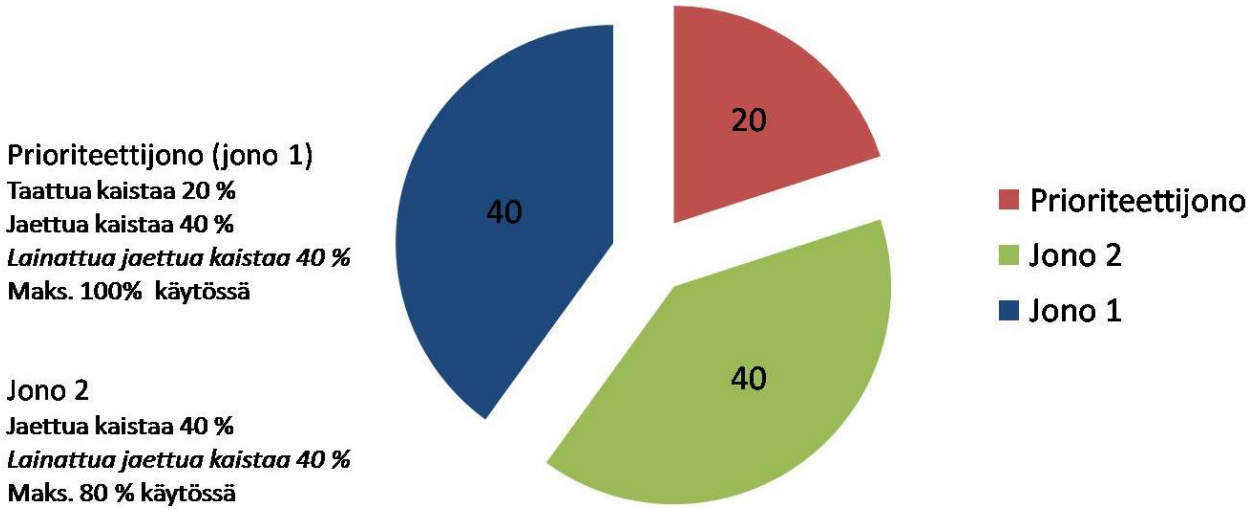


Kuva 15: Catalyst 2960 -kytkimen QoS-prosessi (Ingress)

Laitteen sisäkehällä tapahtuviin toimiin ei tarvitse kiinnittää huomiota QoS-prosessissa. Tärkeintä on vain tietää, että sieltä paketti ohjataan oikeaan ulostuloporttiin.

Catalyst 2960 -kytkin mahdollistaa sisääntuloportissaan kahden jonon käyttämisen. Jonoihin voidaan poimia liikennettä niiden CoS- tai DSCP-merkintöjen avulla. Jonojen purku tapahtuu SRR-algoritmin avulla. Se on round-robin tyylinen algoritmi ja se toimii niin, että se purkaa paketteja vuoronperään jokaisesta jonosta. SRR on kehittyneempi versio perinteisestä round-robinista, ja se pystyy painottamaan eri jonojen purkamista. Lisäksi se mahdollistaa etuoikeutetun jonon tekemisen (priority queue). Etuoikeutettuun jonoon on mahdollista määritellä omaa varattua kaistanleveyttä, ja loppu kaistanleveys on jaettavissa edelleen kaikkien jonojen kesken.

Esimerkki. Kuva 16:sta on esitetty yksi ratkaisu painoarvojen asettamisesta. Sisääntuloportissa on siis käytettävissä kaksi eri jonoa. Toinen jonoista asetetaan prioriteettijonoksi, ja siihen määritellään prosentuaalinen osuus kaistasta, mikä taataan sen käyttöön. Esimerkkitapauksessa taattua kaistaa annetaan 20 %. Tämän jälkeen loppuosa kaistasta jaetaan kaikkien jonojen kesken painoarvojen 50 ja 50 mukaisesti. Prioriteettijonon osuuden jälkeen jää 80 % kaistasta jaettavaksi näiden kahden jonon kesken. Molempien osuus kaistasta on 40 %. Käytännössä tämä tarkoittaa sitä, että prioriteettijono saa taattua kaistaa 20 % käyttöönsä ja vielä tämän lisäksi 40 % jaettua kaistaa. Taatun kaistan ja jaetun kaistan ero on siinä, että taattu kaista on aina varattuna sen käyttöasteesta riippumatta. Jaettu kaista voi kuitenkin olla muiden käytössä, mikäli se on käyttämättömänä.



Kuva 16: Kaistan jakaminen sisääntuloportissa

QoS konfigurointi Catalyst 2960 ja 3560 -kytkimille

Seuraavassa taulukossa on esitelty sisääntuloportin jonot ja niihin kohdistuvat luokat:

	jonoon asetettavat luokat	asetukset
jono 1	EF (DSCP 46)	prioriteettijono
jono 2	kaikki loput	WTD

Yksinkertaisimmillaan, kun paketti saapuu 2960-kytkimelle:

- WTD katsoo ylittyykö mikään raja-arvo
- paketti siirretään johonkin jonoista
- SRR purkaa jonoja toisesta päästä

Sisääntuloportissa asetetaan jono 1 prioriteettijonoksi ja sille allokoidaan taattua kaistaa 15 %. Jono 1 määritellään raja-arvo ID 1:n alaiseksi ja asetetaan siihen liikenne DSCP-arvolla 46. Jäljellä oleva kaista on ns. jaettua kaistaa. Siitä jaetaan jonolle 1 viidennes ja neljä viidennestä jonolle 2. Jonoon 2 osoitetaan liikenne DSCP-arvoilla 0, 16 ja 24, ja se määritellään raja-arvo ID 2:n alaiseksi. Välimuistista allokoidaan 20 % jonolle 1 ja 80 % jonolle 2. WTD:n raja-arvoiksi määritellään jonolle 2 50 % ja 75 %. Jono 1:een ei aseteta WTD:tä aktiiviseksi.

Tee seuraavat asetukset kaikille kytkimille. Ne asettuvat voimaan kaikkiin sisääntuloliitäntöihin.

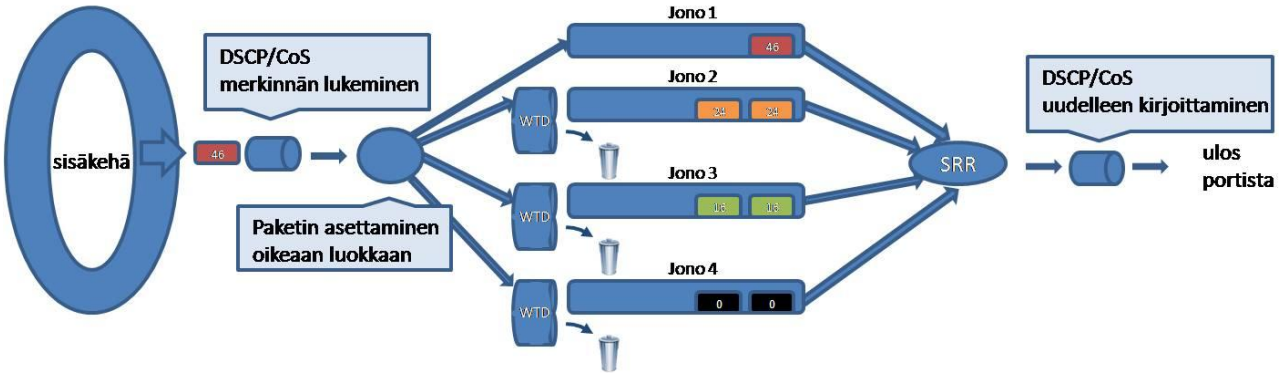
SRR:n ja WTD:n konfigurointi (ingress)

(config)# mls qos srr-queue input priority-queue 1 bandwidth 15	*luodaan prioriteettijono jonosta 1 ja sille allokoidaan 15 % taattua kaistaa*
(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 46	*määritetään jonoon 1 DSCP-arvon 46 omaava liikenne, ja määritellään jono 1 käyttämään raja-arvo ID 1 mukaisia WTD-asetuksia*
(config)# mls qos srr-queue input bandwidth 1 4	*loput kaistasta on jaettua kaistaa, josta 1/5 on jonolle 1 ja 4/5 jonolle 2*
(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 0 16 24	*jonoon 2 osoitetaan DSCP-arvoilla 0, 16 ja 24 oleva liikenne ja määritellään jono 2 käyttämään raja-arvo ID 2 mukaisia WTD-asetuksia*
(config)# mls qos srr-queue input buffers 20 80	*määritellään jonolle 1 välimuistia 20% ja jonolle 2 80 %*
(config)# mls qos srr-queue input threshold 1 100 100	*määritetään raja-arvo ID 1 WTD-arvot*
(config)# mls qos srr-queue input threshold 2 50 75	*määritetään raja-arvo ID 2 WTD-arvot 50 % ja 75 %*

B. EGRESS (ULOSTULOPORTTI)

Ulostuloportissa ruuhkanhallintamenetelmien käyttö on perusteltua, mikäli siihen kytketty linkki on siirtokapasiteetiltaan pienempi kuin sen tarve siirtää liikennettä. Tällainen tilanne on monesti uplinkeissa, joissa suuri määrä linkkejä yhdistyy kulkemaan yhtä linkkiä pitkin.

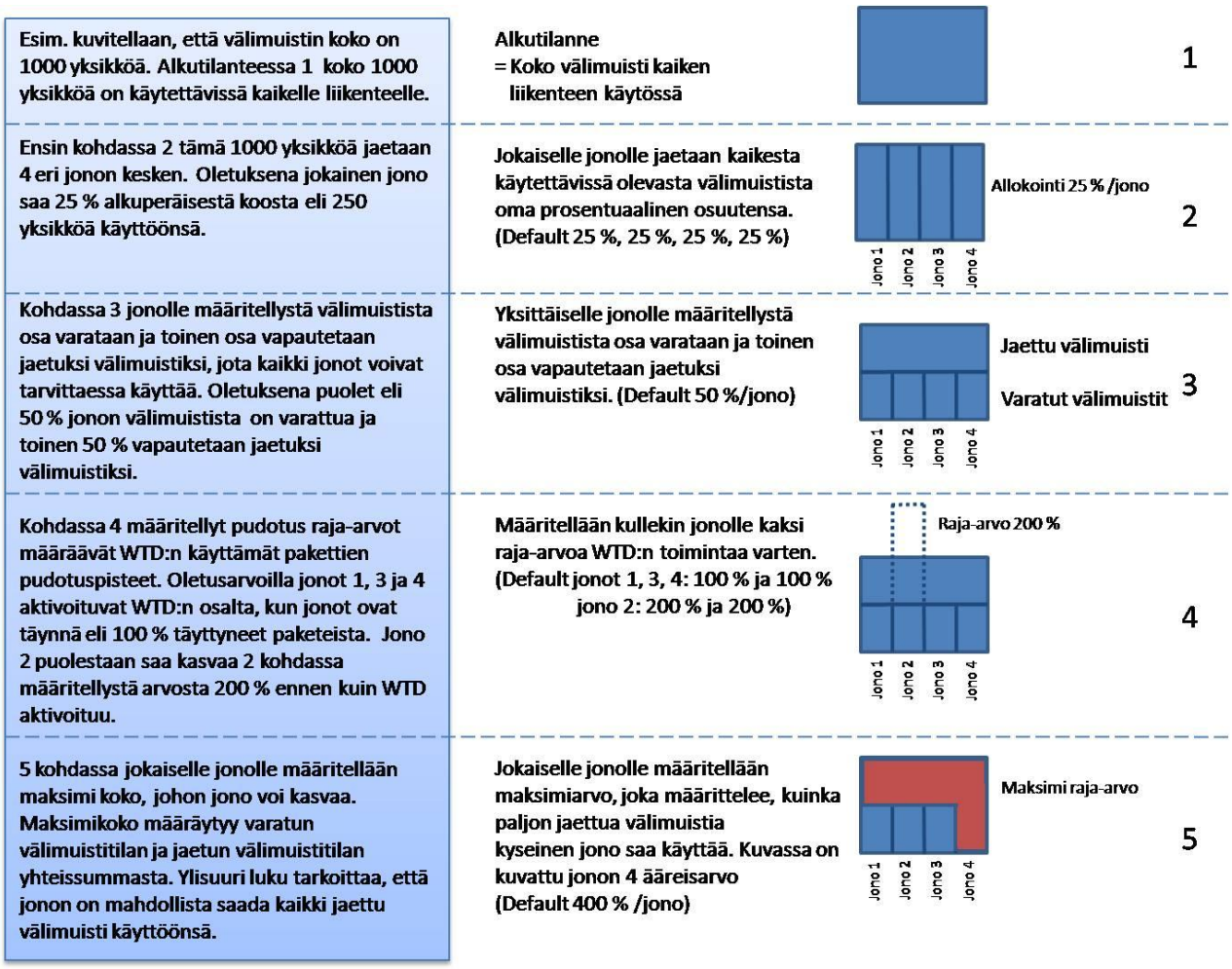
Paketin saapuessa sisäkehältä ulostuloporttiin paketista luetaan ensimmäisenä sen sisältämät luokittelubitit. Tämän jälkeen liikenne ohjataan oikeaan jonoon. Ensimmäisestä jonosta on mahdollista tehdä niin kutsuttu kiirejono (expedite queue). Kiirejonon täytyy aina olla tyhjä ennen kuin muita jonoja voidaan alkaa tyhjentämään. Ennen jonoon asettamista katsotaan, kuuluuko paketti WTD-käsittelyyn. Kiirejono ohittaa WTD-käsittelyn automaattisesti. Jos paketti kuuluu WTD-käsittelyyn, katsotaan, onko se jonkin raja-arvon sisällä. Mikäli paketin koko ylittää raja-arvon tai jono itsessään on täynnä, paketti pudotetaan. Jonon purku tapahtuu SRR:n mukaisesti samalla tavalla kuin sisääntuloportissakin, mutta jonoja on käytössä kahden sijasta neljä. SRR:n poimittua paketti, sen luokittelubittejä voidaan vielä muuttaa. Lopuksi paketti lähetetään portista ulos.



Kuva 17: Catalyst 2960 -kytkimen QoS-prosessi (egress)

Välimuistin varaus jonoille

Jokaisessa liitännässä on olemassa jonoja varten oma välimuistitila (buffer). Sekä sisääntuloliikenteelle että ulos lähtevälle liikenteelle on olemassa oma välimuisti. Tätä välimuistitilaa voidaan jakaa eri jonojen kesken. Mitä enemmän välimuistia jonolle annetaan käyttöön, sitä enemmän jono voi kasvaa ja ottaa vastaan paketteja. Sisääntuloliitännässä on käytössä kaksi jonoa ja ulostuloliitännässä neljä jonoa. Kuvassa 18 on selvitetty välimuistin jakamista. Siinä on käytössä laitteen oletusarvot.



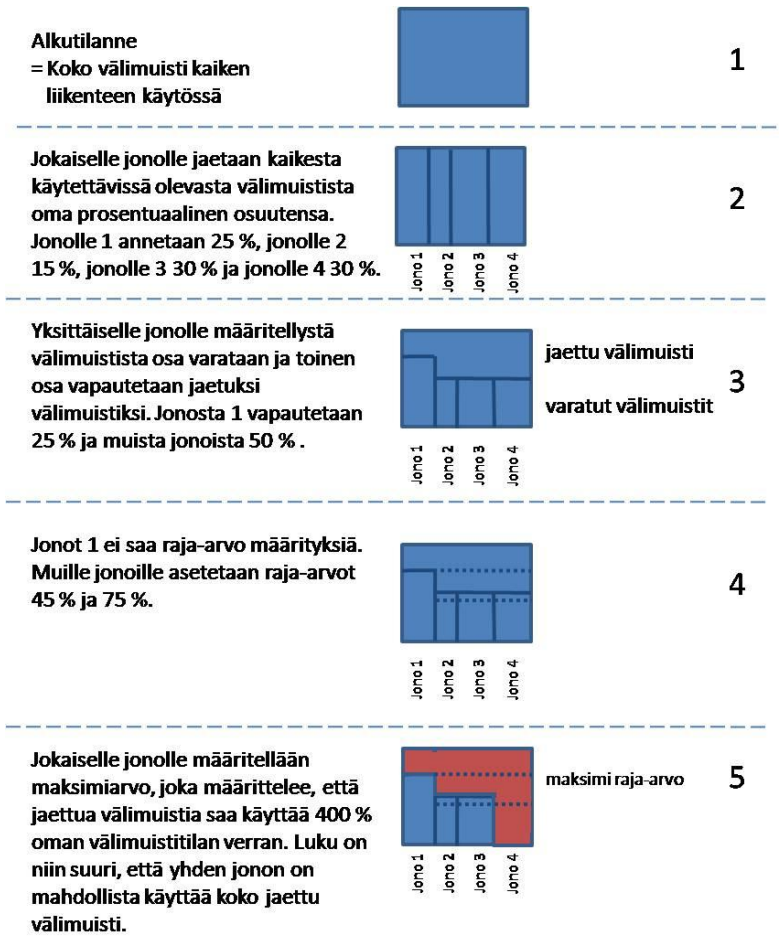
Kuva 18: Välimuistin jakaminen ulostuloportissa oletusasetuksilla

QoS-konfigurointi Catalyst 2960 ja 3560 -kytkimille

Seuraavassa taulukossa on esitelty ulostuloportin jonot ja niihin kohdistuvat luokat:

	jonoon asetettavat luokat	asetukset
jono 1	EF (DSCP 46)	kiirejono (expedite queue)
jono 2	CS3 (DSCP 24)	WTD
jono 3	CS2 (DSCP 16)	WTD
jono 4	kaikki loput	WTD

Ulostuloportissa asetetaan jono 1 kiirejonoksi. Tämä toimii ulostuloportissa niin, että tämän jonon täytyy olla tyhjä ennen kuin muita jonoja aletaan tyhjentää. Muille jonoille määritetään painoarvojen avulla jaettua kaistaa. Loppu kaista jakautuu jonolle 2 15 %, jonolle 3 35 % ja jonolle 4 50 % mukaisesti. Jonoon 1 osoitetaan DSCP-arvolla 46 oleva liikenne, jonoon 2 arvolla 24, jonoon 3 arvolla 16 ja jonoon 4 arvolla 0. Jono 1 liitetään raja-arvo ID 1 määrityksen alaiseksi ja loput jonot raja-arvo ID 2 alaisiksi. Välimuistin jakamista harjoituksen omassa tilanteessa havainnollistetaan kuvan 19 avulla. Voit verrata laitteiden oletusasetuksia ja harjoituksessa tehtäviä asetuksia keskenään vertaamalla kuvia 18 ja 19.



Kuva 19 : Välimuistin jakaminen ulostuloportissa

Tee seuraavat asetukset kaikkiin kytkinten välisiin liitäntöihin molemmille puolille.

SRR:n ja WTD:n konfigurointi (egress)

(config-if)# priority-queue out	*asettaa jonon 1 prioriteetti jonoksi*
(config-if)# srr-queue bandwidth share 10 15 35 50	*ensimmäinen arvo mitätön, koska se on prioriteettijono; jono 2 saa 15 %, jono 3 35 % ja jono 4 50 % jaettua kaistaa käyttöönsä*
(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 46	*määrätään DSCP-arvolla 46 oleva liikenne jonoon 1 ja jono määritetään raja-arvo ID 1 alaiseksi*
(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 24	*määrätään DSCP-arvolla 24 oleva liikenne jonoon 2 ja jono määritetään raja-arvo ID 2 alaiseksi*
(config)# mls qos srr-queue output dscp-map queue 3 threshold 2 16	*määrätään DSCP-arvolla 24 oleva liikenne jonoon 2 ja jono määritetään raja-arvo ID 2 alaiseksi*

(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 0

määrätään DSCP-arvolla 24 oleva liikenne jonoon 2 ja jono määritetään raja-arvo ID 2 alaiseksi

(config)# mls qos queue-set output 1 buffers 25 15 30 30

jakaa välimuistia jonolle 1 25 %, jonolle 2 15 %, jonolle 3 30 % ja jonolle 4 30 %

(config)# mls qos queue-set output 1 threshold 1 100 100 75 400

määritetään raja-arvo ID 1 arvoiksi pudotus raja-arvo 1 = 100, pudotus raja-arvo 2 = 100, varattu välimuisti 75 % ja maksimi välimuistin käyttö 400 % alkuperäisestä

(config)# mls qos queue-set output 1 threshold 2 45 75 50 400

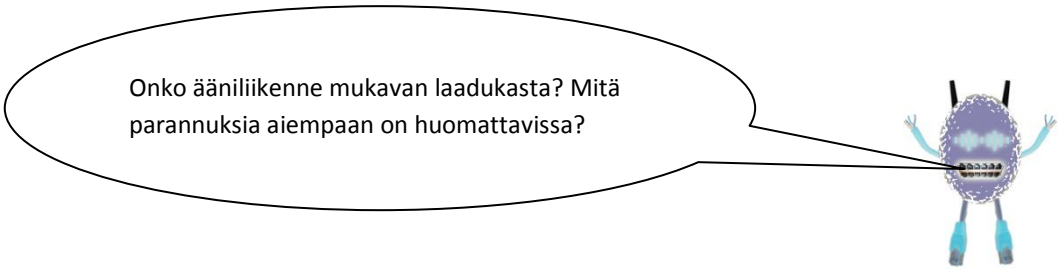
määritetään raja-arvo ID 2 arvoiksi pudotus raja-arvo 1 = 45, pudotus raja-arvo 2 = 75, varattu välimuisti 50 % ja maksimi välimuistin käyttö 400 % alkuperäisestä

Voit varmistaa asetuksien oikeellisuuden show komennoilla:
#show mls qos

Tarkista ainakin, että QoS on aktiivinen!!!

#show mls qos input-queue
#show mls qos interface fa0/24 buffers
#show mls qos interface fa0/24 queueing
show mls qos maps
#show mls qos queue-set 1

Soita nyt uusi IP-puhelu streaming median tukkiessa kaistaa.



5. LOPUKSI

Harjoituksessa opittiin käyttämään Softphone-sovellusta ja streamaan videokuvaa verkkoon. Tämän jälkeen verkkoon aloitettiin tekemään QoS-toimia. Luokittelu tehtiin harjoitus 1:n taidoilla. Laitteiden mahdollistamat palvelun laadun takaamista varten olevat ominaisuudet opeteltiin ja ne asetettiin toimintaan. Palvelun laadun takaaminen onnistui Catalyst 2960 ja 3560 -kytkimissä välimuistia allokoimalla, WTD-algoritmilla ja kaistan jakamisella SRR-algoritmin avulla.

Harjoituksen konfiguraatioissa käytetyt arvot ovat harjoitusta varten suunniteltu. Näiden arvojen lukemat ovat aina verkkokohtaisia, ja ne ovat sidoksissa ennalta tutkittuihin liikennevirta selvityksiin. Ennen VoIP-liikenteen implementointia jo käytössä olevaan verkkoon tarvitsee määritellä, kuinka paljon ääniliikennettä verkossa liikkuu ja kuinka paljon se tarvitsee priorisoitua kaistaa. Kaikki QoS-toimet ovat ehdottoman tärkeitä toteuttaa end-to-end-periaatteiden mukaisesti niin, että kaikki ääniliikenteen matkalla olevat laitteet osallistuvat priorisointiprosessiin, koska yksikin pullonkaula verkossa voi romuttaa kaikkien muiden QoS-toimien hyödyt. Lisäksi on muistettava, että kaikki QoS-toimet ovat vain ratkaisuja tilapäisten ruuhkatilanteiden hallintaan. Jos verkko on ruuhkainen yhtenään, on verkon kapasiteetti alimitoitettu. Tällöin ainoa keino on suunnitella verkon käyttö uudelleen tai lisätä siihen tarvittava määrä lisäkaistaa.

Viimeisenä ota talteen seuraavat asetukset:

- access-tason kytkimiltä liikenteen luokitteluun vaaditut komennot
- acces-tason kytkinten ja distri-kytkimen QoS-käsittelyyn liittyvät komennot

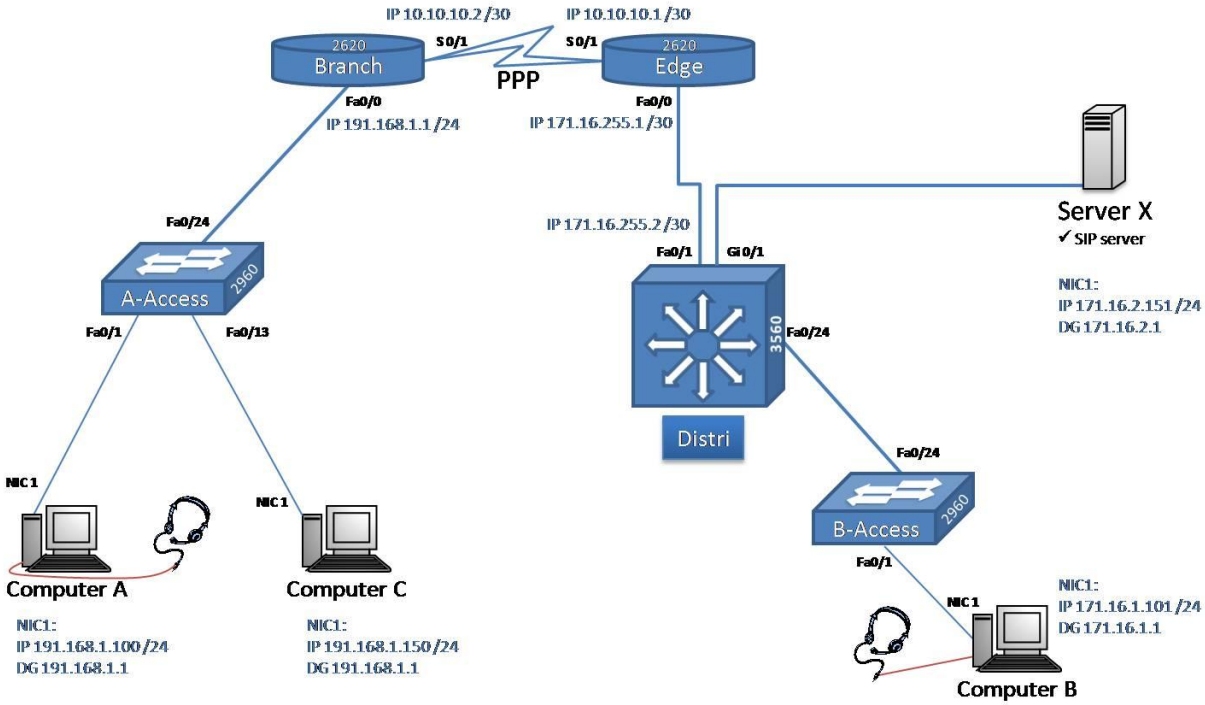
TYÖHARJOITUS 3 – VOIP-LIIKENNE ETÄTOIMIPISTEIDEN VÄLILLÄ

Tämä harjoitus on viimeinen osa kolmen harjoituksen kokonaisuudesta. Harjoituksen tarkoituksena on kasvattaa muodostettu verkko käsittämään myös etätoimipistettä ja omaa sisäverkon palvelinfarmia. Harjoituksessa ensimmäisenä laajennetaan vanhaa topologiaa, tehdään siihen VoIP-liikenteen vaatimat toimenpiteet ja testataan, kuinka end-to-end-yhteys VoIP:n osalta käytännössä toimii.

Esivaatimukset

- ✓ 2 x Cisco Catalyst 2960
- ✓ 1 x Cisco Catalyst 3560
- ✓ 2 x Cisco 2620
- ✓ 4 x PC (Windows XP)
- ✓ 2 x kuulokemikrofoni
- ✓ Perus tiedot/taidot lähiverkoista ja käytettävistä laitteista
- ✓ Ohjelmat: VLC media server, Axon virtual PBX ja Express Talk
- ✓ DiffServ-arkkitehtuurin ymmärtäminen
- ✓ Ciscon laitteiden avulla liikenteen luokitteluun vaadittavat komentorivikomennot
- ✓ Työharjoitus 1 vaihe 2 tehtynä
- ✓ Työharjoitus 2 vaihe 1 ja 3 tehtynä

Verkon rakenne muuttuu hieman. Uutena tulokkaana siihen liitetään yksi etätoimipisteyhteys. Verkko lisääntyy kahdella reitittimellä, ja verkossa oleva palvelin siirretään muodostamaan palvelinfarmi. Yksi reitittimistä toimii reunareitittimenä verkon reunalla ja yksi kuvastaa etätoimipisteen reunareititintä. Etätoimipisteen liitos on toteutettu PPP-linkin avulla.



Kuva 1: Verkon kuva

1. VERKON MUUTOKSET

Tee muutokset aikaisempaan verkkoon kuvan 1 ja alapuolella olevien ohjeiden avulla.

Verkkolaitteet

- Siirrä Server X Distri-kytkimen Giga0/1-porttiin ja liitä se VLAN 120:n
- Liitä Distri-kytkin portista fa0/1 kiinni Edge-reitittimen porttiin fa0/0
- Liitä A-Access-kytkimen fa0/24-portti Branch-reitittimen fa0/0-porttiin
- Ota A-Access-kytkimeltä VLAN:t ja trunk-port-asetukset pois
- Ota tässä vaiheessa kaikilta verkkolaitteilta QoS-asetukset ja luokittelu pois käytöstä. (Älä poista niitä!)
- Vaihda Computer A:n, Computer C:n ja Server X:n IP-asetukset

Reitittimet ja PPP

Etätoimipisteelle muodostettava yhteys kulkee PPP-linkin ylitse. Tee tarvittavat asetukset molempiin reitittimiin

- Tee virtuaalisen PPP-liitännän alle seuraavat toimenpiteet
    - luo virtuaalinen liitäntä 1
    - määrittele kaistanleveydeksi 128 kbps
    - aseta IP-osoite
- Määrittele fyysisen liitännän asetukset
    - linkitä luomasi virtuaalinen PPP-liitäntä tähän fyysiseen liitäntään
    - aseta kapseloinniksi PPP
    - määrittele kaistanleveydeksi 128 kbps
    - aseta kellotaajuudeksi 128000
- Toteuta yksinkertainen reititys haluamallasi tavalla (RIP tai staattiset reitit)
- Aseta ethernet-portteihin IP-osoitteet

Testaa yhteyden toiminta ping-pakettien avulla.

Tarkistuslista:

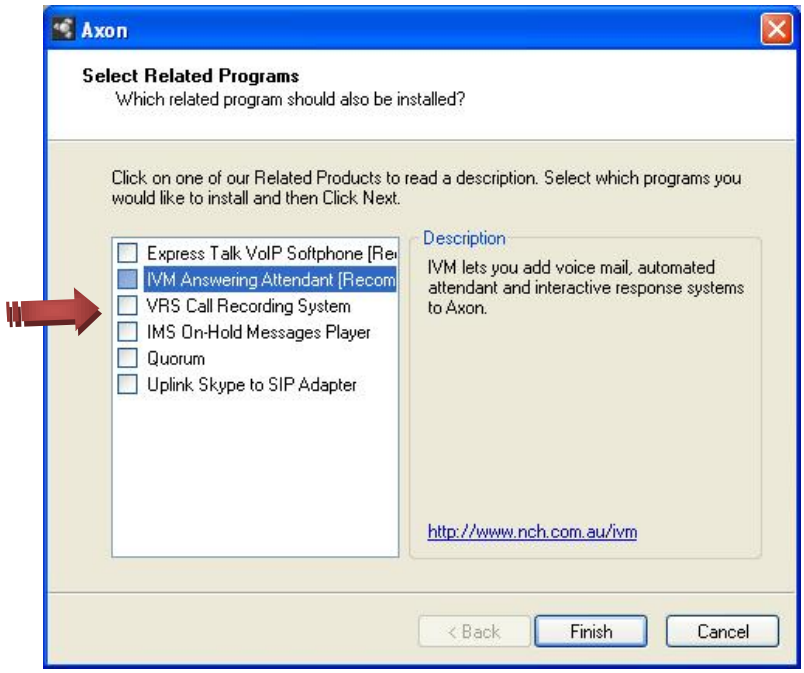
- VLAN-taulukot
- kaapelointi
- liitännät ylhäällä
- reititystauluissa kaikki tarvittavat verkot

2. IP-PUHELINVAIHDE (SIP-PALVELIN)

Oikeassa verkkoympäristössä VoIP-puheluita täytyy pystyä ohjaamaan myös oman sisäverkon ulkopuolelle julkisiin puhelinnumeroihin. Ääniliikennettä voidaan kontrolloida monella eri tavalla. Harjoituksessa käydään läpi ääniliikenteen ohjaus puhelinpalvelimen avulla. Puhelinpalvelimena toimii normaaleissa puhelinverkoissa yleisesti käytössä olevan PBX-puhelinvaihteen IP-sovellutus. Puhelinpalvelin ohjaa VoIP-puheluiden kulkua. Liitos ISDN- tai PSTN-verkkoon toteutetaan ääniyhdyskäytävällä (VoIP gateway). Käytämme harjoituksessa ainoastaan puhelinpalvelinta. Sen avulla VoIP-puhelujen ohjaus voidaan hoitaa keskitetysti yhdestä paikasta. Liitosta julkiseen verkkoon ei toteuteta. Ohjelmana käytämme Express Talk:in tekijöiden toista ilmaista sovellusta nimeltä Axon virtual PBX.

SIP-palvelimen asennus

Nouda tarvittava sovellus osoitteesta http://www.nch.com.au/pbx/ tai CCNP-kurssin verkkosivuilta https://www.wpk.tpu.fi/A4121_CCNP/tavaraa/ccnp3/. Asenna ja tee tarvittavat asetukset ohjelmaan seuraavien ohjeiden avulla.



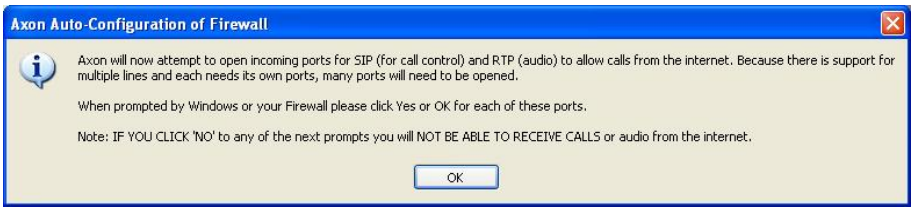
Kuva 2: Axon Virtual PBX – Ohjelmakonponenttien valitseminen

Ensimmäisenä hyväksy lisenssiehdot. Tämän jälkeen ohjelma kysyy, mitä ohjelmakomponentteja haluat asentaa SIP-palvelimen lisäksi. Et tarvitse harjoitustehtävän suorittamiseen mitään tarjottavista lisäominaisuuksista. Poista valinta kaikista kohdista ja jatka asennusta.

Kuva 3: Axon Virtual PBX – Pääkäyttäjätunnukset

Valitaan sisäisten IP-puhelinnumeroiden määrä, jonka ohjelma luo oletusasetuksiin. Aseta määräksi 0, koska haluamme luoda ne itse. Ohjelmistoa hallinnoidaan Web-käyttöliittymällä, ja tätä varten määritellään pääkäyttäjän käyttäjätunnus ja salasana. Arvot voivat olla tehtävässä admin admin.

Kuva 4: Axon Virtual PBX – Ohjelma avaa tarvitsemansa portit



Kuva 5: Axon Virtual PBX – Ohjelma avaa tarvitsemansa portit 2

Kuva 6: Axon Virtual PBX – Ohjelmaa avaa portin 8000

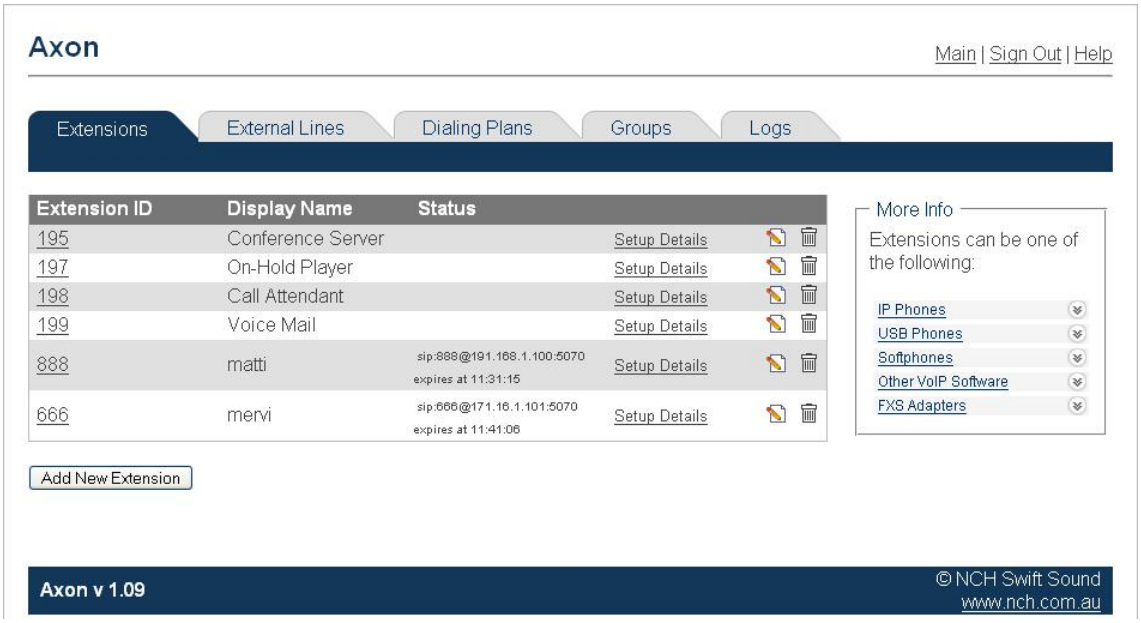
Kuva 7: Axon Virtual PBX – Ohjelma avaa portin 5060

Kuva 8: Axon Virtual PBX – Ohjelma avaa Web-liittymän portit

Ohjelman asennettua se yrittää vielä aukaista palomuurista portteja, joita se käyttää toiminnoissaan. Kuvien 4-8 mukaiset ikkunat avautuvat ruudulle ja ilmoittavat ongelmista porttien avaamisessa. Jos käytössäsi on palomuuri, hyväksy porttien avaaminen. Muuten voit painaa ilmestyviin ikkunoihin No-valinnan. Harjoitusympäristössä ei tulisi käyttää palomuuria, koska se saattaa luoda ongelmatilanteita joihinkin osiin harjoitusta. SIP-palvelin käyttää tiedonvälitykseen porttia 5060. Tämä tulee muistaa huomioida liikennettä luokitellessa.

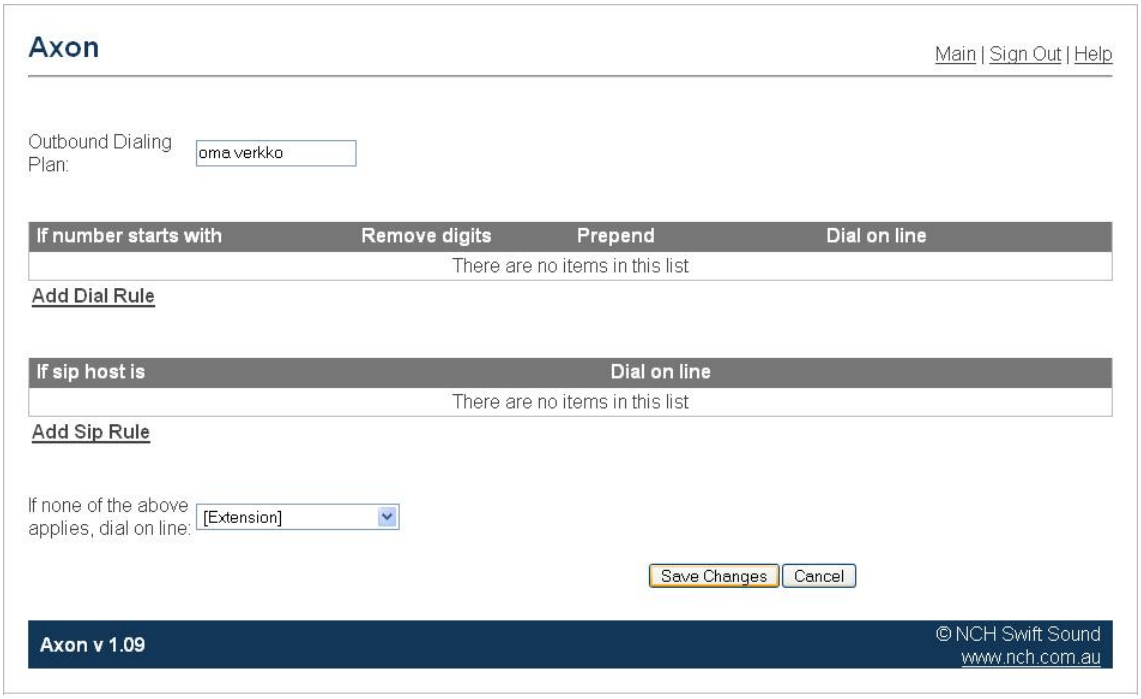
Kuva 9: Axon Virtual PBX – Web-liittymään siirtyminen

Axonin kaikki asetukset tehdään Web-käyttöliittymän avulla. Siirry sinne seuraavaksi.



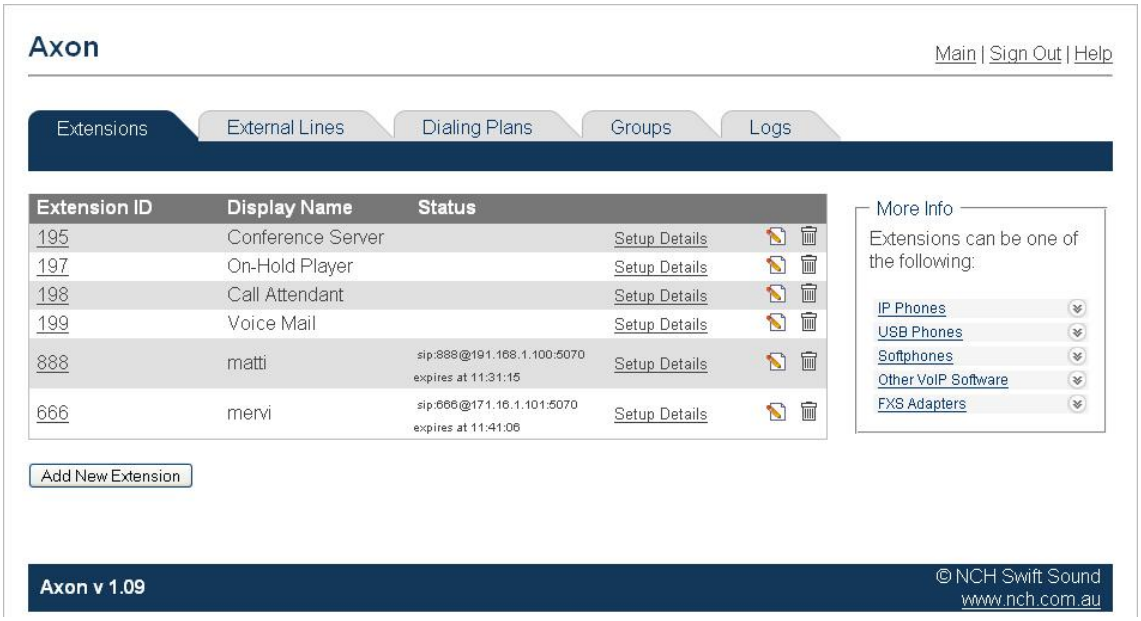
Kuva 10: Axon Virtual PBX – Käyttöliittymä

Syötettyäsi pääkäyttäjätunnuksen pääset hallinnointiasetuksiin käsiksi. Paina Extension-linkkiä. Axonin käyttöliittymä näyttää kuvan 10 kaltaiselta. Ylhäällä olevien välilehtien takaa löytyvät kaikki asetusvaihtoehdot. Ohjelma teki asennusvaiheessa joitakin oletusasetuksia järjestelmään. Ohjelmalle tarvitsee määritellä käytettävä sisäverkko, käyttäjät, soittoryhmät ja puhelujen ohjauksen määritykset. Ensimmäisenä luomme oman soittosuunnitelman, joka määrittelee, kuinka äänipuhelut ohjautuvat verkossa. Mene Dialing Plans -välilehdelle ja klikkaa Add New Outbound Dialing Plan -painiketta luodaksesi oman soittosuunnitelman. Anna sille nimeksi ”oma verkko”.



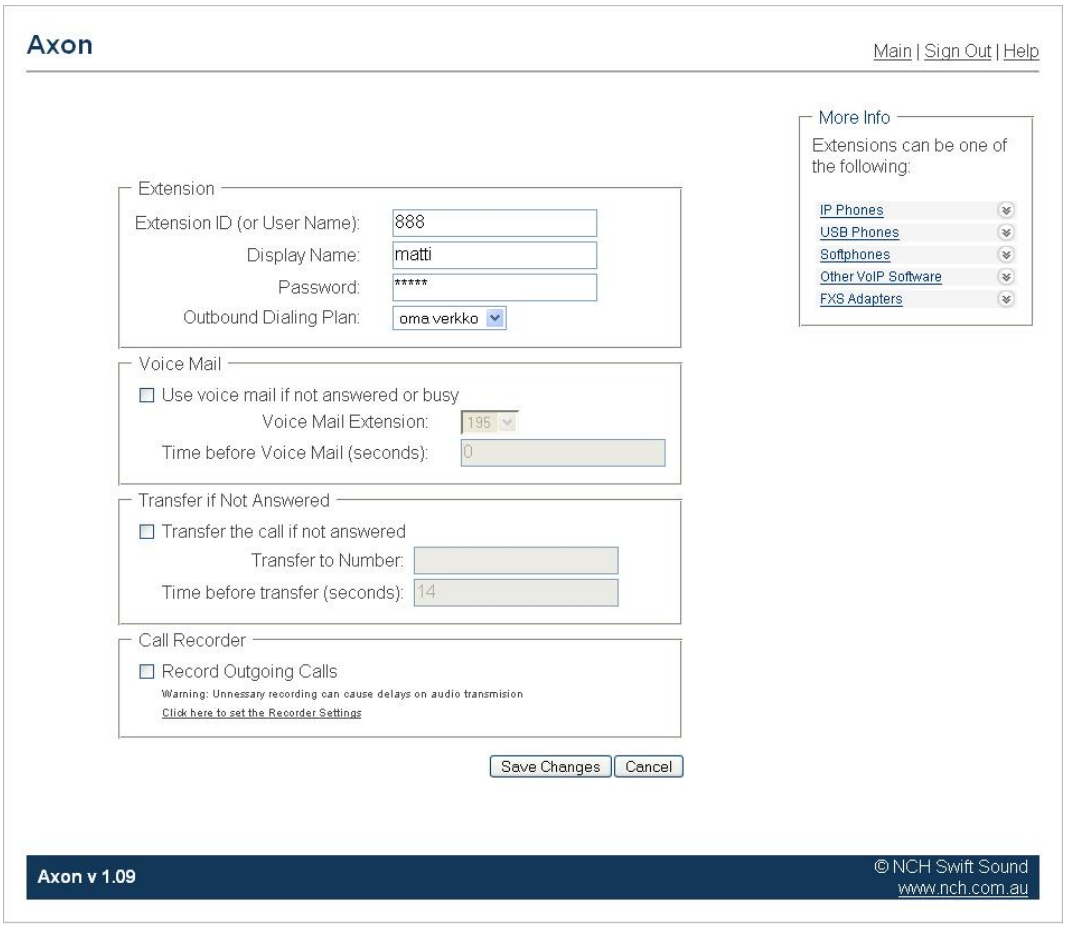
Kuva 11: Axon Virtual PBX – Soittosuunnitelma

Tee kuvan 11 mukaiset määritykset ja tallenna soittosuunnitelma. Mene Extension-välilehdelle.



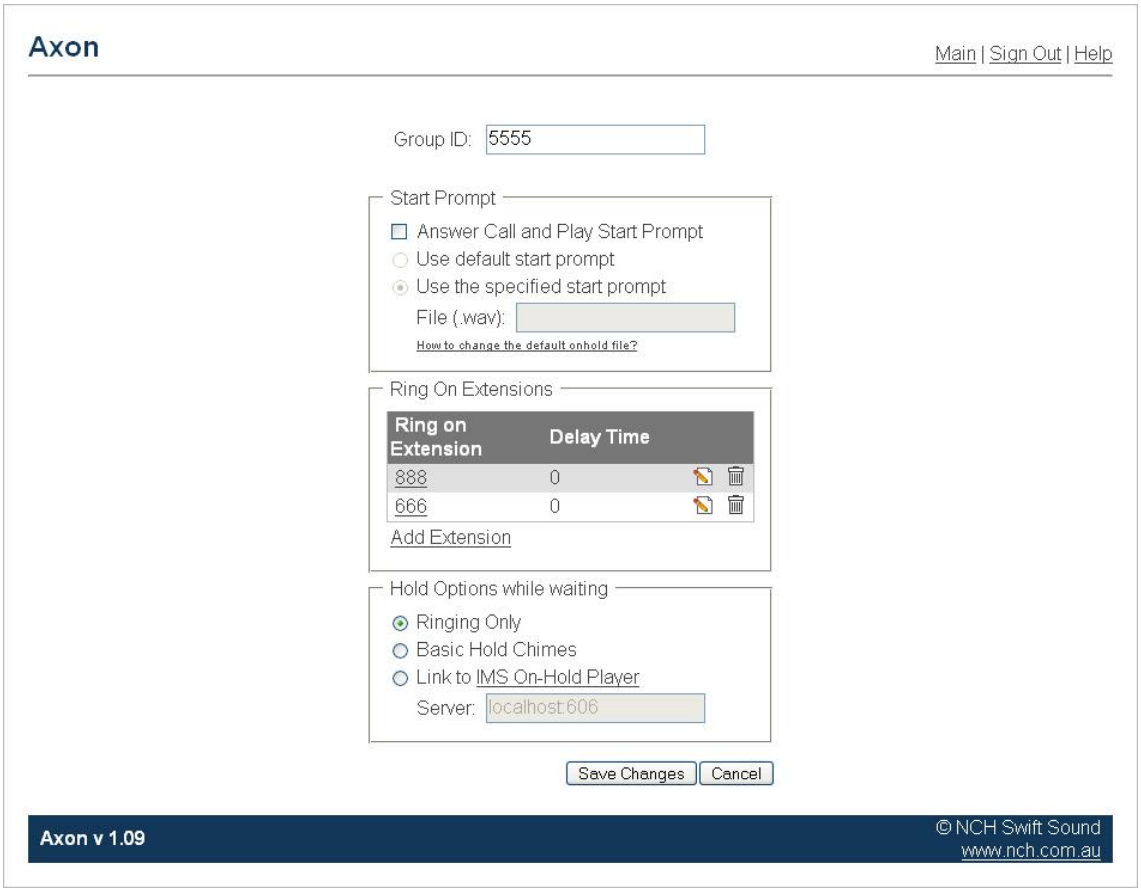
Kuva 12: Axon Virtual PBX – Käyttäjät ja muut liitokset

Extension-välilehdellä näkyy kaikki palvelimeen kytketyt käyttäjät sekä muut verkon VoIP-komponentit. Seuraavaksi luodaan kuvassa 12 näkyvät kaksi alinta käyttäjää. Paina Add New Extension -nappia.



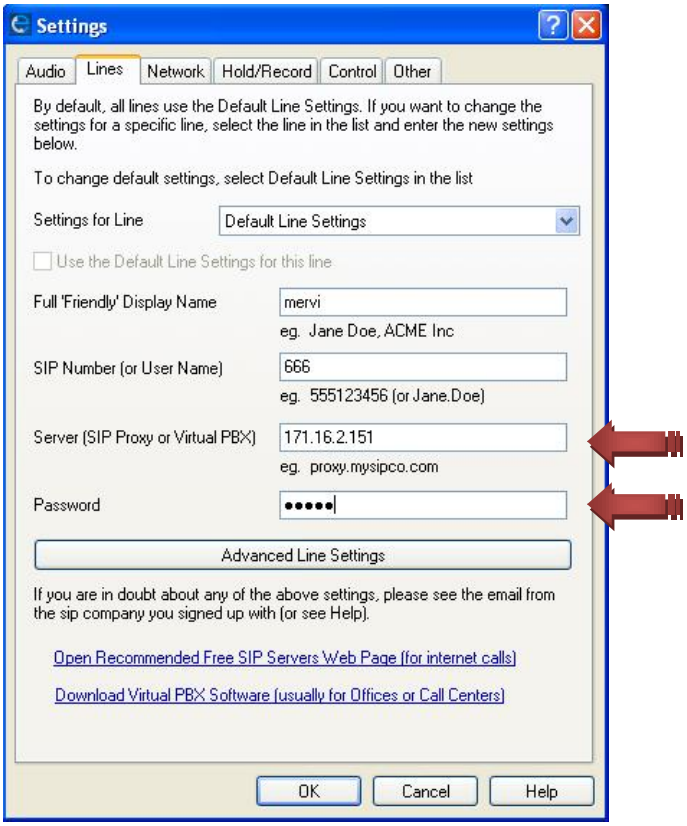
Kuva 13: Axon Virtual PBX – Käyttäjän luominen

Tee kuvan 13 mukaiset asetukset ja tallenna ne. Salasanana voidaan käyttää käyttäjän nimeä. Tee myös käyttäjä mervi. Kuvassa 12 esiintyvien käyttäjien tulisi ilmaantua Extension-välilehdelle. Nämä kaksi käyttäjää liitetään vielä samaan ryhmään. Luo ryhmä Groups-välilehden alla sijaitsevasta Add New Group or Queue -painikkeesta. Anna ryhmälle ID 5555.



Kuva 14: Axon Virtual PBX – Soittajaryhmän luonti

Tee kuvan 14 mukaiset asetukset ryhmälle ja tallenna asetukset. Asetukset ovat valmiit puhelujen soittamiseen SIP-palvelimen osalta, mutta Softphone-sovellukset täytyy vielä asettaa käyttämään luomaamme palvelinta. Käynnistä Express Talk, ja tee sinne seuraavien ohjeiden mukaiset asetusmuutokset.



Kuva 15: Express Talk – SIP-tilin asetukset

Aseta Computer A:lle ja Computer B:lle kuvan 15 osoittamaan kohtaan SIP-palvelimen IP-osoite ja käytettävä salasana. Salasana on Axonissa annettu salasana kyseiselle tilille. Pääset valikkoon Talk -> Options… -> Lines-välilehti.

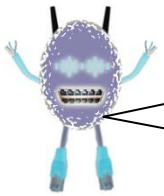
Testaa IP-puhelujen toimivuus verkossa. Soittamiseen käytät ainoastaan SIP-numeroa. Testaa samalla myös puhelun häiriötön ja hyvälaatuinen toiminta.

Tämän jälkeen ruuhkauta verkko ftp-tiedonsiirrolla Server X:ltä Computer C:lle ja testaa IP-puhelun äänenlaadun heikkeneminen.

3. QOS-TOIMENPITEET VERKKOLAITTEILLE

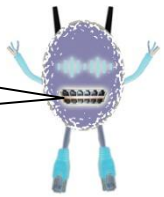
Koska aiemmissa harjoituksissa on opiskeltu liikenteen luokittelu ja Catalyst 2960 ja 3560 -verkkolaitteiden QoS-ominaisuudet ja niiden käyttäminen, voit tehdä nämä seuraavaksi itse harjoitukseen. Toteuta verkkoon luokittelu ja QoS-käsittely Catalyst 2960 ja 3560 -kytkimille. Reitittimien asetukset tehdään ohjatusti myöhemmässä vaiheessa. Tee toimet alla olevien määreiden mukaisesti.

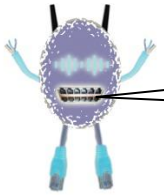
- Käytä harjoituksessa 2 suunnittelemaasi luokittelua, mutta lisää siihen SIP-palvelimen käyttämä porttinumero 5060, ja liitä se äänensignalointiluokkaan.
- Voit käyttää kytkimissä harjoituksessa 2 olleita QoS-konfiguraatioita sellaisenaan. Sinun täytyy vain miettiä tarkkaan, mihin asetukset tulee asettaa.



Mihin liitäntään ja millä laitteilla asetit ulostuloportin QoS-asetukset voimaan?

Missä kohtaa verkossa menee luottamusraja? Missä luokittelu tapahtuu?





Missä porteissa ja millä laitteille tulee asetettuihin pakettien luokittelumerkintöihin luottaa?

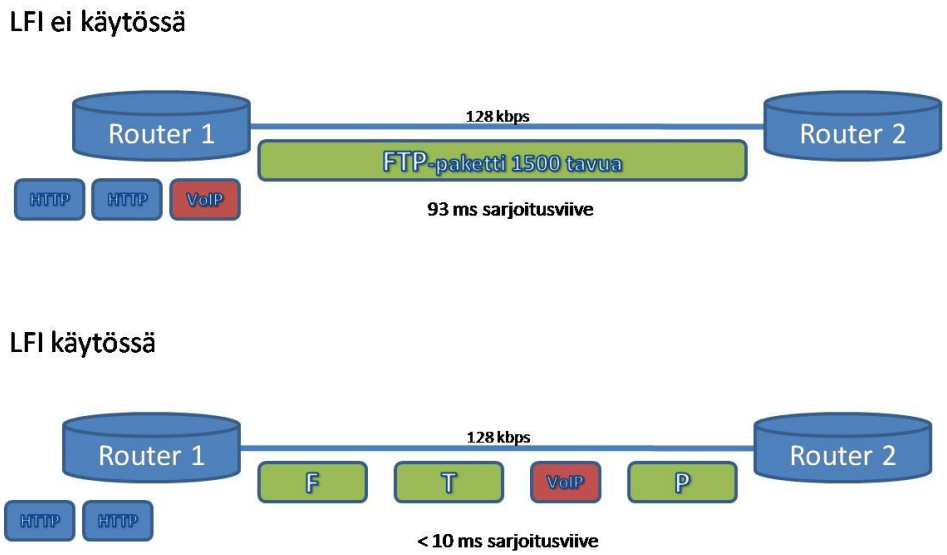
PPP-linkin QoS-asetukset

Seuraavaksi olisi tarkoitus varmistaa ääniliikenteen häiriötön kulku PPP-linkin ylitse. Linkin nopeus on 128 kbps ja siinä liikkuu maksimissaan 3 yhtäaikaista puhelua. Harjoituksessa kaistasta jaetaan 70 kbps ääniliikenteelle, 8 kbps äänensignalointiliikenteelle, 16 kbps tärkeälle data-liikenteelle ja loput jäävät muun verkkoliikenteen käyttöön. Huomio tulisi kiinnittää seuraaviin PPP-linkin VoIP-ominaisuuksiin:

- suurien pakettien aiheuttamat viiveet
- riittävän kaistan varaaminen ääniliikenteelle
- kaistan tehokas käyttö
- ruuhkatilanteen jonotuskäsittely

(Harjoituksessa ei tehdä QoS-asetuksia sisääntuloliitäntöihin reitittimien osalta)

Suuret paketit aiheuttavat ongelmia hitaissa yhteyksissä, koska niiden vieminen rajapintaan kestää suhteellisen kauan. Tämä tarkoittaa sitä, että muut paketit odottavat jonoissa koko tämän ajan. Tästä syystä ensimmäisenä täytyy varmistaa, että äänipaketit eivät joudu odottelemaan isojen pakettien takana. PPP-yhteyksissä voidaan käyttää MLP-LFI:tä eli Multilink PPP - Link Fragmentation and Interleaving -ominaisuutta ratkaisemaan ongelmaa. Isojen pakettien paloitteleminen maksimissaan 10 ms viiveen omaaviin paketteihin on ensisijaisen tärkeää. PPP-linkissä täytyy myös määritellä, että kun isompia paketteja pilkotaan pienemmiksi, saa isojen pakettien osien välissä lähettää myös toisia paketteja (*interleaving*). Kuva 16 esittää LFI:n toimintaa.



Kuva 16: LFI:n toiminta

Tee seuraavien ohjeiden avulla QoS-toimet molempiin reitittimiin. Sovella ohjeita oman suunnitelmasi luokitteluun sopivaksi.

- Tee virtuaalisen PPP-liitännän alle seuraavat toimenpiteet

(config-if)# ppp multilink fragment-delay 10	*määrittele paloiteltujen pakettien yksittäisten palasten (fragment) välisen lähetysvälin 10 millisekunniksi*
(config-if)# ppp multilink interleave	*sallii isojen pakettien palasten väliin toisen liikenteen pakettien lähettämisen (interleaving)*

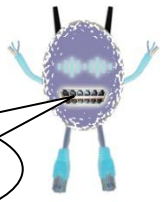
- Ota QoS-toimet käyttöön

(config)# class-map match-all VOICE-TRAFFIC	*luodaan luokkakartta VOICE-TRAFFIC*
(config-cmap)# match ip dscp 46	*liitetään siihen liikenne DSCP-arvolla 46*
(config)# class-map match-all VOICE-SIGNALING	*luodaan luokkakartta VOICE-SIGNALING*
(config-cmap)# match ip dscp 24	*liitetään siihen liikenne DSCP-arvolla 24*
(config)# class-map match-all PRIORITY-DATA-TRAFFIC	*luodaan luokkakartta PRIORITY-DATA-TRAFFIC*
(config-cmap)# match ip dscp 16	*liitetään siihen liikenne DSCP-arvolla 16*
(config)# policy-map CONGESTION-MANAGEMENT	*luodaan politiikka VOICE-POLICY*
(config-pmap)# class VOICE-TRAFFIC	*liitetään siihen luokkakartta VOICE-TRAFFIC*
(config-pmap-c)# priority 70	*määritetään sen liikenne prioriteettijonoon ja taataan kaistaa 70 kbps*
(config-pmap)# class VOICE-SIGNALING	*liitetään politiikkaan luokkakartta VOICE-SIGNALING*
(config-pmap-c)# bandwidth 8	*määrittää liikenteelle 8 kbps kaistaa käyttöön*
(config-pmap)# class PRIORITY-DATA-TRAFFIC	*liittää politiikkaan luokkakartan PRIORITY-DATA-TRAFFIC*
(config-pmap-c)# bandwidth 16	*määrätään siihen kuuluvalle liikenteelle 16 kbps kaistaa käyttöön*
(config-pmap)# class class-default	*muu liikenne kohdistuu default-luokkaan*
(config-pmap-c)# fair-queue	*muu liikenne saa flow-WRED käsittelyn*

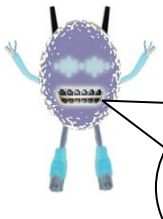
- Otetaan ruuhkankäsittelytoimenpiteet käyttöön virtuaalisessa PPP-liitännässä

(config-if)# service-policy output CONGESTION-MANAGEMENT

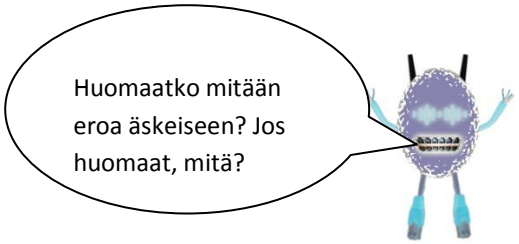
Testaa uudestaan ruuhkaisen verkon toiminta äänipuhelun osalta. Voit testata QoS-toimien vaikutusta äänipuhelun laatuun välillä poistamalla CONGESTION-MANAGEMENT-politiikan ja välillä uudelleen aktivoimalla sitä PPP-linkin molemmissa päissä. Pidä ftp-yhteys koko ajan auki.



Sulje VoIP-yhteys. Lähetä seuraavaksi jatkuvana lähetyksenä 60 tavun ping-lähetystä Computer B:ltä Computer A:lle. Se kuvaa ääniliikenteen paketteja. Pidä ftp-yhteys edelleen päällä.



Ota LFI pois toiminnasta.



4. LOPUKSI

Olet suorittanut kolme harjoitusta liittyen liikenteen luokitteluun ja VoIP-liikenteen priorisointiin. Aluksi opit luokittelemaan liikennettä OSI:n 2- ja 3-kerroksella. Tämän jälkeen opit käyttämään Softphone-ohjelmaa ja streaming-sovellusta. Tehtäväjoukon vaikein osuus oli Catalyst 2960 ja 3560 -kytkinten QoS-asetuksien ymmärtäminen ja niiden konfigurointi. Viimeisenä asiana opit SIP-palvelimen käyttöönoton perusteita ja PPP-yhteyden QoS-asetusten tekemistä. On huomioitava, että harjoituksissa esiintyneet konfigurointi-asetukset olivat suunniteltu harjoitusverkkoon, eivätkä ne ole suoraan sovellettavissa tuotantoympäristöön. Harjoituksessa esiin tulleet palvelun laadun varmistamiseen esitetyt ratkaisut olivat vain yksi mahdollinen ratkaisukeino. Ratkaisuvaihtoehtoja olisi toki ollut runsaasti muitakin.

Lisää tietoa harjoituksissa läpikäydyistä tekniikoista saat tämän harjoitussarjan tuottamiseen liittyneestä opinnäytetyöstä. Työ tulee saataville TAMKin kirjastoon kevään 2007 aikana. Löydät sen tietojenkäsittelyn koulutusohjelman töiden joukosta tekijänä Jesse Laamanen.