Atte Silventoinen

LÄHI- JA REITITINVERKOT

Opinnäytetyö
Tietotekniikan koulutusohjelma

Maaliskuu 2012

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

Opinnäytetyön päivämäärä
9.3.2012

Tekijä(t)
Silventoinen Atte Petteri

Koulutusohjelma ja suuntautuminen
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Nimeke

Lähi- ja reititinverkot

Tiivistelmä

Tämän opinnäytetyön tavoitteena on perehtyä muutamiin lähi- ja reititinverkkojen kannalta oleellisiin tekniikoihin ja protokolliin sekä luoda verkkosimulaatio, jossa hyödynnetään näitä ratkaisuja. Aihepiirin laajuuden vuoksi käsiteltäviä asioita on jouduttu rajaamaan melko paljon. Esimerkiksi verkkojen tietoturva ja langattomat verkkoratkaisut on jätetty käsittelyn ulkopuolelle.

Tietoliikennealan kirjallisuuden pohjalta käsiteltäviä aiheita ovat OSI- ja TCP/IP-malli, Ethernet, IP-, TCP-, UDP- ja DHCP-protokolla, osoitteenmuunnos, lähiverkkotopologiat, verkkolaitteet, virtuaalilähiverkot, IP-reititys, RIP-, EIGRP- ja OSPF-reititysprotokolla, HDLC- ja PPP-protokolla sekä Frame Relay- ja ATM-tekniikka. Verkkosimulaatio toteutetaan Cisco Packet Tracer -ohjelman avulla. Kytkimien ja reitittimien asetusten määrittelyssä käytetään Cisco IOS -käyttöjärjestelmän komentoriviä.

Simuloitavalle verkolle suunnitellaan IP-osoitteistus ja kytkimiin tehdään virtuaalilähiverkkomääritykset. Reitittimet määritellään hoitamaan virtuaalilähiverkkojen välinen reititys, käyttämään OSPF-reititysprotokollaa ja toimimaan DHCP-palvelimina. Lisäksi yksi reititin asetetaan suorittamaan osoitteenmuunnosta. Reitittimien välisille yhteyksille otetaan käyttöön PPP-protokolla. Kaikki halutut ominaisuudet saadaan määritetyksi toimintakuntoon ilman ongelmia.

Asiasanat (avainsanat)

TCP/IP, Ethernet, lähiverkot, reitittimet

Sivumäärä	**Kieli**	**URN**
47	Suomi	

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi
Matti Juutilainen

Opinnäytetyön toimeksiantaja

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

Date of the bachelor's thesis

9 March 2012

Author(s)
Silventoinen Atte Petteri

Degree programme and option
Information Technology

Name of the bachelor's thesis

Local Area Networks and Router Networks

Abstract

The goal of this bachelor's thesis was to deal with some technologies and protocols which are important in the operation of local area networks and router networks. This was achieved by writing about these topics with the help of the literature focusing on networking and creating a network simulation. Since the subject was very extensive only selected topics were discussed. Topics excluded from this bachelor's thesis were, for example, network security and wireless networks.

The topics discussed in this bachelor's thesis involved OSI and TCP/IP models, Ethernet, IP, TCP, UDP, DHCP, NAT, local area network topologies, networking devices, VLANs, IP routing, RIP, EIGRP, OSPF, HDLC, PPP, Frame Relay and ATM. The network simulation was implemented with the Cisco Packet Tracer program. The switches and routers were configured by using the Cisco IOS command line interface.

Creating the network simulation included planning an IP addressing for the network and configuring VLANs, inter-VLAN routing, OSPF, DHCP, NAT and PPP. All these features were configured without problems.

Subject headings, (keywords)

TCP/IP, Ethernet, Local Area Networks, routers

Pages	**Language**	**URN**
47	Finnish	

Remarks, notes on appendices

Tutor	**Bachelor's thesis assigned by**
Matti Juutilainen	

LYHENTEET

ARPANET	Advanced Research Projects Agency Network
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BDR	Backup Designated Router
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Control Identifier
DNS	Domain Name System
DR	Designated Router
EIGRP	Enhanced Interior Gateway Routing Protocol
FCS	Frame Check Sequence
FTP	File Transfer Protocol
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
LAN	Local Area Network
LCP	Link Control Protocol
LLC	Logical Link Control
LSP	Link State Packet
MAC	Media Access Control
NAT	Network Address Translation
NCP	Network Control Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAT	Port Address Translation
PPP	Point-to-Point Protocol
RIP	Routing Information Protocol
SDLC	Synchronous Data Link Control
SFD	Start of Frame Delimiter
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Shielded Twisted Pair
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPI	Virtual Path Identifier
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

SISÄLTÖ

1 JOHDANTO

Tietoliikenteellä ja tietoverkoilla on hyvin suuri merkitys nykypäivän yhteiskunnassa. Tieto- ja tietoliikennetekniikan hyödyntäminen tehostaa lukemattomien yritysten ja muiden organisaatioiden toimintaa sekä helpottaa myös yksittäisen kansalaisen arkisia askareita. Monesti ihmiset pysähtyvätkin miettimään, miten ennen tultiin toimeen ilman tekniikkaa, jonka olemassaolo tuntuu nykyään niin itsestään selvältä. Tietoliikennetekniikan kehitys on ollut viime vuosikymmeninä hyvin nopeaa. Uusien tekniikoiden kehittäminen ja vanhojen parantaminen jatkuu edelleen taukoamatta.

Tämän opinnäytetyön tavoitteena on perehtyä tietoliikennetekniikkaa käsittelevän kirjallisuuden pohjalta muutamiin lähi- ja reititinverkkojen kannalta oleellisiin tekniikoihin ja protokolliin sekä luoda verkkosimulaatio, jossa hyödynnetään näitä ratkaisuja. Aihepiirin laajuuden vuoksi käsiteltäviä asioita on jouduttu rajaamaan melko paljon. Esimerkiksi verkkojen tietoturva ja langattomat verkkoratkaisut on jätetty käsittelyn ulkopuolelle. Opinnäytetyö on tehty Mikkelin ammattikorkeakoulussa syksyn 2011 ja alkuvuoden 2012 aikana.

Toisessa luvussa esitellään tietoliikenneverkkojen toiminnan kuvaamisessa hyvin yleisesti käytetyt OSI- ja TCP/IP-malli sekä useita merkittäviä tietoliikennetekniikoita ja -protokollia, kuten Ethernet, IP, TCP, UDP, DHCP ja osoitteenmuunnos. Kolmannessa luvussa perehdytään lähiverkkoihin. Aluksi luodaan katsaus erilaisiin lähiverkon topologioihin ja verkkolaitteisiin, minkä jälkeen paneudutaan virtuaalilähiverkkoihin.

Neljännessä luvussa edetään lähiverkon ulkopuolelle reitittimien välisiin verkkoihin. Ensin esitellään IP-reitityksen yleisiä periaatteita ja erityyppisiä reititysprotokollia, minkä jälkeen otetaan lähempään tarkasteluun yleiset reititysprotokollat RIP, EIGRP ja OSPF. Tämän jälkeen tarkasteluvuoroon tulevat vielä laajaverkkoprotokollat HDLC, PPP, Frame Relay ja ATM.

Viidennessä luvussa esitellään verkkosimulaatio-ohjelman avulla toteutettu verkko, joka hyödyntää monia aikaisemmissa luvuissa esiteltyjä tekniikoita ja protokollia. Tämän esimerkkiverkon simuloimiseen käytetään Cisco Packet Tracer -ohjelmaa ja se pohjautuu Ciscon kytkimiin ja reitittimiin. Kuudennessa luvussa esitetään vielä lyhyt yhteenveto koko opinnäytetyön tuloksista.

2 OSI, TCP/IP JA PROTOKOLLIA ERI KERROKSILTA

2.1 OSI- ja TCP/IP-malli

OSI-mallia (Open Systems Interconnection) käytetään hyvin yleisesti tietoliikenneverkkojen toiminnan kuvaamisessa. OSI-mallin mukaisia verkkoja ei käytännössä ole, mutta sen tunteminen auttaa hahmottamaan verkon eri toiminnallisuuksien roolia koko verkon toiminnassa. TCP/IP-malli (Transmission Control Protocol / Internet Protocol) on puolestaan luotu kuvaamaan TCP/IP-protokollaperheeseen perustuvan tietoliikenneverkon toimintaa. /1, s. 126 ja 145–147./

OSI-mallin kehittäminen aloitettiin vuonna 1977 ja kansainvälinen standardointijärjestö ISO (International Organization for Standardization) hyväksyi sen vuonna 1983. Kehitystyön tuloksena saatiin aikaan viitemalli, joka antaa perustan tietokoneiden väliselle tietoliikenteelle hajautetuissa tietojärjestelmissä. OSI-malli kehitettiin kerrosmalliksi, jossa alemmat kerrokset tarjoavat palveluitaan ylemmille kerroksille. /2, s. 7./

OSI-mallissa on seitsemän kerrosta (kuva 1), jotka ovat alhaalta ylöspäin lukien *fyysinen-, siirtoyhteys-, verkko-, kuljetus-, istunto-, esitystapa-* ja *sovelluskerros*. *Fyysinen kerros* (physical layer) käsittää käytettävän tiedonsiirtoyhteyden mekaaniset, fyysiset ja toiminnalliset ominaisuudet. Sen tehtävänä on muuntaa siirrettävä data käytettävälle tiedonsiirtoyhteydelle sopivaan muotoon, kuten sähköisiksi pulsseiksi, valoksi tai radiosignaaleiksi. /2, s. 8./

	OSI	TCP/IP	Protokollia
7	Sovelluskerros	Sovelluskerros	HTTP, FTP, Telnet, SMTP, DHCP
6	Esitystapakerros		
5	Istuntokerros	Kuljetuskerros	TCP, UDP
4	Kuljetuskerros		
3	Verkkokerros	Verkkokerros	IP
2	Siirtoyhteyskerros	Liittymäkerros	Ethernet, HDLC, PPP, Frame Relay, ATM
1	Fyysinen kerros		

KUVA 1. OSI- ja TCP/IP-mallin vertailu /3, s. 33/

Siirtoyhteyskerros (link layer) koostuu kahdesta kerroksesta, jotka ovat MAC (Medium Access Control) ja LLC (Logical Link Control). MAC varaa käytettävän tiedonsiirtoyhteyden tiedonsiirtoa varten ja LLC huolehtii siirtovirheiden havaitsemisesta ja niiden korjaamisesta sekä tietovuon hallinnasta. Tietovuon hallinta tarkoittaa sitä, että fyysiselle kerrokselle ei anneta siirrettäväksi sen siirtokykyä tai tiedon vastaanottajan vastaanottokykyä suurempaa määrää dataa. /2, s. 8./

Verkkokerros (network layer) luo tietoverkon yli ulottuvan yhteyden, joka ei ota kantaa verkon rakenteeseen ja kytkentätekniikkaan. Verkkokerroksen toiminnalle tärkeitä palveluja ovat esimerkiksi DNS- (Domain Name System) ja ARP-palvelut (Address Resolution Protocol*)*. DNS huolehtii laitteiden nimien muuntamisen niiden loogisiksi osoitteiksi. ARP puolestaan huolehtii laitteiden loogisten osoitteiden muuntamisen niiden fyysisiksi osoitteiksi. Oleellinen osa verkkokerroksen toimintaa on myös reititys. Reitityksen avulla siirrettävä data kulkee parasta reittiä lähettäjän ja vastaanottajan välillä. Reititys usein myös optimoi verkon eri osien käyttöä tasaamalla käytettävissä oleviin reittivaihtoehtoihin kohdistuvaa kuormaa. /2, s. 8–9./

Kuljetuskerros (transport layer) tarjoaa joko yhteydellisen tai yhteydettömän tiedonsiirtoyhteyden lähettäjän ja vastaanottajan välille. Yhteydellisen yhteyden muodostaminen sisältää aina tiedonsiirtoyhteyden avaamisen ja sulkemisen. Yhteydellisen yhteyden tarkoitus on taata siirrettävän datan virheettömyys ja datan saapuminen vastaanottajalle samassa järjestyksessä kuin se on lähetetty. Yhteydetöntä yhteyttä käytetään puolestaan silloin, kun siirrettävän datan virheettömyys sekä yhteyden avaaminen ja sulkeminen eivät ole tiedonsiirron kannalta oleellisia seikkoja. Esimerkki yhteydellisestä protokollasta on vaikkapa TCP (Transmission Control Protocol) ja yhteydettömästä UDP (User Datagram Protocol). /2, s. 9./

Istuntokerros (session layer) huolehtii sovellusten välisistä ohjaustoiminnoista, kuten yhteyden muodostamisesta, siirtoyhteyspalvelun varaamisesta, yhteyteen liittyvien ominaisuuksien sopimisesta osapuolten välillä, yhteyden varmistamisesta tarkistuspisteillä, yhteyden päättämisestä ja resurssien vapauttamisesta. *Esitystapakerroksessa* (presentation layer) sovitaan yhteisestä tiedon esitystavasta päätelaitteiden välille ja *sovelluskerros* (application layer) toimii sovellusten ja OSI-mallin rajapintana. /2, s. 10./

OSI-malli ei ole yleistynyt käytännön tasolla kovinkaan paljon. Sen standardointi oli hidasta ja sen pohjalta kehitetyt järjestelmät olivat monimutkaisia ja vaikeaselkoisia, mikä johti helposti yhteensopivuusongelmiin. OSI-mallia on moitittu myös liian hienojakoisesta kerrosten erottelusta. OSI-malli onkin jäänyt käyttöön lähinnä siksi, että sen avulla on helppo kuvata erilaisia tietoliikenneverkkoja. /4, s. 14./

TCP/IP-protokollaperheen juuret ulottuvat Yhdysvaltojen puolustusministeriön 1960-luvulla käynnistämään ARPANET-hankkeeseen (Advanced Research Projects Agency Network). ARPANET-verkkoa käytettiin aluksi tutkimuslaitosten, korkeakoulujen ja sotilasviranomaisten väliseen tietoliikenteeseen. Verkon käyttö laajeni kuitenkin nopeasti ja sen pohjalta syntyi lopulta nykymuotoinen Internet. Samalla TCP/IP-protokollaperhe saavutti merkittävän asemansa nykypäivän tietoliikenteessä. /1, s. 142–143./

TCP/IP-protokollaperhe koostuu useista eri tehtäviä hoitavista protokollista. Keskeinen osa tätä perhettä on verkkokerroksen IP-protokolla, jonka alapuolella liittymäkerroksella voidaan käyttää hyvin monenlaisia tekniikoita ja protokollia. Kuljetuskerroksen toiminnoista vastaavat TCP ja UDP. /5, s. 22./

TCP/IP-mallissa on neljä kerrosta, jotka ovat alhaalta ylöspäin lukien *liittymäkerros, verkkokerros, kuljetuskerros* ja *sovelluskerros*. *Liittymäkerros* vastaa toiminnoiltaan OSI-mallin kahta alinta kerrosta. Se määrittelee tavan, jolla laite liittyy verkkoon. /2, s. 6./

Verkkokerroksen tehtävänä on hoitaa siirrettävien datapakettien välittäminen koko verkon yli lähettäjältä vastaanottajalle. TCP/IP-mallin *kuljetuskerros* puolestaan vastaa OSI-mallin kuljetuskerrosta. TCP/IP-verkoissa yhteydelliseen tiedonsiirtoon käytetään TCP-protokollaa ja yhteydettömään tiedonsiirtoon UDP-protokollaa. *Sovelluskerroksen* tunnetuimpia protokollia ovat puolestaan muun muassa FTP (File Transfer Protocol), Telnet ja SMTP (Simple Mail Transfer Protocol). /2, s. 6–7./

2.2 Ethernet

Ethernet on kaikkein yleisin lähiverkkoratkaisu. Se syntyi alun perin Digitalin, Intelin ja Xeroxin kehitystyön tuloksena vuonna 1980. Vuonna 1983 IEEE (Institute of Elect-

rical and Electronics Engineers) julkaisi tämän työn pohjalta suosituksen 802.3. Pian sen jälkeen julkaistiin jo suositus IEEE 802a, joka kuvaa verkon toiminnan 50 ohmin koaksiaalikaapelilla. /2, s. 262./

Vuonna 1987 kahden toistimen välinen maksimietäisyys kasvoi jopa 1 000 metriin IEEE 802.3d -suosituksen myötä. Kyseinen suositus kuvaa toistimien välisen optisen runkolinjan. Vuonna 1990 ilmestyi suositus IEEE 802.3i, joka kuvaa Ethernetin toiminnan parikaapeliyhteyksillä. Suosituksen myötä käyttöön tuli tähtitopologia, jossa parikaapelit kytketään keskittimeen. Vuonna 1993 optisten kuitujen avulla laitteiden väliset maksimietäisyydet kasvoivat jopa 2 000 metriin. /2, s. 262./

Vuonna 1995 Ethernetin nopeus kasvoi IEEE 802.3u -suosituksen myötä 10 megabitistä 100 megabittiin sekunnissa ja vuonna 1997 IEEE 802.3x -suosituksen myötä käyttöön tuli kaksisuuntainen (full duplex) toimintamuoto. Kaksisuuntaisen toimintamuodon ansiosta perinteinen CSMA/CD-kanavanvaraus (Carrier Sense Multiple Access with Collision Detection) alkoi käydä tarpeettomaksi ja Ethernet-verkot alkoivat kehittyä väylistä kohti kaksipisteyhteyksien joukkoja. /2, s. 262–263./

Vuonna 1998 suositus IEEE 802.3z toi mukanaan Gigabit Ethernetin. Tämä tarkoitti verkon nopeuden kasvamista 1 000 megabittiin sekunnissa. Vuonna 2001 IEEE 802.3ae -suositus puolestaan nosti nopeuden jo 10 gigabittiin sekunnissa. /2, s. 263./

IEEE 802.3 -kehyksen rakenne

IEEE 802.3 -kehyksen (kuva 2) osat ovat *alkutahdistus* (preamble), *SFD* (Start of Frame Delimiter), *vastaanottajan osoite* (Destination Address), *lähettäjän osoite* (Source Address), *sanoman pituus, hyötykuorma* ja *FCS* (Frame Check Sequence). 56-bittinen *alkutahdistus* lukitsee vastaanottajan tahdistuksen sisään tulevaan bittivirtaan ja *SFD* on tavun mittainen binaarikoodi 10101011. /2, s. 264./

Pituus tavuina	7	1	6	6	2	enintään 1500	4
Kenttä	alkutahdistus	SFD	DA	SA	pituus	hyötykuorma	FCS

KUVA 2. IEEE 802.3 -kehyksen rakenne /2, s. 264/

Vastaanottajan osoite ja *lähettäjän osoite* ovat laitteiden fyysiset osoitteet eli MAC-osoitteet (Media Access Control). MAC-osoite on yleensä 48-bittinen ja koostuu neljästä eri osasta (kuva 3), jotka ovat *Individual/Group* (bitti 0), *Universal/Local* (bitti 1), *OUI* (bitit 2–23) ja *vapaa numerointi* (bitit 24–47). /2, s. 264–265./

Bitti	0	1	2-23	24-47
Kenttä	I/G	U/L	OUI	vapaa numerointi

KUVA 3. MAC-osoitteen rakenne /2, s. 265/

Kun *Individual/Group*-bitti on nolla, on kyseessä suora osoite ja kun se on yksi, on kyseessä ryhmäosoite (multicast address). Kun *Universal/Local*-bitti on nolla, on kyseessä yleinen IEEE:n myöntämä osoite ja kun se on yksi, on kyseessä paikallisesti annettu osoite. *OUI* puolestaan on laitevalmistajan ilmaiseva merkintä ja *vapaa numerointi* laitevalmistajan vapaavalintaisesti päättämä arvo. /2, s. 265./

Sanoman pituus IEEE 802.3 -kehyksessä ilmaisee sanoman pituuden alkaen vastaanottajan osoitteesta ja päättyen hyötykuorman viimeiseen tavuun. *Hyötykuorma* on nimensä mukaisesti IEEE 802.3 -kehyksen sisältämä verkon ylemmältä kerrokselta peräisin oleva hyötydata. IEEE 802.3 -kehys kykenee kuljettamaan enimmillään 1 500 tavua hyötykuormaa. Kehyksen päättää lopulta *FCS*, joka on CRC-periaatteella (Cyclic Redundancy Check) laskettu kehystarkiste. /2, s. 266./

Vuonna 1998 esiteltiin IEEE 802.3ac -laajennus (kuva 4), joka toi mukanaan neljän tavun pituisen tyyppi, prioriteetti ja VLAN -tunnisteen, joka sijoitetaan lähettäjän osoitteen ja sanoman pituuden väliin. Tämän ansiosta samalla yhteydellä voidaan siirtää useiden virtuaalilähiverkkojen tietoliikennettä, sillä kyseisen tunnisteen avulla Ethernet-kehykset voidaan ohjata omiin virtuaalilähiverkkoihinsa. Näin eri työryhmien tietoliikenteen siirtämiseen voidaan käyttää samaa siirtotietä tietoturvallisuuden siitä oleellisesti kärsimättä. IEEE 802.3ac toi mukanaan myös mahdollisuuden priorisoida Ethernet-tietoliikennettä. /2, s. 267./

Pituus tavuina	7	1	6	6	4	2	enintään 1500	4
Kenttä	alkutahdistus	SFD	DA	SA	tunniste	pituus	hyötykuorma	FCS

KUVA 4. IEEE 802.3 -kehys 802.3ac -laajennuksella /2, s. 267/

CSMA/CD

Ethernet-verkot perustuivat alun perin väylätopologiaan ja CSMA/CD-tekniikkaan (Carrier Sense Multiple Access with Collision Detection). Kun laitteiden välinen etäisyys väylämuotoisessa verkossa kasvaa, kasvaa samalla myös niiden välinen siirtoviive. Tällöin kaikki laitteet eivät välttämättä havaitse, onko jokin toinen laite jo aloittanut tiedon lähettämisen verkossa, koska kyseinen lähetys ei ole vielä saavuttanut jokaista verkon laitetta. Tällaisissa tilanteissa laite voi tulkita verkon vapaaksi ja aloittaa oman lähetyksensä, joka törmää jo aikaisemmin lähetyksen aloittaneen laitteen lähetyksen kanssa. Törmäys aiheuttaa sen, että jännitteet summautuvat ja lähetetyt signaalit vääristyvät. /2, s. 269–270./

Kun laite havaitsee lähettämässään signaalissa vääristymiä, se lopettaa sen lähetyksen ja lähettää verkkoon 32-bittisen jam-signaalin, joka ilmoittaa kaikille muillekin laitteille törmäyksen tapahtuneen. Törmäyksien havaitsemisen edellytys on, että jokainen laite ehtii havaita lähettämäänsä signaaliin vaikuttaneen törmäyksen sinä aikana, kun lähetys on vielä käynnissä. Muuten laite vain toteaisi lähetyksen loputtua sen onnistuneen, vaikka siihen voisi myöhemmin kohdistua vielä törmäys. Tämän vuoksi on tärkeää, että lähetettävän sanoman minimipituus on mitoitettu oikein laitteiden välisen etäisyyden ja verkon tiedonsiirtonopeuden suhteen. /2, s. 270–272./

Törmäyksen takia epäonnistuneet lähetykset on luonnollisesti uusittava jossain vaiheessa. Uudelleenlähetyksen ajankohta valitaan satunnaisuuden kautta. Aluksi muodostetaan kaksi samanpituista aikaväliä, joista toisen alku valitaan uudelleenlähetyksen ajankohdaksi. Jos lähetys päättyy taas törmäykseen, aikavälejä muodostetaan neljä, minkä jälkeen niistä valitaan taas satunnaisesti yksi. Lisäämällä jatkuvasti aikavälien määrää pienennetään samalla törmäyksen todennäköisyyttä. Yhden aikavälin pituus vastaa signaalin edestakaista siirtoviivettä pisimmällä mahdollisella yhteydellä. /2, s. 272./

Väylätopologiasta tähtitopologiaan

Väylätopologiaa käyttävässä Ethernet-verkossa kaikkien verkon laitteiden lähettämä tietoliikenne näkyy kaikissa muissa verkon laitteissa. Verkkoa on myös hankala ylläpitää, jos sen koko kasvaa suureksi ja jopa yhden väylään liitetyn laitteen vioittuminen voi haitata merkittävästi koko verkon toimintaa. Väylämuotoisten Ethernet-verkkojen kaapeloinnissa käytetään koaksiaalikaapelia. /2, s. 273./

Parikaapeloinnin yleistymisen myötä Ethernet-verkoissa alettiin käyttää tähtitopologiaa. Tähtitopologiassa verkon eri laitteiden parikaapelit kytkettiin keskittimeen. Vaikka topologia muuttuikin, verkko toimi edelleen väylän tavoin. Kaikki verkon tietoliikenne näkyi edelleen kaikissa verkon laitteissa ja verkossa oli yhä törmäyksiä. /2, s. 273./

Yleislähetys- ja törmäysalueet

Kun tähtitopologiassa keskitin korvataan kytkimellä, verkko voidaan jakaa osiin, joiden tietoliikenne ei ole nähtävillä muissa verkon osissa. Verkkoon voidaan nähdä syntyvän *yleislähetysalueita* (broadcast domain) ja *törmäysalueita* (collision domain). /2, s. 274./

Yleislähetysalueen muodostavat kaikki laitteet, jotka vastaanottavat toistensa lähettämiä yleislähetyssanomia. Verkon aktiivilaitteet, kuten kytkimet, välittävät yleislähetyssanomia eteenpäin kaikista porteistaan, ellei niiden välitystä rajoiteta. Liiallinen yleislähetyssanomien määrä voi aiheuttaa yleislähetyssanomien myrskyn (broadcast storm), joka voi huonontaa merkittävästi verkon suorituskykyä. /2, s. 274./

Törmäysalueen puolestaan muodostavat kaikki ne laitteet, jotka havaitsevat verkossa tapahtuvan törmäyksen. Kaikki samaan kaapeliin tai keskittimeen liitetyt laitteet havaitsevat verkossa tapahtuvat törmäykset, mutta kytkimen avulla saadaan muodostettua yksi törmäysalue jokaisen kytkimeen liitetyn laitteen ja kytkimen portin välille. Törmäysalueiden koolla on suuri vaikutus verkon suorituskykyyn. /2, s. 274./

Täsmälähetys, yleislähetys ja ryhmälähetys

Ethernet-verkon eri tietoliikennetyyppejä ovat *täsmälähetys* (unicast), *yleislähetys* (broadcast) ja *ryhmälähetys* (multicast). *Täsmälähetyksessä* Ethernet-kehyksellä on vain yksi tietty vastaanottaja, jonka MAC-osoite ilmaistaan kehyksen osoitetiedoissa. *Yleislähetyksessä* puolestaan kehyksen vastaanottavat kaikki Ethernet-verkon laitteet. Yleislähetyskehyksen voi tunnistaa siitä, että sen vastaanottajan MAC-osoitteen kaikki bitit ovat ykkösiä. Heksadesimaalimuodossa ilmaistuna kyseinen osoite on siis FF-FF-FF-FF-FF-FF. /6, s. 332–333./

Ryhmälähetyksen avulla laite voi lähettää kehyksen tietylle vastaanottajien joukolle. Jotta laite voisi vastaanottaa ryhmälähetyskehyksiä, on sen suoritettava ohjelmaa tai palvelua, joka määrittää sen vastaanottamaan niitä. Ryhmälähetyksiin tarkoitetut MAC-osoitteet alkavat aina heksadesimaaliarvolla 01-00-5E. Osoitteen seuraavat 23 bittiä saadaan lähetykseen käytettävän IP-osoitteen 23:sta vähiten merkitsevästä bitistä. Viimeinen bitti puolestaan on aina nolla. /6, s. 333–334./

STP ja link aggregation

Laajojen Ethernet-verkkojen suorituskykyä ja vikasietoisuutta parantamaan kehitettyjä tekniikoita ovat muun muassa *STP* (Spanning Tree Protocol) ja *link aggregation*. *STP* on verkon aktiivilaitteiden protokolla, joka sulkee verkossa esiintyvät tarpeettomat yhteydet ja näin ollen estää sanomien tarpeettoman kiertämisen niiden muodostamissa silmukoissa. STP osaa kuitenkin ottaa sulkemiaan yhteyksiä uudelleen käyttöön, jos jokin alkuperäisistä yhteyksistä lopettaa jostain syystä toimintansa. /2, s. 278./

Koska STP ei salli kuormantasausta kahden eri yhteyden välillä, julkaistiin suositus IEEE 802.3ad, joka mahdollistaa yhden loogisen yhteyden muodostamisen useista rinnakkaisista yhteyksistä. Tästä käytetään nimitystä *link aggregation*. Yhden loogisen yhteyden muodostaminen saavutetaan MAC-kerroksen yläpuolelle sijoitettavan niin sanotun Link Aggregation Layerin ansiosta. Se käyttää alla olevia siirtoyhteyksiä normaaliin tapaan erillisinä, mutta näyttää ne ylemmille kerroksille yhtenä siirtoyhteytenä ja MAC-osoitteena. /2, s. 278–279./

Ethernetin fyysiset toteutukset

Ethernet-verkkojen fyysistä toteutusta kuvataan siten, että ensimmäisenä mainitaan kyseessä olevan ratkaisun nimellisnopeus. Seuraavaksi ilmaistaan, toimiiko ratkaisu kantataajuus- (Base) vai laajakaistaperiaatteella (Broad) ja lopuksi annetaan kaapelointia kuvaava koodi. Esimerkiksi merkintä 10Base-T tarkoittaa kantataajuusperiaatteella toimivaa parikaapeliratkaisua, jonka nimellissiirtonopeus on kymmenen megabittiä sekunnissa (taulukko 1). /2, s. 280./

TAULUKKO 1. Ethernet-verkon fyysisiä toteutuksia /6, s. 343/

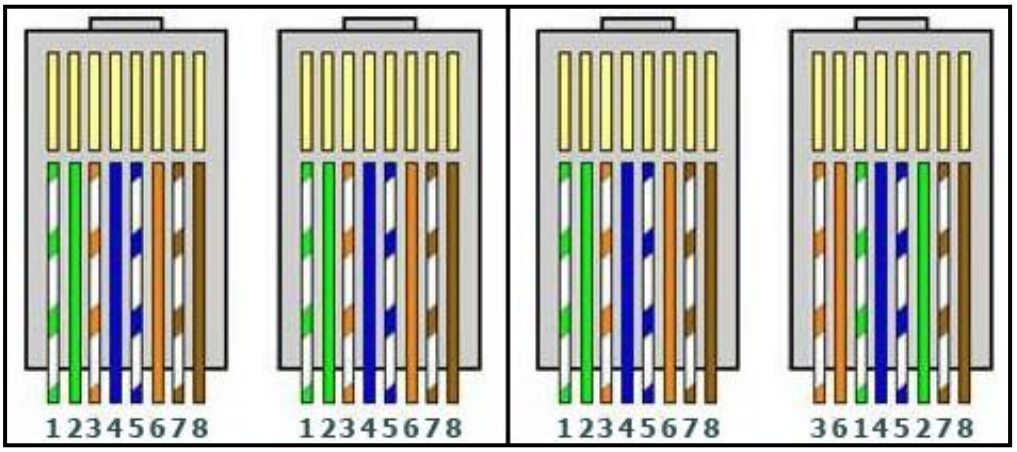
Ratkaisu	**Siirtonopeus**	**Kaapeli**	**Enimmäispituus (m)**
10Base-5	10 Mb/s	paksu koaksiaali	500
10Base-2	10 Mb/s	ohut koaksiaali	185
10Base-T	10 Mb/s	Cat 3 / Cat 5 UTP	100
100Base-TX	100 Mb/s	Cat 5 UTP	100
100Base-FX	100 Mb/s	moni-/yksimuotokuitu	400/2 000
1000Base-T	1 Gb/s	Cat 5e UTP	100
1000Base-TX	1 Gb/s	Cat 6 UTP	100
1000Base-SX	1 Gb/s	monimuotokuitu	550
1000Base-LX	1 Gb/s	yksimuotokuitu	2 000
10GBase-T	10 Gb/s	Cat 6a / Cat 7 UTP	100
10GBase-LX4	10 Gb/s	monimuotokuitu	300
10GBase-LX4	10 Gb/s	yksimuotokuitu	10 000

10Base-5 on vanhin Ethernet-ratkaisu. Siinä käytetään siirtotienä koaksiaalikaapelia. Koodi 5 tarkoittaa suurinta mahdollista verkon segmentin pituutta, joka on 500 metriä. 10Base-2-ratkaisussa siirtotienä käytetään myös koaksiaalikaapelia. Tässä ratkaisussa se on kuitenkin ohuempaa ja verkon segmentin maksimipituus on noin 200 metriä. /2, s. 281–282./

TAULUKKO 2. Parikaapeleiden kaapeliluokat /3, s. 160/

Luokka	Siirtonopeus	Johdinparien lkm	Käyttökohteita
Cat 1	< 1 Mb/s	2	Analoginen data, POTS, ISDN
Cat 2	4 Mb/s	2	Token Ring -verkot
Cat 3	16 Mb/s	4	Ääni/data, 10Base-T, puhelinliikenne
Cat 4	20 Mb/s	4	Token Ring -verkot
Cat 5	100 Mb/s - 1 Gb/s	4	10Base-T, 100Base-T, Gigabit Ethernet, ATM, FDDI
Cat 5e	100 Mb/s	4	ATM, FDDI
Cat 6	> 100 Mb/s	4	Laajakaistaverkot
Cat 6e	10 Gb/s	4	Gigabit Ethernet
Cat 7	1,2 Gb/s	4	Gigabit Ethernet

10Base-T käyttää siirtotienä parikaapelia. Parikaapeliksi kelpaa luokan Cat 3 parikaapeli (taulukko 2), mutta suositeltavaa olisi kuitenkin käyttää luokan Cat 5 parikaapelia. Päätelaitteen ja verkkolaitteen välisen kaapelin pituus saa olla enintään noin 92 metriä. Kahden päätelaitteen kytkeminen keskenään onnistuu puolestaan ristikytketyllä parikaapelilla (kuva 5). Suojaamattomien UTP-parikaapeleiden (Unshielded Twisted Pair) lisäksi Ethernet-verkoissa käytetään myös maadoitetulla metalliverkolla suojattuja STP-parikaapeleita (Shielded Twisted Pair). /2, s. 282; 4, s. 39–40./



KUVA 5. Suorakytketyn (vasen) ja ristikytketyn parikaapelin johtimet kaapeleiden eri päissä /7/

Myös 100Base-TX käyttää siirtotienään parikaapelia. Parikaapelin johdinpareista on käytössä kaksi ja kaapelin luokan on oltava vähintään Cat 5. 100Base-TX-yhteydet ovat aina kaksipisteyhteyksiä ja tuettuina ovat sekä vuoro- että kaksisuuntainen liikenne. 100Base-FX on puolestaan valokuitua siirtotienään käyttävä ratkaisu. Käytet-

tävä valokuitu voi olla joko moni- tai yksimuotokuitua. Vuorosuuntaisessa liikenteessä yhteyden maksimipituus on noin 412 metriä ja kaksisuuntaisessa liikenteessä noin 2 000 metriä. /2, s. 285./

1000Base-LX ja 1000Base-SX ovat lasertekniikkaan perustuvia joko moni- tai yksimuotokuitua käyttäviä ratkaisuja. Näillä ratkaisuilla yhteyksien pituudet voivat maksimissaan olla monimuotokuidulla noin 550 metriä ja yksimuotokuidulla jopa 5 000 metriä. 1000Base-CX puolestaan käyttää twinax-kaapelointia. Tätä ratkaisua käytetään lyhyiden yhteyksien toteuttamisessa. Kaapelin maksimipituus onkin vain 25 metriä. 1000Base-T käyttää parikaapelin jokaista neljää johdinparia kaksisuuntaisesti. Tämä ratkaisu vaatii luokan Cat 5 parikaapelin. /2, s. 288–289./

10GBase-ratkaisujen myötä Ethernet-tekniikkaa alettiin hyödyntää lähiverkkojen lisäksi myös laajaverkoissa (Wide Area Network). 10GBase-ratkaisut tukevat ainoastaan kaksisuuntaista liikennettä ja kaikki yhteydet ovat kaksipisteyhteyksiä, joten CSMA/CD-kilpavarausta ei tarvita. Valokuitua hyödyntäviä 10GBase-ratkaisuja ovat esimerkiksi 10GBase-SR, 10GBase-LR ja 10GBase-ER. 10GBase-SR kykenee 300 metrin, 10GBase-LR 10 kilometrin ja 10GBase-ER 40 kilometrin yhteyksiin. 10GBase-T perustuu puolestaan parikaapelin käyttöön ja mahdollistaa 100 metrin yhteyden. /2, s. 289–291./

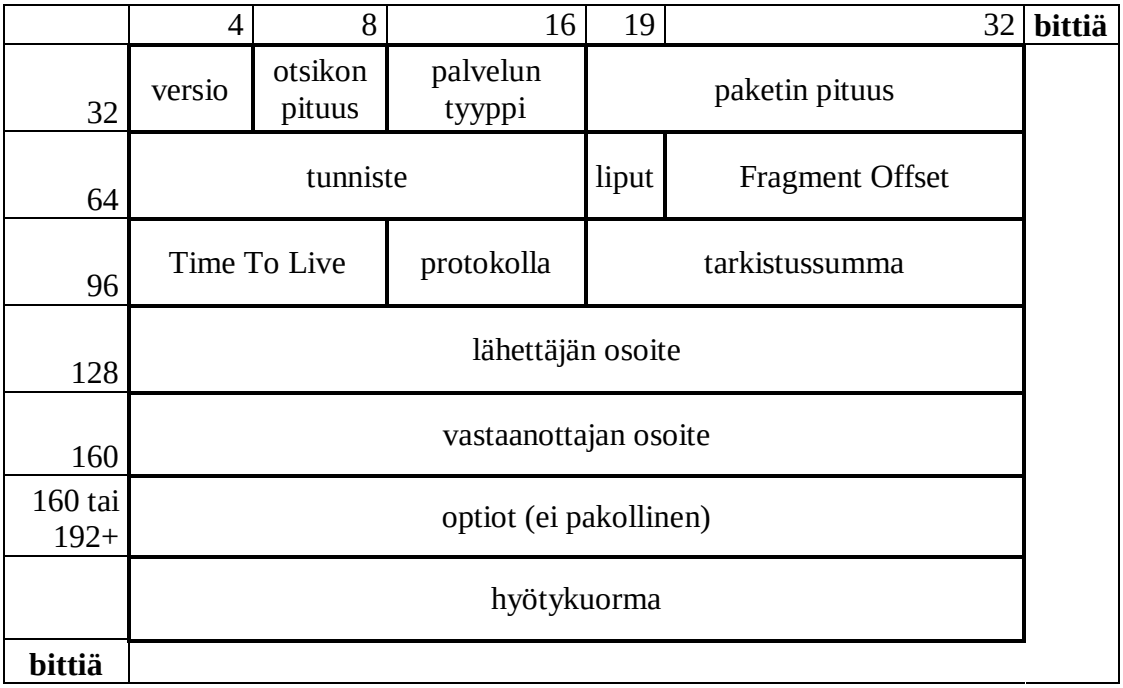
2.3 IP

IP-protokollasta (Internet Protocol) on käytössä kaksi eri versiota, jotka ovat IPv4 (Internet Protocol version 4) ja IPv6 (Internet Protocol version 6). IPv4-osoitteet ovat 32-bittisiä ja ne koostuvat neljästä kahdeksan bitin oktetista. Näin ollen jokainen oktetti voi saada kymmenlukujärjestelmällä tarkasteltuna arvokseen luvun 0–255. IPv4-osoitteita on yhteensä 4 294 967 296 kappaletta, mikä on liian vähän nykymaailman tarpeisiin nähden. /3, s. 478./

IPv4-osoitteiden liian pienen määrän vuoksi kehitetty korvaava IPv6-protokolla on yleistynyt hitaasti, joten IPv4 on vielä hyvin yleisesti käytössä. IPv6-osoitteet ovat peräti 128-bittisiä ja IPv6 sisältää myös joukon muita uudistuksia, jotka liittyvät esimerkiksi tietoliikenteen priorisointiin ja tietoturvaan. IPv6:n vuoksi monista eri protokollista on kehitetty IPv6-yhteensopivia versioita. /6, s. 235–236./

IPv4-paketin rakenne

IPv4-paketin (kuva 6) osat ovat *versio, otsikon pituus, palvelun tyyppi, paketin pituus, tunniste, liput, Fragment Offset, Time To Live, protokolla, tarkistussumma, lähettäjän osoite, vastaanottajan osoite, optiot* ja *hyötykuorma*. *Versio* kertoo, onko kyse IPv4- vai IPv6-paketista. *Otsikon pituus* ilmoittaa otsikkotietojen kokonaispituuden ja *palvelun tyyppi* sisältää tietoa, jota voidaan käyttää tietoliikenteen luokittelussa ja priorisoinnissa. /3, s. 487–489./



KUVA 6. IPv4-paketin rakenne /3, s. 489/

Paketin pituus kertoo koko paketin pituuden ja *tunnisteen* avulla tunnistetaan yhteen kuuluvat pilkotut paketit. *Lipuilla* puolestaan ilmaistaan, voidaanko pakettia pilkkoa ja onko kyseinen paketti pilkotuista paketeista viimeinen. *Fragment Offset* kertoo pilkottujen pakettien alkuperäisen järjestyksen. /3, s. 487./

Time To Live (TTL) ilmoittaa, kuinka monta kertaa paketin voi vielä reitittää eteenpäin. TTL-arvoa pudotetaan jokaisen reitityspäätöksen kohdalla yhdellä ja kun se on nolla, reititin hylkää paketin ja lähettää tästä ilmoituksen paketin lähettäjälle. *Protokolla* kertoo paketin sisältämän ylemmän kerroksen protokollatyypin. Esimerkiksi arvo kuusi ilmoittaa paketin sisältämäksi protokollaksi TCP:n ja seitsemäntoista UDP:n. /3, s. 487–488./

Tarkistussumma kertoo paketin otsikkotietojen virheettömyyden. Reititin vertaa itse laskemaansa tarkistussummaa paketin alkuperäiseen tarkistussummaan. Jos se havaitsee niissä eroavaisuuden, paketti hylätään. *Lähettäjän osoite* ja *vastaanottajan osoite* sisältävät kyseiset IPv4-osoitteet. *Optioiden* avulla voidaan tehdä erilaisia lisämäärityksiä. Ne voidaan jättää kokonaan pois, jos niitä ei tarvita. *Hyötykuorma* sisältää lopulta paketin kuljettaman hyötydatan. /3, s. 488./

IPv4-osoitteet

IPv4-osoitteissa on kaksi osaa, jotka ovat verkko-osa ja laiteosa (kuva 7). Aliverkon peitteen tehtävänä on määrittää, kuinka monta eniten merkitsevää bittiä osoitteesta kuuluu verkko-osaan. Verkkokerroksen näkökulmasta laitteet, joiden IPv4-osoitteessa on samanlainen verkko-osa, kuuluvat samaan aliverkkoon. Laiteosalle jäävästä bittimäärästä puolestaan näkee helposti, kuinka paljon osoitteita aliverkossa on käytettävissä. /6, s. 174./

	Verkko-osa			**Laiteosa**
Osoite	192.	168.	1.	1
	1100 0000.	1010 1000.	0000 0001.	0000 0001
Aliverkon peite	255.	255.	255.	0.
	1111 1111.	1111 1111.	1111 1111.	0000 0000

KUVA 7. Aliverkon peitteen ykkösbitit määrittävät IPv4-osoitteen verkko-osan

Aliverkon peite on IPv4-osoitteen tapaan 32-bittinen ja se koostuu neljästä kahdeksan bitin oktetista. Sen eniten merkitsevistä biteistä tietty määrä on aina ykkösiä. Loput biteistä ovat puolestaan kaikki nollia. Ykkösten avulla ilmaistaan, että vastaava IPv4-osoitteen bitti kuuluu verkko-osaan. /6, s. 191./

IPv4-aliverkon ensimmäistä osoitetta kutsutaan verkon osoitteeksi. Kyseisessä osoitteessa kaikki laiteosan bitit ovat nollia ja sitä ei voida määrittää minkään aliverkon laitteen osoitteeksi. Aliverkkoja eriteltäessä niihin viitataan usein verkon osoitteen avulla. Osoite, jonka kaikki laiteosan bitit ovat ykkösiä, on puolestaan aliverkon yleislähetysosoite. Kaikki aliverkon laitteet vastaanottavat kyseiseen osoitteeseen lähetetyn paketin. Kaikki osoitteet aliverkon osoitteen ja yleislähetysosoitteen välillä ovat laiteosoitteita. Ne ovat vapaasti määriteltävissä aliverkon eri laitteille. /6, s. 188–189./

IPv4-osoitteet 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255 ja 192.168.0.0–192.168.255.255 ovat yksityisiä osoitteita. Ne on tarkoitettu käytettäviksi yksityisissä verkoissa. Jotta yksityiseen verkkoon kuuluva laite voisi kommunikoida julkisen verkon välityksellä, täytyy esimerkiksi yksityisen ja julkisen verkon rajalla olevan reitittimen suorittaa osoitteenmuunnos (Network Address Translation). Osoitteenmuunnoksessa yksityinen osoite korvataan julkisella osoitteella. /6, s. 192–193./

Täsmälähetys, yleislähetys ja ryhmälähetys

IPv4-verkossa on kolmenlaista tietoliikennettä. Niitä ovat *täsmälähetys* (unicast), *yleislähetys* (broadcast) ja *ryhmälähetys* (multicast). *Täsmälähetyksessä* lähettäjä lähettää dataa vain yhdelle laitteelle. Tällöin lähetettävään pakettiin merkitään vastaanottajan osoitteeksi kyseisen laitteen IPv4-osoite. /6, s. 183–184./

Yleislähetys on puolestaan tarkoitettu kaikkien aliverkon laitteiden vastaanotettavaksi. Jos laite haluaa lähettää yleislähetyspaketin omaan aliverkkoonsa, se merkitsee vastaanottajan osoitteeksi osoitteen, jonka kaikki bitit ovat ykkösiä. Kymmenlukujärjestelmän avulla esitettynä kyseinen osoite on 255.255.255.255. Jos laite haluaa jostain syystä suorittaakin johonkin toiseen aliverkkoon kohdistuvan yleislähetyksen, se merkitsee vastaanottajan osoitteeksi kyseisen aliverkon viimeisen osoitteen. /6, s. 184–186./

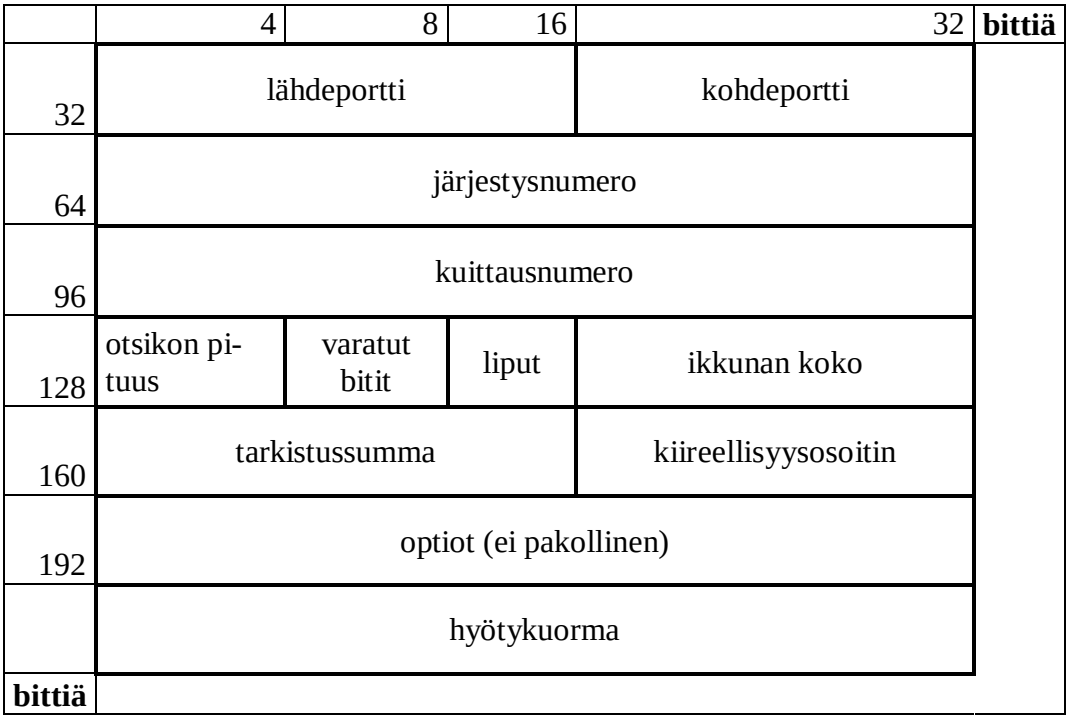
Ryhmälähetysten avulla paketti voidaan lähettää tietylle joukolle laitteita. Ryhmälähetyksiä vastaanottavissa laitteissa on käynnissä sovellus, joka määrittää ne vastaanottamaan tiettyyn ryhmälähetysosoitteeseen lähetetyt paketit. Ryhmälähetysosoitteita ovat IPv4-osoitteet 224.0.0.0–239.255.255.255. /6, s. 186–187./

2.4 TCP ja UDP

TCP-protokollaa (Transmission Control Protocol) käytetään, kun halutaan muodostaa luotettava tiedonsiirtoyhteys. TCP varmistaa, että lähetty data saapuu perille virheettömänä. Kaikissa tapauksissa, kuten äänen tai videokuvan siirrossa, ei kuitenkaan välttämättä aina tarvita täysin virheetöntä tiedonsiirtoa ja sen mukanaan tuomaa yhteyden hallintaan liittyvää ylimääräistä dataa. Tällöin UDP-protokolla (User Datagram Protocol) on parempi ratkaisu. /3, s. 455–456./

TCP-segmentin rakenne

TCP-segmentti (kuva 8) koostuu *lähdeportista, kohdeportista, järjestysnumerosta, kuittausnumerosta, otsikon pituuden määrityksestä, varatuista biteistä, lipuista, ikkunan koosta, tarkistussummasta, kiireellisyysosoittimesta, optioista ja hyötykuormasta. Lähdeportti* ja *kohdeportti* ovat numeroita, jotka kuvaavat, millaista ja millaiselle sovellukselle tarkoitettua dataa segmentti sisältää. *Järjestys-* ja *kuittausnumero* puolestaan liittyvät yhteyden hallintaan. *Järjestysnumero* ilmaisee segmentin hyötykuorman ensimmäisen tavun järjestysnumeron koko kyseisen TCP-yhteyden aikana siirrettyjen hyötytavujen joukossa ja *kuittausnumero* ilmaisee, mitä tavua vastaanottaja seuraavaksi tarvitsee. /3, s. 457–460./



KUVA 8. TCP-segmentin rakenne /3, s. 458/

Otsikon pituuden määritys varmistaa, että kaikkien TCP-segmenttien otsikko on yhtä pitkä. *Varatuilla biteillä* ei puolestaan ole mitään erityistä tehtävää, vaan ne asetetaan tavallisesti nolliksi. *Lippuja* on yhteensä kahdeksan. Ne liittyvät yhteyden hallintaan sekä ilmaisevat, ovatko muiden segmentin kenttien sisältämät tiedot merkityksellisiä. Yksi lippu esimerkiksi ilmaisee, milloin kuittausnumero on luettava. /3, s. 459./

Ikkunan koko antaa vastaanottajalle mahdollisuuden määritellä, kuinka suuren määrän dataa se on valmis vastaanottamaan ja *tarkistussummaa* käytetään tiedonsiirron aikana

vahingoittuneiden segmenttien havaitsemiseen. *Kiireellisyysosoitin* puolestaan ilmaisee eron nykyisen segmentin järjestysnumeron ja viimeisen kiireellisen tavun järjestysnumeron välillä. Tämän jälkeen TCP-segmentissä on vielä tilaa erilaisille *optioille* ja luonnollisesti *hyötykuormalle*. /3, s. 459–460./

TCP:n toimintaperiaate

TCP-tiedonsiirto aloitetaan luomalla virtuaalinen yhteys lähettäjän ja vastaanottajan välille. Yhteyttä voidaan kutsua virtuaaliseksi, sillä lähettäjän ja vastaanottajan välillä kulkevien IP-pakettien reitti voi vaihdella. Vastaanottaja ja lähettäjä tunnistetaan IP-osoitteiden ja porttinumeroiden perusteella. /3, s. 461./

Yhteyden muodostaminen tapahtuu kolmitiekättelyn avulla. Ensin lähettäjä lähettää vastaanottajalle TCP-segmentin, jossa SYN-lippu on asetettu aktiiviseksi. Tämän jälkeen vastaanottaja lähettää lähettäjälle segmentin, jossa SYN- ja ACK-lippu on asetettu aktiivisiksi. Seuraavaksi lähettäjä lähettää vastaanottajalle vielä segmentin, jonka ACK-lippu on asetettu aktiiviseksi. Tämän jälkeen TCP-yhteys on muodostettu. /3, s. 461./

Tiedonsiirron aikana vastaanotetut segmentit tallennetaan puskurimuistiin ja järjestetään oikeaan järjestykseen. Jos jotkin segmentit havaitaan puuttuviksi tai vahingoittuneiksi, niitä pyydetään uudelleenlähetettäviksi. Vastaanotetut hyötytavut kuitataan säännöllisesti segmenteillä, joiden ACK-lippu on asetettu aktiiviseksi. /3, s. 462./

TCP-yhteyden sulkeminen puolestaan tapahtuu niin, että ensin osapuoli A lähettää osapuolelle B segmentin, jossa FIN-lippu on asetettu aktiiviseksi. Tämän jälkeen B lähettää A:lle segmentin, jossa ACK-lippu on asetettu aktiiviseksi. Tämän seurauksena A sulkee yhteyden omalta osaltaan ja yhteys jää puoliavoimeen tilaan. Seuraavaksi B lähettää A:lle segmentin, jossa FIN-lippu on asetettu aktiiviseksi, minkä jälkeen A lähettää B:lle vielä segmentin, jossa ACK-lippu on asetettu aktiiviseksi. Tämä sulkee TCP-yhteyden lopullisesti. /3, s. 462./

UDP:n toimintaperiaate

UDP-protokolla luo tilattomia yhteyksiä. Se ei pyri takaamaan siirtämänsä tiedon virheettömyyttä. Vastaanottaja ei järjestä saapuneita UDP-datagrammeja oikeaan järjestykseen eikä välitä siitä, että kaikki lähetetyt datagrammit saapuvat perille asti. Tiedonsiirron kannalta UDP onkin huomattavasti nopeampi protokolla kuin TCP, mutta ei läheskään yhtä luotettava. /3, s. 467./

UDP-datagrammi (kuva 9) on paljon yksinkertaisempi TCP-segmenttiin verrattuna. Se sisältää vain lähdeportin, kohdeportin, tarkistussumman, datagrammin pituuden ja hyötykuorman. /3, s. 468./

KUVA 9. UDP-datagrammin rakenne /3, s. 468/

Porttinumerot

TCP:n tavoin myös UDP käyttää porttinumeroita tunnistaakseen, mille sovellukselle lähetetty data on tarkoitettu. Portit on jaettu *hyvin tunnettuihin, rekisteröityihin* ja *dynaamisiin tai yksityisiin portteihin*. Portit 0 – 1 023 ovat *hyvin tunnettuja portteja* ja ne ovat yleisimpien protokollien käytössä. Portit 1 024 – 49 151 ovat puolestaan *rekisteröityjä portteja* ja ne ovat valmistajiensa rekisteröimien sovellusten käytössä. Portit 49 152 – 65 535 sitä vastoin ovat *dynaamisia tai yksityisiä* eli ne ovat vapaasti käytettävissä. /3, s. 469./

2.5 DHCP

DHCP-protokollaa (Dynamic Host Configuration Protocol) käytetään verkkoasetusten automaattiseen määrittelyyn. Sen avulla laitteelle voidaan määritellä esimerkiksi IP-

osoite, aliverkon peite, oletusyhdyskäytävä ja käytettävät DNS-palvelimet. DHCP:n toiminta perustuu asiakas–palvelin-periaatteeseen. /5, s. 66–71./

DHCP-asiakas lähettää käynnistyessään yleislähetysosoitteeseen DISCOVER-sanoman. DISCOVER-sanoman vastaanottanut DHCP-palvelin vastaa siihen OFFER-sanomalla, joka sisältää palvelimen tarjoamat verkkoasetukset. Jos asiakas hyväksyy tarjotut asetukset, se lähettää palvelimelle REQUEST-sanoman, jonka avulla se pyytää tarjottuja asetuksia käyttöönsä. Jos asiakas ei hyväksy tarjottuja asetuksia, se lähettää palvelimelle DECLINE-sanoman. Vastaanotettuaan REQUEST-sanoman palvelin joko vahvistaa kyseisten asetusten käyttöönoton ACK-sanomalla tai kieltää niiden käyttöönoton NAK-sanomalla. Asiakkaan saamat verkkoasetukset ovat käytössä niille annetun varausajan umpeutumiseen asti. Asiakas voi myös luopua käyttämistään asetuksista lähettämällä palvelimelle RELEASE-sanoman. Asiakas voi lisäksi pyytää palvelimelta lisäasetuksia INFORM-sanoman avulla. /5, s. 66–68./

2.6 Osoitteenmuunnos

Osoitteenmuunnos (Network Address Translation) kääntää osoitteenmuunnosta suorittavaan laitteeseen, kuten reitittimeen, yhteydessä olevien verkkojen laitteiden IP-osoitteita eri IP-osoitteeksi tai -osoitteiksi. Näin esimerkiksi yksityisiä osoitteita käyttävien aliverkkojen laitteet voivat kommunikoida julkisia osoitteita käyttävissä aliverkoissa. Osoitteenmuunnos on ollut suuressa roolissa IPv4-osoitteiden säästämisessä, sillä sen avulla monissa verkoissa voidaan käyttää samoja yksityisiä osoitteita julkisten osoitteiden sijaan. Yksityisten osoitteiden käyttäminen myös helpottaa eri organisaatioiden verkkojen suunnittelua ja ylläpitoa. /8, s. 183–184./

Erilaisia osoitteenmuunnostyyppejä ovat esimerkiksi *staattinen* ja *dynaaminen osoitteenmuunnos* sekä *porttimuunnos* (Port Address Translation). *Staattisessa osoitteenmuunnoksessa* tietty sisäinen osoite käännetään aina tietyksi ulkoiseksi osoitteeksi ja *dynaamisessa osoitteenmuunnoksessa* sisäinen osoite voidaan kääntää miksi tahansa vapaana olevaksi ulkoiseksi osoitteeksi. Staattinen ja dynaaminen osoitteenmuunnos vaativat, että jokaiselle käännettävälle sisäiselle osoitteelle on riitettävä ulkoinen osoite. *Porttimuunnos* voi puolestaan kääntää useita sisäisiä osoitteita yhdeksi ulkoiseksi osoitteeksi. Porttimuunnosta käytettäessä eri laitteille kuuluva tietoliikenne tunniste-

taan porttinumeron perusteella. Muunnosta suorittava laite pitää huolen siitä, että jokainen käännetty osoite käyttää eri lähdeporttinumeroa. /8, s. 185./

Osoitteenmuunnoksen käyttäminen voi tuoda mukanaan ongelmia. Esimerkiksi joidenkin sovellusten tai protokollien toiminta voi kärsiä IP-pakettien osoitetietojen muutoksien vuoksi. Osoitetietojen muutokset vaikeuttavat myös pakettien jäljitystä ja vianetsintää. Osoitteenmuunnos voi myös estää aliverkon ulkopuolelta tulevien TCP- ja UDP-yhteyksien muodostamisen. Toisaalta nämä seikat parantavat toki verkon tietoturvaa. Osoitteenmuunnoksen suorittaminen vie tietysti myös oman aikansa, mikä lisää verkkoviivettä. /8, s. 186–187./

3 LÄHIVERKOT

3.1 Topologiat

Lähiverkon (Local Area Network) avulla yhdistetään fyysisesti lähellä toisiaan sijaitsevia laitteita. Lähiverkko voi olla esimerkiksi yksittäisen rakennuksen sisäinen verkko. Lähiverkkoa hallinnoi yleensä yksi organisaatio. Verkon kautta siihen liitetyt päätelaitteet pääsevät käsiksi niiden tarvitsemiin palveluihin. /4, s. 28./

Lähiverkon toteuttamista varten on olemassa useita eri kaapelointitapoja eli topologioita, joita ovat esimerkiksi *väylä*, *rengas* ja *tähti*. *Väylätopologia* on näistä vanhin ja siinä laitteet on kytketty samaan avoimeen kaapeliin. *Rengastopologiassa* puolestaan kaapeli muodostaa renkaan, joten kaapelilla ei ole päitä, kuten väylätopologiassa. Rengasverkon tietoliikenne kulkee määrättyyn suuntaan, minkä vuoksi laitteiden sijoittelulla voidaan vaikuttaa verkon tehokkuuteen. /4, s. 28–30./

Tähtitopologia perustuu jokaisen verkon päätelaitteen kytkemiseen kytkentäkeskukseen, kuten kytkimeen (switch) tai keskittimeen (hub). Näin ollen yksittäisen päätelaitteen vioittuminen ei pääse häiritsemään koko verkon toimintaa, kuten väylä- ja rengastopologiassa. Parikaapeleilla toteutetut tähtiverkot ovat nykyisin hyvin suosittuja. Tähtitopologiaan pohjautuvan verkon koon muuttaminen on vaivatonta ja uusien päätelaitteiden lisääminen sekä vanhojen poistaminen on helppoa. /4, s. 30–31./

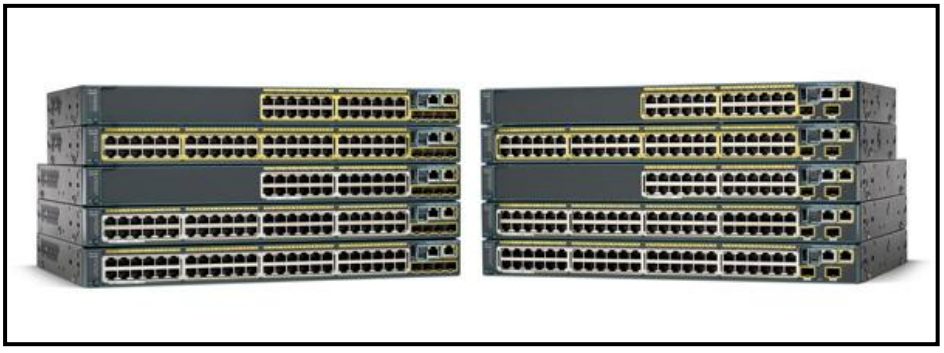
3.2 Verkkolaitteet

Lähiverkoista löytyy erilaisten päätelaitteiden, kuten työasemien, palvelimien ja tulostimien lisäksi monia eri verkkolaitteita. Näitä ovat esimerkiksi *toistin, keskitin, silta, kytkin* ja *reititin*. /5, s. 28–31./

Toistin (repeater) on yksinkertainen laite, joka vahvistaa tai generoi uudelleen verkossa kulkevia signaaleja. Nykyään pelkästään toistimina toimivat laitteet ovat harvinaisia, sillä niiden tilalle on tullut monipuolisempia laitteita. Toistin toimii OSI-mallin fyysisellä kerroksella. /5, s. 28–29./

Keskitin (hub) välittää yhdestä portista saamansa signaalin ulos kaikista muista porteistansa. Tällaisten passiivisten keskittimien lisäksi on olemassa aktiivisia keskittimiä, joissa voi esimerkiksi olla myös suodatus- ja verkonhallintaominaisuuksia. Keskitin toimii OSI-mallin fyysisellä kerroksella. /4, s. 45–46./

Silta (bridge) yhdistää kaksi verkkoa ja osaa suodattaa liikennettä. Esimerkiksi kahden Ethernet-verkon välinen silta ei päästä turhaan toisen verkon sisäistä liikennettä toiseen verkkoon. Silta tutkii yhdistämiensä verkkojen kehyksiä eli se toimii OSI-mallin siirtoyhteyskerroksella. /5, s. 29–30./



KUVA 10. Cisco Catalyst 2960 -sarjan kytkimiä /9/

Kytkin (switch) (kuva 10) pystyy välittämään useista eri lähdeporteista vastaanottamansa liikenteen kohdeportteihinsa samanaikaisesti. Kytkin tunnistaa portteihinsa liitetyt laitteet ja osaa näin ollen ohjata liikenteen vain tarpeellisiin kohdeportteihin. Kytkimet toimivat yleensä OSI-mallin siirtoyhteyskerroksella, mutta on olemassa myös verkkokerroksella toimivia kytkimiä. *Reititin* (router) toimii verkkokerroksella ja se hallitsee IP-pakettien reitittämisen kohti kohdeverkkoaan. /5, s. 30–31./

3.3 Virtuaalilähiverkot

Kytkimien avulla voidaan luoda virtuaalilähiverkkoja (Virtual Local Area Network). Virtuaalilähiverkot mahdollistavat samaan kytkimeen tai useisiin eri kytkimiin kytkettyjen laitteiden jakamisen eri aliverkkoihin ja yleislähetysalueisiin. Niiden välinen tietoliikenne vaatii luonnollisesti verkkokerroksella toimivan laitteen apua. Erilaisia virtuaalilähiverkkojen toteutustapoja ovat *porttiperusteinen-* (port based VLAN), *MAC-osoitteeseen perustuva-* (MAC-based VLAN), *verkkokerrokseen perustuva-* (layer 3 based VLAN) ja *policy-perusteinen virtuaalilähiverkko* (policy based VLAN). /1, s. 90–96./

Porttiperusteisia virtuaalilähiverkkoja saadaan aikaan, kun määritellään kytkimen portit kuulumaan haluttuihin virtuaalilähiverkkoihin. *MAC-osoitteeseen perustuvia virtuaalilähiverkkoja* luodaan puolestaan verkossa olevien päätelaitteiden fyysisten osoitteiden perusteella luotujen ryhmien avulla. /1, s. 93–94./

Verkkokerroksella toimivien kytkimien avulla voidaan muodostaa *verkkokerrokseen perustuvia virtuaalilähiverkkoja*. Tällöin virtuaalilähiverkot muodostetaan laitteiden loogisten osoitteiden pohjalta. *Policy-perusteisia virtuaalilähiverkkoja* voidaan puolestaan määrittää useiden eri perusteiden avulla. Näitä ovat esimerkiksi laitteiden fyysiset ja loogiset osoitteet sekä niiden käyttämät erilaiset protokollatyypit. /1, s. 95–96./

Virtuaalilähiverkkojen käytöllä voidaan parantaa tietoturvan tasoa, sillä eri virtuaalilähiverkot on erotettu toisistaan ja niiden välisen tietoliikenteen on kuljettava verkkokerroksella toimivan laitteen kautta. Virtuaalilähiverkkojen ansiosta myös verkon suorituskyky kasvaa, koska verkko on tällöin jaettu useisiin pienempiin yleislähetysalueisiin. Myös verkon ylläpito selkeytyy ja helpottuu, koska samankaltaiset käyttäjät voidaan ryhmitellä omiin virtuaalilähiverkkoihinsa. On tärkeää huomata, että virtuaalilähiverkkojen avulla voidaan päästä merkittäviinkin kustannussäästöihin verkon ylläpidon suhteen. /10, s. 72./

Nykyään virtuaalilähiverkkojen määrittelyssä käytetään lähinnä porttiperusteisia virtuaalilähiverkkoja. Virtuaalilähiverkkojen määrittelytapaa kuvaavien termien lisäksi virtuaalilähiverkkoja kuvataan usein myös niiden tehtävän näkökulmasta. On yleistä,

että ääntä (Voice VLAN), kytkinten hallintadataa (Management VLAN) ja muuta dataa (Data VLAN) siirtävät virtuaalilähiverkot erotetaan toisistaan. /10, s. 73–74./

Äänen siirtoon käytettävä virtuaalilähiverkko on tarpeellinen, kun käytetään IP-puhetta (Voice over IP). Tällöin pyritään takaamaan verkon riittävä suorituskyky siirtää hyvälaatuista ääntä. Kytkimien hallintadataa siirtävän virtuaalilähiverkon avulla puolestaan päästään määrittelemään kytkimien asetuksia esimerkiksi HTTP-, Telnet-, SSH- tai SNMP-protokollan avulla. Muun datan siirtoon käytettävä virtuaalilähiverkko huolehtii nimensä mukaisesti kaikesta muusta verkkoliikenteestä. /10, s. 73–75./

Muita tärkeitä virtuaalilähiverkkotermejä ovat muun muassa *oletusvirtuaalilähiverkko* (Default VLAN) ja *perusvirtuaalilähiverkko* (Native VLAN). *Oletusvirtuaalilähiverkko* on se virtuaalilähiverkko, johon kaikki kytkimen portit oletusarvoisesti kuuluvat. *Perusvirtuaalilähiverkkoon* on määritetty kuuluviksi runkoyhteysportteja (trunk port), jotka kuvataan IEEE 802.1Q -suosituksessa. Nämä runkoyhteysportit voivat siirtää useista eri virtuaalilähiverkoista peräisin olevaa liikennettä ja myös liikennettä, jota ei ole merkitty olemaan peräisin virtuaalilähiverkosta. /10, s. 74./

Runkoyhteysporttien avulla voidaan siirtää eri virtuaalilähiverkkojen tietoliikennettä kokonaisessa useista kytkimistä koostuvassa verkossa. Niiden avulla muodostetaan kaksipisteyhteyksiä kytkimien välille. Näitä yhteyksiä varten Ethernet-kehykseen on lisättävä VLAN-tunniste, joka ilmaisee mihin virtuaalilähiverkkoon kyseinen kehys kuuluu. /10, s. 80–81./

VTP

Suurissa useista kytkimistä koostuvissa verkoissa ajantasaisten virtuaalilähiverkkomääritysten ylläpitäminen voi olla hyvin työlästä, jos konfiguraatiomuutokset täytyy tehdä jokaiseen kytkimeen yksitellen. Cisco-kytkimien VTP (VLAN Trunking Protocol) on hyvä apukeino yhdenmukaisten virtuaalilähiverkkomääritysten ylläpitämiseen suuressakin verkossa. /10, s. 95./

VTP:n toimintaperiaatteena on, että VTP-palvelimena toimiva kytkin päivittää VTP-asiakkaina toimivien kytkimien virtuaalilähiverkkomääritykset omiensa kaltaisiksi. Näin ollen verkon ylläpitäjän tarvitsee tehdä konfiguraatiomuutokset vain VTP-

palvelimena toimivaan kytkimeen. VTP:n kautta päivittyvät virtuaalilähiverkkojen lisäykset, poistot ja uudelleennimeämiset. /10, s. 96./

Osallistuakseen VTP:n toimintaan kytkimien on kuuluttava samalle VTP-toimialueelle (VTP domain). Kytkimet lähettävät säännöllisesti VTP-sanomia kaikista runkoyhteysporteistaan varattuun ryhmäosoitteeseen. Viereiset kytkimet vastaanottavat nämä sanomat ja päivittävät virtuaalilähiverkkomäärityksensä tarpeen vaatiessa. /10, s. 98–99./

VTP-toimialueen kytkimet vertaavat vastaanottamiensa VTP-sanomien määritysversionumeroa omiin senhetkisiin määritysversionumeroihin. Määritysversionumero on oletusarvoltaan nolla ja se kasvaa yhdellä aina, kun uusi virtuaalilähiverkko lisätään tai vanha poistetaan. Kytkimen VTP-toimialueen nimen muuttaminen nollaa määritysversionumeron. /10, s. 100./

Kytkimiä voidaan määritellä eri rooleihin VTP:n toiminnassa. Nämä roolit ovat *VTP-palvelin*, *VTP-asiakas* ja *passiivinen* (transparent). *VTP-palvelimen* avulla voidaan muokata koko VTP-toimialueen kytkimien virtuaalilähiverkkomäärityksiä. *VTP-asiakkaina* toimivissa kytkimissä puolestaan virtuaalilähiverkkomääritysten muokkaaminen ei ole mahdollista. Määritykset häviävät VTP-asiakkaan muistista aina, kun virta sammutetaan ja sen on pyydettävä ne uudelleen VTP-palvelimelta uudelleenkäynnistyksen yhteydessä. *Passiiviset kytkimet* vain välittävät eteenpäin toisten kytkimien lähettämiä VTP-sanomia. Ne eivät päivitä omia virtuaalilähiverkkomäärityksiään VTP-sanomien pohjalta eivätkä lähetä omia VTP-sanomia. /10, s. 102./

Eräs VTP:n kätevistä ominaisuuksista on myös VTP-karsiminen (VTP pruning). Sen ansiosta kytkimet voivat suodattaa tarpeettoman virtuaalilähiverkkoliikenteen pois niiden välisiltä runkoyhteyksiltä. Tällöin esimerkiksi kahden kytkimen välisellä runkoyhteydellä ei siirretä virtuaalilähiverkon yleislähetys- ja ryhmäosoiteliikennettä, mikäli kyseiseen virtuaalilähiverkkoon liitettyjä portteja ei ole molemmissa kytkimissä. Tämä parantaa runkoyhteyden suorituskykyä. /10, s. 103./

4 REITITINVERKOT

4.1 Reititys

Reititys on IP-pakettien välittämistä kohti niiden kohdealiverkkoja. Reitittimet (kuva 11) ohjaavat saapuvan paketin oikeaan lähtöporttiin reititystaulun ja paketin osoitetietojen perusteella. Reitittimet eivät tiedä paketin koko reittiä. Ne lähettävät paketin vain seuraavalle reitittimelle, joka on niiden oman reititystaulun mukaan seuraava etappi parhaalla reitillä paketin kohdealiverkkoon. /5, s. 82./

KUVA 11. Cisco 1841 -reititin /11/

Reitittimen reititystaulu sisältää tiedon IP-osoitteista tai sen omista porteista, joiden kautta päästään eri kohdealiverkkoihin. Reititystaulussa voi olla *suoraan yhdistettyjä*, *staattisia* ja *dynaamisia reittejä*. *Suoraan yhdistetyt reitit* ovat reittejä aliverkkoihin, joihin jokin kyseessä olevan reitittimen oma portti kuuluu. *Staattiset* ja *dynaamiset reitit* ovat puolestaan reittejä aliverkkoihin, joihin päästäkseen paketin on kuljettava vielä toisen reitittimen kautta. Staattiset reitit ovat verkon ylläpitäjän manuaalisesti määrittelemiä ja dynaamiset reitit reititin on oppinut automaattisesti jonkin reitityksprotokollan kautta. /12, s. 34–35./

Reitittimet valitsevat parhaan reitin kohdealiverkkoon metric-arvon pohjalta. Eri reitityksprotokollat laskevat metric-arvot eri tavoin, joten eri protokollien metric-arvoja ei pidä vertailla keskenään. Metric-arvojen laskemiseen voidaan käyttää esimerkiksi reitin varrella olevien reitittimien määrää, siirtokapasiteettia, kuormitusta, viivettä, luotettavuutta tai näiden yhdistelmiä. Parhaalla reitillä on aina pienin metric-arvo. /12, s. 160–162./

Jos Cisco-reititin saa reitin tietoonsa useasta eri lähteestä, ratkaistaan käytettävä reitti hallinnollisen etäisyyden (administrative distance) avulla. Hallinnollinen etäisyys on lukuarvo, joka vaihtelee sen mukaan, mitä kautta reitti on opittu. Reititin valitsee käytettäväksi aina reitin, jolla on pienin mahdollinen hallinnollinen etäisyys. Esimerkiksi suoraan yhdistettyjen reittien hallinnollinen etäisyys on aina nolla ja staattisten reittien oletusarvoisesti yksi. Kaikilla reititysprotokollilla on oletusarvoisesti näitä suuremmat hallinnolliset etäisyydet (taulukko 3). /12, s. 165–170./

TAULUKKO 3. Oletusarvoisia hallinnollisia etäisyyksiä /12, s. 170/

Reitin lähde	Hallinnollinen etäisyys
suoraan yhdistetty reitti	0
staattinen reitti	1
EIGRP-yhdistelmäreitti	5
ulkoinen BGP-reitti	20
sisäinen EIGRP-reitti	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
ulkoinen EIGRP-reitti	170
sisäinen BGP-reitti	200

4.2 Reititysprotokollat

Reititysprotokollia tarvitaan dynaamiseen reititykseen. Samaa reititysprotokollaa käyttävät reitittimet voivat automaattisesti vaihtaa keskenään tietoja tuntemistaan reiteistä ja päivittää reititystaulunsa niiden pohjalta. Reititysprotokollien avulla reitittimet pystyvät sopeutumaan nopeasti verkon topologian muutoksiin. Staattista reititystä käytettäessä verkon ylläpitäjän olisi määriteltävä uuden topologian vaatimat staattiset reitit reitittimiin manuaalisesti. /12, s. 41./

Reititysprotokollat voidaan jakaa sisäisiin ja ulkoisiin reititysprotokolliin (taulukko 4). Sisäisiä reititysprotokollia käytetään Internetiin liitettyjen verkkojen sisäisessä liikenteessä ja ulkoisia reititysprotokollia Internet-operaattoreiden reitittimissä, jotka yhdistävät Internetin osaverkkoja. /1, s. 226./

TAULUKKO 4. Reititysprotokollien jaottelu /12, s. 149/

	Sisäiset reititysprotokollat				**Ulkoiset reititys-protokollat**
	Etäisyysvektoriprotokol-lat		**Linkkitilaprotokol-lat**		
Luokallinen IPv4-reititys	RIP	IGRP			EGP
Luokaton IPv4-reititys	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6-reititys	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGPv4 for IPv6

Sisäisiä reititysprotokollia on suuri määrä. Jotkin niistä ovat standardoituja ja jotkin reititinvalmistajien omia protokollia. Reititinvalmistajien omat reititysprotokollat ovat usein tehokkaampia ja luotettavampia, mutta ne eivät toimi kuin yhden valmistajan reitittimien välillä. Sisäiset reititysprotokollat voidaan jakaa etäisyysvektoriprotokolliin ja linkkitilaprotokolliin. /1, s. 226./

Etäisyysvektoriprotokollat tekevät reitityspäätöksiä pääasiassa reitin varrella olevien reitittimien lukumäärän mukaan. Reititettävälle paketille valitaan reitti, joka kulkee mahdollisimman harvan reitittimen kautta. Reititin tietää, kuinka monen reitittimen takana ja missä suunnassa kohdealiverkko sijaitsee. Etäisyysvektoriprotokollat saattavat välittää myös tietoa eri yhteyksien nopeudesta, kuormituksesta ja virhealttiudesta. Etäisyysvektoriprotokollat ovat toiminnaltaan yksinkertaisia ja ne eivät vaadi reitittimeltä kovinkaan paljon muistia ja prosessoritehoa. Ne kuitenkin kuormittavat verkkoa säännöllisillä reititystaulupäivityksillä ja yhteyksien testaamisella. Ne eivät myöskään muodosta kokonaiskuvaa verkon topologiasta. /1, s. 226./

Linkkitilaprotokollat puolestaan huolehtivat siitä, että reitittimillä on käytössään verkon topologiaan pohjautuva reittikartta, josta käyvät ilmi eri yhteyksien siirtokapasiteetit, kuormitukset ja virhealttiudet. Reitityspäätökset tehdään näiden tekijöiden perusteella. Muutokset verkon topologiassa aiheuttavat kaikkien reitittimien reittikarttojen päivittymisen. /1, s. 227./

4.3 RIP

Vanhin reititysprotokolla on etäisyysvektoriprotokolliin lukeutuva RIP (Routing Information Protocol). RIP käyttää metric-arvonaan reitin varrella olevien reitittimien

lukumäärää, joka voi olla enintään 15. Metric-arvo 16 tulkitaan jo äärettömäksi etäisyydeksi. /5, s. 90./

RIP-reitittimet lähettävät naapurireitittimilleen päivitysviestejä normaalisti 30 sekunnin välein. Jos reittitietoa ei virkistetä uuden päivitysviestin myötä kolmen minuutin aikana, sen metric-arvoksi asetetaan 16 ja lopulta se poistetaan kokonaan. Yksi päivitysviesti voi sisältää enintään 25 reitin tiedot. /5, s. 91./

Nopeuttaakseen ajantasaisten reititystietojen leviämistä verkossa RIP käyttää säännöllisten päivitysviestien lisäksi myös välittömästi muutoksien tapahtumisen jälkeen lähetettäviä päivitysviestejä. Uudet reitit reititystaulussa, reittien muuttuminen toimimattomiksi tai jälleen toimiviksi sekä reitittimen porttien tilojen muutokset aikaansaavat päivitysviestin lähettämisen jo ennen säännöllisen päivitysviestin lähettämisen ajankohtaa. /12, s. 198–199./

RIP:n ensimmäinen versio ei tunne vaihtelevan pituisia aliverkon peitteitä, joten sen avulla voidaan toteuttaa vain IP-osoitteiden luokkajakoon perustuva reititys. Tämä tekee ensimmäisestä versiosta ehdottomasti vanhanaikaisen. RIP:n toisen version päivitysviestit sisältävät ensimmäisen version viesteistä poiketen kohdealiverkon aliverkon peitteen ja seuraavan reitin varrella olevan reitittimen IP-osoitteen, mikä tekee vaihtelevan pituisen aliverkon peitteen avulla luotujen aliverkkojen välisen reitityksen mahdolliseksi. /5, s. 90–92./

Eräs RIP:n ongelma on reitityssilmukat. Reitityssilmukka syntyy esimerkiksi silloin, kun reititin ei ehdi ilmoittaa naapurireitittimelleen toimimattomasta reitistä ennen kuin se vastaanottaa naapurireitittimeltä päivitysviestin. Tämä saa reitittimen olettamaan, että aliverkkoon, johon se on juuri menettänyt yhteyden, on olemassa naapurireitittimen kautta kulkeva reitti. Näin ollen aliverkkoon, johon yhteys on menetetty, lähetetyt paketit jäävät kulkemaan silmukkaan näiden kahden reitittimen välille kunnes niiden TTL-arvot putoavat nollaan. /12, s. 200–201./

Reitityssilmukoita pyritään ehkäisemään esimerkiksi *split horizon*- ja *poison reverse* -*menetelmällä*. *Split horizon -menetelmä* tarkoittaa sitä, että reitittimet eivät opeta naapurireitittimilleen takaisin niiltä oppimiaan reittejä. *Poison reverse -menetelmä* puo-

lestaan tarkoittaa sitä, että naapurireitittimiltä opitut reitit opetetaan niille takaisin, mutta niiden metric-arvoiksi asetetaan 16. /1, s. 229–231./

RIP käyttää myös Hold-down-ajastinta reitityssilmukoiden ehkäisemisessä. Kun reititin saa päivitysviestin kautta tiedon siitä, että reitti on muuttunut toimimattomaksi, se käynnistää kyseisen reitin Hold-down-ajastimen. Kun ajastin on käynnissä, reititin ei huomioi kyseessä olevaan aliverkkoon suuntautuvien reittien päivityksiä, jos niiden metric-arvo on sama tai suurempi kuin alkuperäisen reitin metric-arvo. Tämä ehkäisee virheellisten reittitietojen lisäämisen reititystauluun ja takaa sen, että oikeat reititystiedot ehtivät levitä kaikkiin verkon reitittimiin. Toimimaton reitti poistetaan reititystaulusta vasta ajastimen pysähdyttyä. /12, s. 203–206./

4.4 EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) on Ciscon kehittämä etäisyysvektoriprotokolla, joka toimii ainoastaan Ciscon valmistamissa reitittimissä. EIGRP voi muistuttaa joiltakin piirteiltään linkkitilaprotokollaa ja sitä kutsutaankin joskus hybridiprotokollaksi, joka sisältää näiden molempien reititysprotokollaryhmien ominaisuuksia. EIGRP on kuitenkin etäisyysvektoriprotokolla, joten termiä hybridiprotokolla voidaan pitää harhaanjohtavana. /12, s. 392./

EIGRP:n toiminta poikkeaa kuitenkin huomattavasti perinteisten etäisyysvektoriprotokollien, kuten RIP:n, toiminnasta. EIGRP ei lähetä säännöllisiä päivitysviestejä, vaan vasta muutokset reititystiedoissa aikaansaavat uuden päivitysviestin lähettämisen. EIGRP-reitittimet kuitenkin tarkkailevat naapurireitittimiensä tilaa Hello-pakettien avulla. EIGRP myös ylläpitää perinteisistä etäisyysvektoriprotokollista poiketen reititystaulusta erillistä topologiataulua, joka sisältää parhaiden mahdollisten reittien lisäksi myös varareittejä, joita voidaan ottaa tarvittaessa heti käyttöön reititystaulun puolelle. /12, s. 394–395./

EIGRP:n päivitysviestit sisältävät tiedon vain niistä reiteistä, joiden tietoihin on tullut muutoksia. Tämä on selkeä ero RIP:n päivitysviesteihin nähden, jotka sisältävät aina koko reitittimen reititystaulun sisällön. Lisäksi EIGRP:n päivitysviestit lähetetään vain niille reitittimille, joiden toimintaan muuttunut reittitieto vaikuttaa. /12, s. 405./

EIGRP:n toiminta alkaa sillä, että naapurireitittimet havaitsevat toisensa lähettämiensä Hello-pakettien avulla. Tämän jälkeen Hello-paketteja käytetään naapurireitittimien tilan valvontaan. Jos reititin ei vastaanota naapuriltaan Hello-pakettia aina tietyn ajan kuluessa, se tulkitsee sen kautta kulkevat reitit toimimattomiksi. /12, s. 404./

Kun reitti muuttuu toimimattomaksi, reititin yrittää etsiä varareitin topologiataulusta ja siirtää sen käyttöön reititystauluun. Jos varareittejä ei kuitenkaan ole, reititin tiedustelee naapurireitittimiltään, onko niiden tiedossa vaihtoehtoisia reittejä vanhan reitin tilalle. Jos varareittejä ei löydy tälläkään tavalla, kyseessä oleva kohdealiverkko on poistettava reititys- ja topologiataulusta. /12, s. 441–446./

Jotta EIGRP voi hyväksyä reitin varareitiksi topologiatauluun, on sen täytettävä ehto, jonka avulla ehkäistään reitityssilmukoiden syntyminen. Naapurireitittimen, jonka kautta varareitti kulkee, metric-arvo kohdealiverkkoon on oltava pienempi kuin reitittimen itsensä käyttämän ensisijaisen reitin metric-arvo samaan kohdealiverkkoon. /12, s. 434./

EIGRP voi käyttää metric-arvon laskemiseen siirtokapasiteettia, viivettä, luotettavuutta ja kuormitusta. Oletusarvoisesti laskemiseen käytetään vain siirtokapasiteettia ja viivettä. Laskennassa käytetty siirtokapasiteettiarvo voidaan määritellä reitittimen eri porteille. Tämä ei kuitenkaan määritä porttien todellisia tiedonsiirtonopeuksia. Myöskään viive ei kuvaa yhteyden todellista siirtoviivettä, vaan sekin on verkon ylläpitäjän määriteltävissä oleva staattinen arvo. /12, s. 423–426./

Luotettavuus ja kuormitus puolestaan mitataan dynaamisesti. Luotettavuus kertoo, kuinka todennäköisesti yhteys kärsii ongelmista. Luotettavuus ilmaistaan arvolla, joka voi vaihdella välillä 0–255. Arvo 255 kuvaa täysin luotettavaa yhteyttä. Myös kuormitus ilmaistaan samalla arvoasteikolla, jossa arvo 255 kuvaa täysin kuormitettua yhteyttä. /12, s. 427./

4.5 OSPF

OSPF (Open Shortest Path First) on linkkitilaprotokolliin kuuluva sisäinen reititysprotokolla. Käytössä olevia OSPF-versioita on kaksi kappaletta ja ne ovat OSPFv2 ja

OSPFv3. OSPFv2 on tarkoitettu käytettäväksi IPv4-verkoissa ja OSPFv3 IPv6-verkoissa. /12, s. 500–501./

OSPF:n toimintaprosessi alkaa sillä, että reititin havaitsee siihen suoraan yhteydessä olevat linkit ja aliverkot käymällä läpi omien aktiivisten porttiensa IP-osoitteet ja aliverkon peitteet. Tämän jälkeen se havaitsee naapurireitittimensä vaihtamalla niiden kanssa Hello-paketteja. /12, s. 474./

Seuraavaksi reititin muodostaa linkkitilapaketin (Link State Packet), joka sisältää kaikkien siihen suorassa yhteydessä olevien linkkien tilan. Reititin lähettää linkkitilapaketin kaikille naapurireitittimilleen, jotka tallentavat sen omiin tietokantoihinsa. Reitittimet lähettävät vastaanotetutkin linkkitilapaketit naapureilleen, kunnes jokaisella reitittimellä on kaikkien toisten reitittimien linkkitilapaketit tietokannassaan. Lopuksi jokainen reititin muodostaa vastaanottamiensa linkkitilapakettien pohjalta kartan verkon topologiasta ja laskee parhaan mahdollisen reitin jokaiseen kohdealiverkkoon. /12, s. 474./

OSPF ei käytä säännöllisiä päivityksiä, vaan linkkitilapaketteja lähetetään vain, kun linkkien tiloihin kohdistuu muutoksia. Tällöin linkkitilapaketti sisältää vain muutoksia kokeneen linkin tiedot. OSPF-reitittimet kuitenkin lähettävät oletusarvoisesti omien linkkiensä tilan sisältävän linkkitilapaketin 30 minuutin välein. Reitittimet tarkkailevat naapurireitittimiensä tilaa Hello-pakettien avulla. Jos reititin ei vastaanota Hello-pakettia naapuriltaan tietyn ajan kuluessa, se poistaa naapurin tietokannastaan. /12, s. 488–489 ja 505./

OSPF käyttää metric-arvonaan hintaa (cost), jonka verkon ylläpitäjä voi määritellä reitittimen eri porteille. Esimerkiksi Ciscon reitittimet laskevat hinnan porttien tiedonsiirtonopeuksien perusteella. Näin ollen koko reitin hinnaksi tulee sen varrella olevien reitittimien lähtöporttien yhteenlasketut hinnat. Ciscon reitittimen portille voi määrittää joko hinnan laskemisessa käytettävän siirtonopeuden tai suoraan hintana käytettävän arvon. Porteille määritellyt siirtonopeudet eivät kuitenkaan määritä niiden todellisia siirtonopeuksia. /12, s. 523–527./

Yli kahden OSPF-reitittimen aliverkot

Aliverkoissa, joissa on suuri määrä reitittimiä, reitittimien ei kannata lähettää linkkitilapakettejaan kaikille naapurireitittimilleen. Tämä aiheuttaisi paljon liikennettä, mikä voi heikentää verkon suorituskykyä tuntuvasti. Aliverkoissa, joissa on enemmän kuin kaksi reititintä, reitittimet valitsevat joukostaan yhden, jonka tehtävänä on vastaanottaa kaikkien muiden linkkitilapaketit ja välittää ne eteenpäin kaikille muille reitittimille. Tätä reititintä kutsutaan nimellä Designated Router (DR). DR:lle valitaan myös varareititin, joka ottaa DR:n tehtävät, jos se jostain syystä sattuu lopettamaan toimintansa. Myös tämä varareititin vastaanottaa jatkuvasti muiden linkkitilapaketteja, mutta se ei välitä niitä eteenpäin. Varareititintä kutsutaan nimellä Backup Designated Router (BDR). Kaikkia muita reitittimiä puolestaan kutsutaan nimellä DROther. /12, s. 530–536./

DR:n ja BDR:n valitsemisessa käytetään OSPF-portin prioriteettiarvoa, joka on verkon ylläpitäjän määriteltävissä ja voi saada arvokseen luvun 0–255. Jos arvo on nolla, reititin ei voi olla DR tai BDR kyseisen portin aliverkossa. Reitittimestä, jonka portilla on korkein prioriteettiarvo, tulee kyseisen aliverkon DR ja toiseksi korkein prioriteettiarvo oikeuttaa BDR:n tehtäviin. Oletuksena kaikkien OSPF-porttien prioriteetti on yksi. Jos reitittimien porttien prioriteetit ovat samat, ratkaistaan DR:n ja BDR:n valintaprosessi reitittimien ID-arvojen perusteella. Korkeammalla ID-arvolla varustettu reititin voittaa pienemmällä ID-arvolla varustetun reitittimen samaan tapaan kuin prioriteettiarvoihin pohjautuvassa valinnassa. /12, s. 537 ja 542./

OSPF käyttää IPv4-osoitteen muodossa olevia reitittimien ID-arvoja niiden yksilölliseen tunnistamiseen. Ciscon reitittimet valitsevat ID-arvoksi ensisijaisesti verkon ylläpitäjän erikseen määrittelemän ID-arvon. Jos ID-arvoa ei ole määritelty, reititin valitsee ID-arvokseen korkeimman määritellyn loopback-osoitteensa. Jos loopback-osoitteitakaan ei ole määritelty, ID-arvona käytetään korkeinta aktiivisena olevan portin IP-osoitetta. /12, s. 514./

DR:n ja BDR:n valitseminen vie vain muutaman sekunnin ja se aloitetaan heti, kun ensimmäinen reititin liitetään verkkoon. DR ja BDR eivät luovu tehtävistään, vaikka verkkoon liitettäisiinkin myöhemmin suuremmalla OSPF-portin prioriteetillä tai ID-arvolla varustettu reititin. Jos DR lopettaa toimintansa, BDR ottaa sen tehtävät ja vali-

taan uusi BDR. Jos taas BDR lopettaa toimintansa, valitaan vain uusi BDR. Jos halutaan varmistaa, että juuri tietystä reitittimestä tulee DR, kannattaa se liittää verkkoon ensimmäisenä. /12, s. 539–542./

4.6 Laajaverkkoprotokollat

Laajaverkot (Wide Area Network) kattavat maantieteellisesti laajoja alueita. Ne yhdistävät toisiinsa lähiverkkoja (Local Area Network), jotka käsittävät usein vain yksittäisen rakennuksen tai muun pienen alueen sisäisen verkon. Laajaverkkoja varten kehitettyjä tekniikoita ja protokollia ovat esimerkiksi HDLC, PPP, Frame Relay ja ATM. /8, s. 5 ja 13./

HDLC

HDLC (High-Level Data Link Control) on ISO:n SDLC-protokollan (Synchronous Data Link Control) pohjalta standardoima tiedonsiirtoprotokolla. HDLC:n avulla voidaan muodostaa yhteydellisiä tai yhteydettömiä synkronisia sarjaliikenneyhteyksiä. HDLC sisältää vuonhallinta- ja virheenkorjausmekanismit. /8, s. 34./

Cisco on kehittänyt oman versionsa HDLC:sta, jota kutsutaan nimellä Cisco HDLC tai cHDLC. Cisco-laitteet käyttävät tätä protokollaa synkronisten sarjaliikenneyhteyksien oletusprotokollana. Cisco HDLC toimii Ciscon valmistamien laitteiden lisäksi joissakin muiden valmistajien laitteissa, mikäli Cisco on antanut kyseisten laitevalmistajien varustaa laitteensa Cisco HDLC -tuella. /8, s. 34–35./

PPP

PPP (Point-to-Point Protocol) on yksinkertainen kahden osapuolen väliseen tiedonsiirtoon tarkoitettu protokolla. Sitä käytetään verkkolaitteiden sekä verkkojen ja päätelaitteiden välisillä yhteyksillä. PPP koostuu useasta erillisestä protokollasta, joita käytetään yhteyksien avaamiseen ja ylläpitämiseen. /2, s. 248 ja 252./

LCP (Link Control Protocol) hoitaa PPP-yhteyden avaamisen ja ylläpidon. Yhteyden avaamisen yhteydessä osapuolet sopivat siihen liittyvistä määrityksistä ja yhteyden

ollessa avattuna ne voivat lähettää toisilleen palautetta virheellisistä kehyksistä sekä testata yhteyden toimintaa. /8, s. 39./

Kun LCP on avannut yhteyden, määritetään sen yli siirrettävät verkkokerroksen protokollat. NCP (Network Control Protocol) mahdollistaa verkkokerroksen protokollan siirtämisen PPP-yhteyden yli. Jokaiselle PPP:n tukemalle verkkokerroksen protokollalle, joita ovat muun muassa IP, IPX ja AppleTalk, on olemassa oma NPC. /8, s. 40./

Frame Relay

Frame Relay -tekniikan ajatuksena on korvata reitittimien välisiä kiinteitä yhteyksiä. Frame Relay yhdistää eri lähiverkkojen reitittimiä Frame Relay -solmujen muodostaman verkon avulla, mikä mahdollistaa sen, että useat käyttäjät voivat käyttää samaa siirtotietä. /4, s. 16./

Lähiverkon liittyessä Frame Relay -verkkoon on sen reitittimen ja Frame Relay -solmun välille muodostettava kiinteä yhteys. Loogiset Frame Relay -yhteydet erotetaan toisistaan DLCI-numeron (Data Link Control Identifier) avulla. Frame Relay ei sisällä vuonhallintaa tai virheenkorjausta. /4, s. 16–17./

ATM

ATM-verkko (Asynchronous Transfer Mode) muodostuu ATM-kytkimistä, jotka välittävät dataa tuloliitännästä lähtöliitäntään sisäisten kytkentätaulujensa mukaisesti. ATM-verkossa siirrettävä data koostuu keskenään samankokoisista ATM-soluista. /4, s. 22./

Kahden osapuolen välinen ATM-yhteys koostuu kahdesta virtuaalikanavasta, joiden avulla saadaan aikaan kaksisuuntainen liikenne. Nämä virtuaalikanavat muodostavat yhdessä virtuaalipolun. Virtuaalipoluista on apua ATM-kytkimien vikaantumistilanteissa. Tällöin virtuaalipolut voidaan kytkeä kulkemaan jotain toista reittiä eikä eri virtuaalikanavia tarvitse kytkeä erikseen. Eri virtuaaliyhteyksille kuuluvat solut voidaan erottaa niiden sisältämän VPI- (Virtual Path Identifier) ja VCI-arvon (Virtual Channel Identifier) pohjalta. /4, s. 23–24./

5 ESIMERKKI LÄHI- JA REITITINVERKOSTA

5.1 Cisco Packet Tracer ja Cisco IOS

Esimerkkiverkon mallintamiseen ja tarkasteluun on käytetty Cisco Packet Tracer -ohjelman versiota 5.3.2.0027. Packet Tracer on verkkojen simuloimiseen tarkoitettu ohjelma, jota käytetään yleisesti Cisco Networking Academy -kursseilla. Sen avulla voi harjoitella Ciscon kytkimien ja reitittimien konfigurointia komentorivin avulla. Packet Tracerin tukemat protokollat on esitetty taulukossa 5. /13, s. 1–3./

TAULUKKO 5. Cisco Packet Tracerin tukemat protokollat /13, s. 3/

Layer	Cisco Packet Tracer Supported Protocols
Application	• FTP , SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Transport	• TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Network	• BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/ v2/ng, Multi-Area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL , Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN
Network Access/ Interface	• Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP

Ciscon kytkimet ja reitittimet käyttävät Cisco IOS -käyttöjärjestelmää. IOS:n ominaisuudet vaihtelevat eri laitemallien ja käyttöjärjestelmäversion mukaan. Laitteiden asetuksia voidaan määritellä IOS:n komentorivin avulla. IOS:n komentoriviin voi päästä käsiksi useilla eri tavoilla. /6, s. 410–411./

Yksi vaihtoehto on yhdistää tietokone IOS-laitteen Console-porttiin ja muodostaa sarjaliikenneyhteys pääte-emulaattoriohjelman avulla. Tämä keino toimii silloinkin, kun IOS-laitteeseen ei ole määritelty lainkaan verkkotoimintoja. Toinen vaihtoehto on ottaa yhteys IOS-laitteeseen Telnet- tai SSH-protokollan avulla. Tällöin laitteessa on oltava vähintään yksi aktiivinen portti, jolle on määritelty IP-osoite. IOS-komentoriville voi päästä myös muodostamalla puhelinmodeemiyhteyden laitteen Auxiliary-porttiin. Tämä keino toimii myös silloin, kun laitteeseen ei ole määritelty verkkotoimintoja. Lisäksi Auxiliary-portin kautta laitteeseen voi muodostaa yhteyden Console-portin tavoin myös pääte-emulaattoriohjelman avulla. /6, s. 411–413./

Cisco IOS -käyttöjärjestelmässä on useita eritasoisia komentotiloja, joita ovat *user executive mode, privileged executive mode, global configuration mode* sekä palvelu- ja porttikohtaiset komentotilat. *User executive mode* on hyvin rajoittunut tila, jossa pääsee tarkastelemaan laitteen tilaa muutamien valvontakomentojen avulla. Se ei anna käyttäjän tehdä muutoksia laitteen asetuksiin. /6, s. 414–417./

Privileged executive mode puolestaan mahdollistaa laitteen tilan yksityiskohtaisemman tarkastelun, testauksen ja asetustiedostojen hallinnan. *Global configuration modea* käytetään koko laitteen toimintaan vaikuttavien asetusten määrittämiseen. Lisäksi on olemassa monia palvelu- tai porttikohtaisia komentotiloja, joissa annetut komennot vaikuttavat vain kyseessä olevan palvelun tai portin toimintaan. /6, s. 414–417./

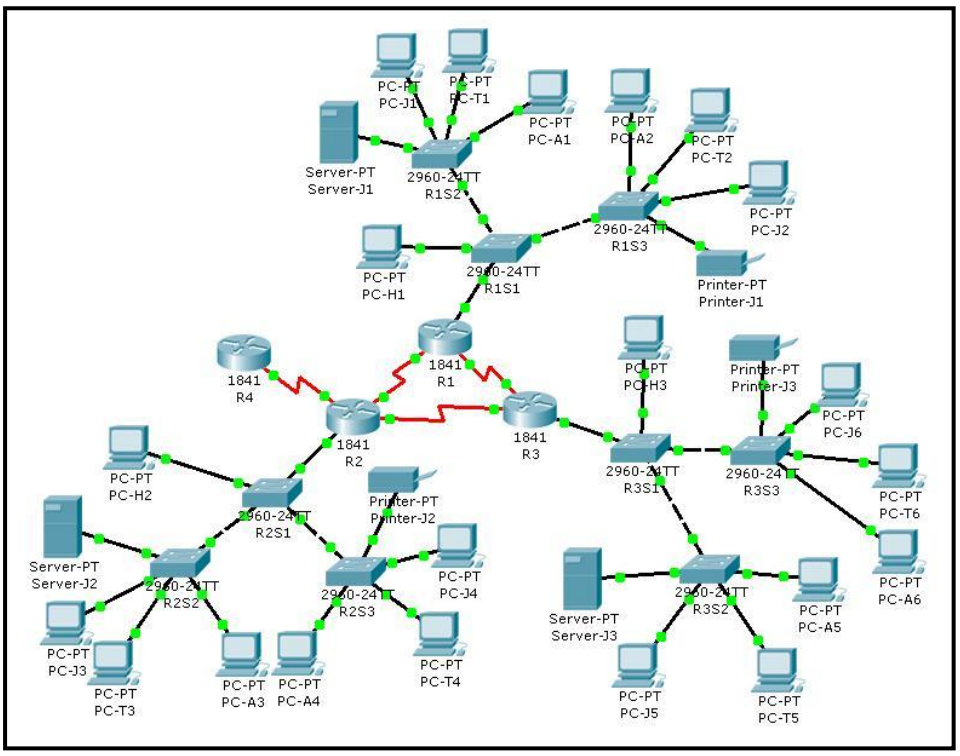
```
hostname>enable
hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hostname(config)#interface fastethernet0/1
hostname(config-if)#exit
hostname(config)#router ospf 1
hostname(config-router)#end
hostname#
```

KUVA 12. Siirtyminen eri komentotilojen välillä

Käytössä olevan komentotilan voi tunnistaa komentokehotteesta (kuva 12). Komentokehote alkaa aina laitteen nimellä, joka on seuraavissa esimerkeissä *hostname*. User executive modessa komentokehote on muodossa *hostname>*, privileged executive modessa *hostname#*, global configuration modessa *hostname(config)#* ja palvelu- tai porttikohtaisissa komentotiloissa *hostname(config-mode)#*. Tällöin sanan *mode* tilalla on kyseessä olevaa palvelua tai porttia kuvaava merkintä. /6, s. 415–416./

5.2 Katsaus esimerkkiverkkoon

Esimerkkiverkon rakenne on esitetty kuvassa 13. Verkossa on yhteensä yhdeksän Cisco Catalyst 2960 -kytkintä ja neljä Cisco 1841 -reititintä. Reitittimien R1, R2, R3 ja R4 asetukset ovat liitteissä 3–6 ja kytkimien R1S1, R1S2 ja R1S3 asetukset liitteissä 7–9. Muiden kytkimien asetukset vastaavat hyvin pitkälti tämän kolmikon asetuksia, joten niitä ei esitetä liitteissä.



KUVA 13. Esimerkkiverkon rakenne

IP-osoitteet

Verkon IP-osoitteistus on toteutettu siten, että osoiteavaruus 192.168.1.0 /24 on jaettu pienempiin aliverkkoihin (taulukko 6) käyttämällä eripituisia aliverkon peitteitä. Jokainen virtuaalilähiverkko muodostaa oman IP-aliverkkonsa. Tämän lisäksi reitittimien väliset yhteydet ovat myös aliverkkoja. Verkon laitteiden IP-osoitteet ovat liitteessä 1.

TAULUKKO 6. Esimerkkiverkon aliverkot

		Aliverkko		**Aliverkko**
VLAN:t	R1 VLAN 10	192.168.1.192 /29	R1 VLAN 20	192.168.1.96 /28
	R2 VLAN 10	192.168.1.200 /29	R2 VLAN 20	192.168.1.112 /28
	R3 VLAN 10	192.168.1.208 /29	R3 VLAN 20	192.168.1.128 /28
	R1 VLAN 30	192.168.1.0 /27	R1 VLAN 99	192.168.1.144 /28
	R2 VLAN 30	192.168.1.32 /27	R2 VLAN 99	192.168.1.160 /28
	R3 VLAN 30	192.168.1.64 /27	R3 VLAN 99	192.168.1.176 /28
Reitittimien väliset yhteydet	R1-R2	192.168.1.216 /30		
	R1-R3	192.168.1.220 /30		
	R2-R3	192.168.1.224 /30		

Aliverkkojen muodostaminen vaihtelevan pituisen aliverkon peitteen avulla on keino säästää IP-osoitteita varaamalla aliverkkoihin ennakoitujen tarpeiden mukaiset määrät laiteosoitteita. IP-osoitteen laiteosan pituus kertoo, kuinka paljon osoitteita aliverkossa on. Kun laiteosan pituutta kasvatetaan bitti kerrallaan, osoitteiden määrä kasvaa kahden potensseina. Esimerkiksi yhdellä laiteosan bitillä saadaan kaksi osoitetta, kahdella bitillä neljä osoitetta, kolmella bitillä kahdeksan osoitetta, neljällä bitillä kuusitoista osoitetta ja niin edelleen. On kuitenkin muistettava, että näistä osoitteista yksi on aina verkon osoite ja toinen yleislähetysosoite, joita ei voida määritellä yksittäisille laitteille.

Esimerkkiverkon aliverkotuksessa on lähdetty liikkeelle ennakkoarvioiden perusteella suurimmiksi kaavailluista Aspa-virtuaalilähiverkoista (VLAN 30). Näiden kolmen aliverkon IP-osoitteiden laiteosat ovat 5-bittisiä, mikä mahdollistaa yhteensä 30 IP-osoitteen määrittelyn kunkin aliverkon laitteille.

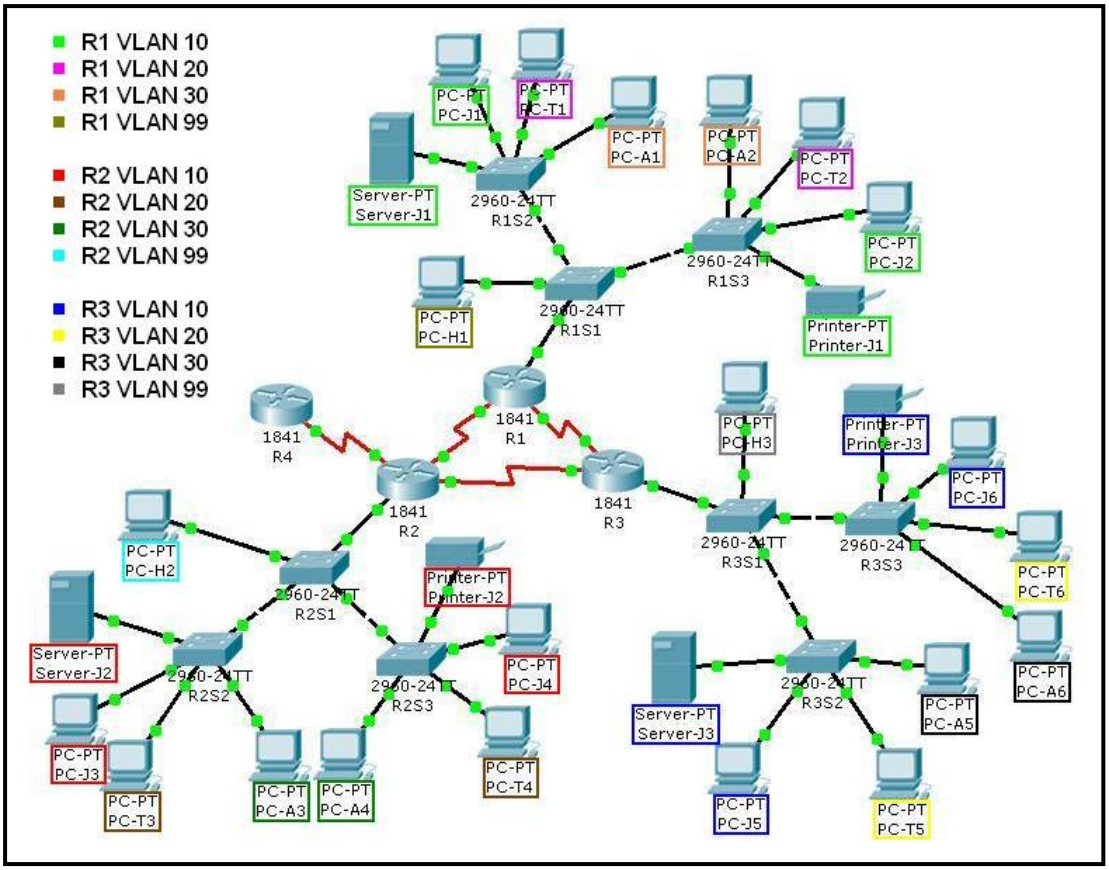
Toimisto- (VLAN 20) ja Hallinta-virtuaalilähiverkkoon (VLAN 99) mahtuu puolestaan 4-bittisten laiteosien myötä 14 laiteosoitetta. Johto-virtuaalilähiverkot (VLAN 10) saavat tyytyä 3-bittisten laiteosien vuoksi kuuteen laiteosoitteeseen. Reitittimien väliset yhteydet ovat vain kahden laitteen välisiä yhteyksiä, joten niille riittävät 2-bittiset laiteosat, jotka tarjoavat täsmälleen sopivan määrän osoitteita kahdelle laitteelle.

Yksityisten IP-osoitteiden suuren määrän vuoksi esimerkkiverkon aliverkoista olisi voitu toki tehdä paljon suurempiakin. Jokainen aliverkko olisi voitu muodostaa vaikkapa samalla aliverkon peitteellä. Esimerkiksi käyttämällä pelkästään aliverkon peitettä 255.255.255.0 olisi jokaiseen aliverkkoon mahtunut 254 laitetta. Tällöin jokaisessa aliverkossa olisi ollut reilusti ylimääräisiä osoitteita, mikä toisaalta vähentäisi verkon osoitteistuksen suunnittelutyötä, mikäli jokin aliverkoista kasvaisi laitemäärältään ennakoitua suuremmaksi.

Kytkimet

Kytkimet R1S1, R2S1 ja R3S1 toimivat VTP-palvelimina ja muut kytkimet ovat VTP-asiakkaita. Näin ollen esimerkiksi kytkimeen R1S1 tehdyt virtuaalilähiverkkomääritysmuutokset päivittyvät automaattisesi kytkimiin R1S2 ja R1S3. Tämä helpottaa

ajantasaisten määritysten ylläpitoa, sillä tarvittavat muutokset täytyy tehdä vain VTP-palvelimiin. Kuvassa 14 on esitetty, mihin virtuaalilähiverkkoon kukin esimerkkiverkon päätelaite kuuluu.



KUVA 14. Esimerkkiverkon virtuaalilähiverkot

Jokaiseen VTP-palvelimeen on määritetty neljä eri virtuaalilähiverkkoa, jotka ovat Johto (VLAN 10), Toimisto (VLAN 20), Aspa (VLAN 30) ja Hallinta (VLAN 99). VTP-asiakkaiden portit FastEthernet 0/1–3 on määritetty kuuluvaksi Johtoon, portit FastEthernet 0/4–10 Toimistoon ja portit FastEthernet 0/11–24 Aspaan (liite 2). Näihin portteihin saadaan tarvittaessa kytkettyä eri virtuaalilähiverkkoihin tarkoitettuja päätelaitteita. Kuvassa 15 näkyvät kytkimen R1S2 VTP-palvelimelta vastaanottamat virtuaalilähiverkkomääritykset ja eri virtuaalilähiverkkoihin kuuluvat portit.

```
R1S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/2
10   johto                            active    Fa0/1, Fa0/2, Fa0/3
20   toimisto                         active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10
30   aspa                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
99   hallinta                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

KUVA 15. Kytkimen R1S2 virtuaalilähiverkkomääritykset

VTP-palvelimien ja VTP-asiakkaiden sekä VTP-palvelimien ja reitittimien väliset yhteydet voivat siirtää useiden virtuaalilähiverkkojen liikennettä. Näiden yhteyksien kytkinportit on määritelty runkoyhteysporteiksi (trunk port). Kytkimiä voidaan hallita työasemien PC-H1, PC-H2 ja PC-H3 kautta, sillä niiden kytkinportit on määritetty kuuluviksi Hallinta-virtuaalilähiverkkoon (VLAN 99) ja kytkimien Hallinta-virtuaalilähiverkoille on määritetty IP-osoitteet samoista aliverkoista kuin kyseisille työasemille. Työasemalla PC-H1 voidaan hallita kytkimiä R1S1, R1S2 ja R1S3, työasemalla PC-H2 kytkimiä R2S1, R2S2 ja R2S3 sekä työasemalla PC-H3 kytkimiä R3S1, R3S2 ja R3S3. Kaikkien kytkimien käyttämättömät portit on sammutettu komennolla 1.

hostname(config-if)#**shutdown** (1)

Kytkimet on määritelty VTP-palvelimiksi komennolla 2 ja VTP-asiakkaiksi komennolla 3. VTP-toimialueet on määritelty komennolla 4 ja VTP-salasanat komennolla 5. Kytkimet R1S1, R1S2 ja R1S3 kuuluvat toimialueeseen R1, kytkimet R2S1, R2S2 ja R2S3 toimialueeseen R2 ja kytkimet R3S1, R3S2 ja R3S3 toimialueeseen R3. VTP-salasana kaikissa kytkimissä on testi.

hostname(config)#**vtp mode server** (2)

hostname(config)#**vtp mode client** (3)

hostname(config)#**vtp domain** (toimialueen nimi) (4)

hostname(config)#**vtp password** (salasana) (5)

Virtuaalilähiverkot on luotu komennolla 6 ja nimetty komennolla 7. Kytkimien portit on määritelty kuulumaan virtuaalilähiverkkoihinsa komennolla 8. Runkoyhteysportit on puolestaan määritelty komennoilla 9 ja 10. Hallinta-virtuaalilähiverkkoja varten (VLAN 99) on jokaiselle kytkimelle määritetty oma IP-osoite komennolla 11.

hostname(config)#**vlan** (virtuaalilähiverkon numero) (6)

hostname(config-vlan)#**name** (virtuaalilähiverkon nimi) (7)

hostname(config-if)#**switchport access** (virtuaalilähiverkon numero) (8)

hostname(config-if)#**switchport mode trunk** (9)

hostname(config-if)#**switchport trunk native vlan 99** (10)

hostname(config-if)#**ip address** (IP-osoite) (aliverkon peite) (11)

Reitittimet

Reitittimet R1, R2 ja R3 toimivat DHCP-palvelimina, jotka jakavat verkkoasetuksia virtuaalilähiverkkojen 10, 20 ja 30 laitteille (kuva 16). Palvelimien ja tulostimien verkkoasetukset on määritelty manuaalisesti. Niiden ja reitittimien IP-osoitteet on rajattu pois DHCP-palvelimen avulla jaettavien osoitteiden listalta. Reitittimien FastEthernet 0/0 -porteille on määritetty aliportteja (subinterface). Virtuaalilähiverkoille 10, 20 ja 30 on olemassa omat aliporttinsa, mikä mahdollistaa tietoliikenteen reitityksen kyseisten virtuaalilähiverkkojen välillä.

```
R3#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.212    000A.F3A0.D2AC            --                    Automatic
192.168.1.213    00D0.BCAA.D258            --                    Automatic
192.168.1.130    0060.4714.7291            --                    Automatic
192.168.1.131    0001.638B.CA3A            --                    Automatic
192.168.1.67     00D0.589A.CB5A            --                    Automatic
192.168.1.66     0002.178C.B292            --                    Automatic
```

KUVA 16. Reitittimen R3 DHCP:n avulla jakamia IP-osoitteita

DHCP:n avulla jaettavien IP-osoitteiden listat on luotu komennon 12 avulla. Tämän jälkeen kunkin listan osoitteet on määritelty komennolla 13. Lisäksi oletusyhdyskäytävä on määritelty komennolla 14. DHCP:n avulla jaettavien osoitteiden listoilta on jätetty osoitteita pois komennolla 15.

hostname(config)#**ip dhcp pool** (listan nimi) (12)

hostname(dhcp-config)#**network** (aliverkon osoite) (aliverkon peite) (13)

hostname(dhcp-config)#**default-router** (IP-osoite) (14)

hostname(config)#**ip dhcp excluded-address** (ensimmäinen pois jätettävä osoite) (viimeinen pois jätettävä osoite) (15)

Reitittimien FastEthernet-porttien aliportit on luotu komennon 16 avulla. Tämän jälkeen aliportit on määritelty vastaanottamaan haluttujen virtuaalilähiverkkojen liikenne komennolla 17. Aliporteille on myös annettu IP-osoitteet komennolla 18.

hostname(config)#**interface** (aliportin nimi) (16)

hostname(config-subif)#**encapsulation dot1q** (virtuaalilähiverkon numero) (17)

hostname(config-subif)#**ip address** (IP-osoite) (aliverkon peite) (18)

Reitittimien väliset yhteydet on toteutettu WIC-2T-moduulien avulla. Ne sisältävät kaksi sarjaporttia. Toinen reitittimistä tarjoaa kahden reitittimen väliselle yhteydelle kellotahdin. Tämä kellotahti on määritetty komennon 19 avulla. Reitittimien väliset yhteydet käyttävät PPP-protokollaa, joka on otettu käyttöön komennolla 20.

hostname(config-if)#**clock rate** (kellotahti) (19)

hostname(config-if)#**encapsulation ppp** (20)

Reitittimien R1, R2 ja R3 välillä on käytössä OSPF-reititysprotokolla. Reitittimet on määritetty kertomaan kaikista niihin suoraan yhdistetyistä reiteistä muille reitittimille OSPF:n avulla. Reitittimeen R2 on määritetty oletusreitti, jonka avulla muut laitteet saavat yhteyden reitittimeen R4. Reitin R4 simuloi julkisessa verkossa sijaitsevaa laitetta ja reititin R2 toimii yksityisen ja julkisen verkon rajapintana. Kuvassa 17 on reitittimen R3 reititystaulu, josta käyvät ilmi sen tuntemat reitit. Osa reiteistä on suoraan yhdistettyjä reittejä ja osa on OSPF:n kautta opittuja.

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.225 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 14 subnets, 5 masks
O       192.168.1.0/27 [110/65] via 192.168.1.221, 00:16:02, Serial0/0/0
O       192.168.1.32/27 [110/65] via 192.168.1.225, 00:16:02, Serial0/0/1
C       192.168.1.64/27 is directly connected, FastEthernet0/0.30
O       192.168.1.96/28 [110/65] via 192.168.1.221, 00:16:02, Serial0/0/0
O       192.168.1.112/28 [110/65] via 192.168.1.225, 00:16:02, Serial0/0/1
C       192.168.1.128/28 is directly connected, FastEthernet0/0.20
O       192.168.1.192/29 [110/65] via 192.168.1.221, 00:16:02, Serial0/0/0
O       192.168.1.200/29 [110/65] via 192.168.1.225, 00:16:02, Serial0/0/1
C       192.168.1.208/29 is directly connected, FastEthernet0/0.10
O       192.168.1.216/30 [110/128] via 192.168.1.225, 00:16:02, Serial0/0/1
                         [110/128] via 192.168.1.221, 00:16:02, Serial0/0/0
C       192.168.1.220/30 is directly connected, Serial0/0/0
C       192.168.1.221/32 is directly connected, Serial0/0/0
C       192.168.1.224/30 is directly connected, Serial0/0/1
C       192.168.1.225/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 192.168.1.225, 00:16:02, Serial0/0/1
```

KUVA 17. Reitittimen R3 reititystaulu

OSPF on otettu käyttöön komennon 21 avulla. Tämän jälkeen on määritelty reitittimeen suoraan yhdistetyt aliverkot, joista reititin ilmoittaa naapurireitittimilleen. Tämä on tehty komennolla 22. Lisäksi reitin R2 on saatu ilmoittamaan oletusreitistään OSPF:n kautta muille reitittimille komennolla 23. Itse oletusreitti on määritetty reitittimeen R2 komennolla 23. Reitittimille R1, R2 ja R3 on määritetty myös ID-arvot komennolla 24.

hostname(config)#**router ospf** (OSPF-prosessin numero) (21)

hostname(config-router)#**network** (aliverkon osoite) (wildcard mask) **area** (OSPF-alueen numero) (22)

R2(config-router)#**default-information originate** (23)

R2(config)#**ip route 0.0.0.0 0.0.0.0 serial0/1/0** (23)

hostname(config-router)#**router-id** (reitittimen ID-arvo) (24)

Reitin R2 suorittaa osoitteenmuunnosta. Käännettäviksi on määritelty kaikki osoitteet osoiteavaruudesta 192.168.1.0 /24. Osoitteenmuunnoksen tyyppi on porttimuunnos ja se kääntää sisäisen osoiteavaruuden 192.168.1.0 /24 osoitteet ulkoiseksi osoitteeksi 101.202.40.44, joka on reitittimen R2 portin Serial 0/1/0 osoite. Reitittimen R2 aliportit FastEthernet 0/0.10, 0/0.20 ja 0/0.30 sekä sarjaportit Serial 0/0/0 ja 0/0/1 on määritetty sisäisten aliverkkojen porteiksi. Portti Serial 0/1/0 puolestaan on ulkoisen verkon portti. Kuvassa 18 näkyvät reitittimen R2 suorittamat osoitteenmuunnokset, kun reitittimelle R4 on lähetetty ping-paketti kuudelta työasemalta. Inside local -osoite on työaseman sisäinen osoite, jota se käyttää yksityisessä verkossa. Reititin kääntää tämän osoitteen julkisessa verkossa käytettäväksi ulkoiseksi osoitteeksi, joka on nimetty kuvassa inside global -osoitteeksi. Outside local ja outside global -osoitteet ovat puolestaan yhteyksien julkisessa verkossa sijaitsevien osapuolten osoitteita.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 101.202.40.44:1   192.168.1.196:1    101.202.40.1:1     101.202.40.1:1
icmp 101.202.40.44:1024192.168.1.197:1    101.202.40.1:1     101.202.40.1:1024
icmp 101.202.40.44:1025192.168.1.204:1    101.202.40.1:1     101.202.40.1:1025
icmp 101.202.40.44:1026192.168.1.205:1    101.202.40.1:1     101.202.40.1:1026
icmp 101.202.40.44:1027192.168.1.212:1    101.202.40.1:1     101.202.40.1:1027
icmp 101.202.40.44:1028192.168.1.213:1    101.202.40.1:1     101.202.40.1:1028
```

KUVA 18. Reitittimen R2 osoitteenmuunnoksen avulla kääntämät IP-osoitteet

Käännettäviksi valitut IP-osoitteet on määritelty pääsylistan (access-list) avulla. Pääsylista on luotu komennolla 25. Tämän jälkeen osoitteenmuunnos on otettu käyttöön komennolla 26. Sisäisten aliverkkojen portit on määritelty komennolla 27 ja ulkoisen verkon portti komennolla 28.

R2(config)#**access-list 1 permit 192.168.1.0 0.0.0.255** (25)

R2(config)#**ip nat inside source list 1 interface serial0/1/0 overload** (26)

R2(config-if)#**ip nat inside** (27)

R2(config-if)#**ip nat outside** (28)

6 YHTEENVETO

Tietoliikennetekniikoiden ja -protokollien tunteminen on hyödyllistä tietoverkkojen suunnittelun, toteutuksen ja ylläpidon kannalta. Tietoliikennetekniikasta on julkaistu runsaasti kirjallisuutta, jonka kautta omaa tietämystään voi kasvattaa. Tietoliikennetekniikka kehittyy kuitenkin niin nopeasti, että tiedonhaussa on otettava tarkasti huomioon tiedon ajantasaisuus. Kaikista esimerkkiverkon toiminnalle tärkeimmistä tekniikoista ja protokollista löytyy kiitettävästi teoriatietoa sekä alan kirjallisuudesta että Internetistä.

Tietoverkkojen luominen Cisco Packet Tracer -ohjelmalla on helppoa, kun tietää tarvittavat perusasiat niiden toiminnasta sekä kytkimien ja reitittimien konfiguroinnista Cisco IOS -käyttöjärjestelmän komentorivin avulla. Packet Tracer tarjoaa oivallisen työkalun verkkojen toteuttamisen harjoitteluun ja niiden toiminnan testaamiseen. Sen

avulla on mielenkiintoista tehdä uusia kokeiluja ja hankkia vastauksia mieltä askarruttaviin seikkoihin. Koska Ciscon valmistamat tietoliikennelaitteet ovat erittäin yleisiä, niiden konfigurointia ja ylläpitoa varten on saatavilla paljon tietoa ja neuvoja eri lähteistä. Esimerkkiverkon toteuttamisessa ei tullut vastaan erikoisia yllätyksiä, vaan kaikki sujui jouhevasti ja odotetunlaisesti.

LÄHTEET

1 Hakala, Mika & Vainio, Mika. Tietoverkon rakentaminen. Jyväskylä: Docendo. 2002.

2 Granlund, Kaj. Tietoliikenne. Jyväskylä: Docendo. 2007.

3 Sosinsky, Barrie. Networking Bible. Indianapolis: Wiley Publishing. 2009.

4 Hämeen-Anttila, Tapio. Tietoliikenteen perusteet. Jyväskylä: Docendo. 2003.

5 Kaario, Kimmo. TCP/IP-verkot. Jyväskylä: Docendo. 2002.

6 Dye, Mark A., McDonald, Rick & Rufi, Antoon W. Network Fundamentals, CCNA Exploration Companion Guide. Indianapolis: Cisco Press. 2008.

7 Learn Networking. 2008. The Difference Between Straight Through, Crossover And Rollover Cables. WWW-dokumentti. Learn Networking. http://learn-networking.com/network-design/the-difference-between-straight-through-crossover-and-rollover-cables Päivitetty 27.1.2008. Luettu 14.11.2011.

8 Cisco. CCNA Exploration Course Booklet: Accessing the WAN, Version 4.0. Indianapolis: Cisco Press. 2010.

9 Cisco. Cisco Catalyst 2960 Series Switches. WWW-dokumentti. Cisco. http://www.cisco.com/en/US/products/ps6406/prod_view_selector.html Ei päivitystietoa. Luettu 14.11.2011.

10 Cisco. CCNA Exploration Course Booklet: LAN Switching and Wireless, Version 4.0. Indianapolis: Cisco Press. 2010.

11 Cisco. Cisco 1841 Integrated Services Router. WWW-dokumentti. Cisco. http://www.cisco.com/en/US/products/ps5875/prod_view_selector.html Ei päivitystietoa. Luettu 14.11.2011.

12 Graziani, Rick & Johnson, Allan. Routing Protocols and Concepts, CCNA Exploration Companion Guide. Indianapolis: Cisco Press. 2008.

13 Cisco. 2010. Cisco Packet Tracer. PDF-dokumentti. Cisco. http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html Ei päivitystietoa. Luettu 18.11.2011.

LIITE 1(1).

Laitteiden IP-osoitteet

Laite	Liitäntä	IP-osoite	Aliverkon peite	Oletusyhdyskäytävä
R1	Fa0/0.10	192.168.1.193	255.255.255.248	-
	Fa0/0.20	192.168.1.97	255.255.255.240	-
	Fa0/0.30	192.168.1.1	255.255.255.224	-
	S0/0/0	192.168.1.217	255.255.255.252	-
	S0/0/1	192.168.1.221	255.255.255.252	-
R2	Fa0/0.10	192.168.1.201	255.255.255.248	-
	Fa0/0.20	192.168.1.113	255.255.255.240	-
	Fa0/0.30	192.168.1.33	255.255.255.224	-
	S0/0/0	192.168.1.218	255.255.255.252	-
	S0/0/1	192.168.1.225	255.255.255.252	-
	S0/1/0	101.202.40.44	255.255.252.0	-
R3	Fa0/0.10	192.168.1.209	255.255.255.248	-
	Fa0/0.20	192.168.1.129	255.255.255.240	-
	Fa0/0.30	192.168.1.65	255.255.255.224	-
	S0/0/0	192.168.1.222	255.255.255.252	-
	S0/0/1	192.168.1.226	255.255.255.252	-
R4	S0/0/0	101.202.40.1	255.255.252.0	-
R1S1	VLAN 99	192.168.1.146	255.255.255.240	192.168.1.145
R1S2	VLAN 99	192.168.1.147	255.255.255.240	192.168.1.145
R1S3	VLAN 99	192.168.1.148	255.255.255.240	192.168.1.145
R2S1	VLAN 99	192.168.1.162	255.255.255.240	192.168.1.161
R2S2	VLAN 99	192.168.1.163	255.255.255.240	192.168.1.161
R2S3	VLAN 99	192.168.1.164	255.255.255.240	192.168.1.161
R3S1	VLAN 99	192.168.1.178	255.255.255.240	192.168.1.177
R3S2	VLAN 99	192.168.1.179	255.255.255.240	192.168.1.177
R3S3	VLAN 99	192.168.1.180	255.255.255.240	192.168.1.177
Server-J1	NIC	192.168.1.194	255.255.255.248	192.168.1.193
Server-J2	NIC	192.168.1.202	255.255.255.248	192.168.1.201
Server-J3	NIC	192.168.1.210	255.255.255.248	192.168.1.209
Printer-J1	NIC	192.168.1.195	255.255.255.248	192.168.1.193
Printer-J2	NIC	192.168.1.203	255.255.255.248	192.168.1.201
Printer-J3	NIC	192.168.1.211	255.255.255.248	192.168.1.209
PC-J1	NIC	DHCP	255.255.255.248	192.168.1.193
PC-J2	NIC	DHCP	255.255.255.248	192.168.1.193
PC-J3	NIC	DHCP	255.255.255.248	192.168.1.201
PC-J4	NIC	DHCP	255.255.255.248	192.168.1.201
PC-J5	NIC	DHCP	255.255.255.248	192.168.1.209
PC-J6	NIC	DHCP	255.255.255.248	192.168.1.209

Laitteiden IP-osoitteet

Laite	Liitäntä	IP-osoite	Aliverkon peite	Oletusyhdyskäytävä
PC-T1	NIC	DHCP	255.255.255.240	192.168.1.97
PC-T2	NIC	DHCP	255.255.255.240	192.168.1.97
PC-T3	NIC	DHCP	255.255.255.240	192.168.1.113
PC-T4	NIC	DHCP	255.255.255.240	192.168.1.113
PC-T5	NIC	DHCP	255.255.255.240	192.168.1.129
PC-T6	NIC	DHCP	255.255.255.240	192.168.1.129
PC-A1	NIC	DHCP	255.255.255.224	192.168.1.1
PC-A2	NIC	DHCP	255.255.255.224	192.168.1.1
PC-A3	NIC	DHCP	255.255.255.224	192.168.1.33
PC-A4	NIC	DHCP	255.255.255.224	192.168.1.33
PC-A5	NIC	DHCP	255.255.255.224	192.168.1.65
PC-A6	NIC	DHCP	255.255.255.224	192.168.1.65
PC-H1	NIC	192.168.1.158	255.255.255.240	-
PC-H2	NIC	192.168.1.174	255.255.255.240	-
PC-H3	NIC	192.168.1.190	255.255.255.240	-

LIITE 2.

Kytkimien porttien tehtävät

Kytkin	Portit	Tehtävä	Aliverkko
R1S1	G1/1-2	trunk (native VLAN 99)	192.168.1.144 /28
	Fa0/1	trunk (native VLAN 99)	192.168.1.144 /28
	Fa0/2	VLAN 99 (hallinta)	192.168.1.144 /28
	Fa0/3-24	VLAN 1	-
R1S2	G1/1-2	trunk (native VLAN 99)	192.168.1.144 /28
	Fa0/1-3	VLAN 10 (johto)	192.168.1.192 /29
	Fa0/4-10	VLAN 20 (toimisto)	192.168.1.96 /28
	Fa0/11-24	VLAN 30 (aspa)	192.168.1.0 /27
R1S3	G1/1-2	trunk (native VLAN 99)	192.168.1.144 /28
	Fa0/1-3	VLAN 10 (johto)	192.168.1.192 /29
	Fa0/4-10	VLAN 20 (toimisto)	192.168.1.96 /28
	Fa0/11-24	VLAN 30 (aspa)	192.168.1.0 /27
R2S1	G1/1-2	trunk (native VLAN 99)	192.168.1.160 /28
	Fa0/1	trunk (native VLAN 99)	192.168.1.160 /28
	Fa0/2	VLAN 99 (hallinta)	192.168.1.160 /28
	Fa0/3-24	VLAN 1	-
R2S2	G1/1-2	trunk (native VLAN 99)	192.168.1.160 /28
	Fa0/1-3	VLAN 10 (johto)	192.168.1.200 /29
	Fa0/4-10	VLAN 20 (toimisto)	192.168.1.112 /28
	Fa0/11-24	VLAN 30 (aspa)	192.168.1.32 /27
R2S3	G1/1-2	trunk (native VLAN 99)	192.168.1.160 /28
	Fa0/1-3	VLAN 10 (johto)	192.168.1.200 /29
	Fa0/4-10	VLAN 20 (toimisto)	192.168.1.112 /28
	Fa0/11-24	VLAN 30 (aspa)	192.168.1.32 /27
R3S1	G1/1-2	trunk (native VLAN 99)	192.168.1.176 /28
	Fa0/1	trunk (native VLAN 99)	192.168.1.176 /28
	Fa0/2	VLAN 99 (hallinta)	192.168.1.176 /28
	Fa0/3-24	VLAN 1	-
R3S2	G1/1-2	trunk (native VLAN 99)	192.168.1.176 /28
	Fa0/1-3	VLAN 10 (johto)	192.168.1.208 /29
	Fa0/4-10	VLAN 20 (toimisto)	192.168.1.128 /28
	Fa0/11-24	VLAN 30 (aspa)	192.168.1.64 /27
R3S3	G1/1-2	trunk (native VLAN 99)	192.168.1.176 /28
	Fa0/1-3	VLAN 10 (johto)	192.168.1.208 /29
	Fa0/4-10	VLAN 20 (toimisto)	192.168.1.128 /28
	Fa0/11-24	VLAN 30 (aspa)	192.168.1.64 /27

LIITE 3(1).

Reitittimen R1 asetukset

```
Current configuration : 1566 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
ip dhcp excluded-address 192.168.1.193 192.168.1.195
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.97
!
ip dhcp pool VLAN10
 network 192.168.1.192 255.255.255.248
 default-router 192.168.1.193
ip dhcp pool VLAN20
 network 192.168.1.96 255.255.255.240
 default-router 192.168.1.97
ip dhcp pool VLAN30
 network 192.168.1.0 255.255.255.224
 default-router 192.168.1.1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.193 255.255.255.248
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.97 255.255.255.240
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.1.1 255.255.255.224
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.1.217 255.255.255.252
```

```
 encapsulation ppp
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.1.221 255.255.255.252
 encapsulation ppp
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.31 area 0
 network 192.168.1.96 0.0.0.15 area 0
 network 192.168.1.192 0.0.0.7 area 0
 network 192.168.1.216 0.0.0.3 area 0
 network 192.168.1.220 0.0.0.3 area 0
!
ip classless
!
line con 0
line vty 0 4
 login
!
end
```

LIITE 4(1).

Reitittimen R2 asetukset

```
Current configuration : 1952 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
ip dhcp excluded-address 192.168.1.201 192.168.1.203
ip dhcp excluded-address 192.168.1.33
ip dhcp excluded-address 192.168.1.113
!
ip dhcp pool VLAN10
 network 192.168.1.200 255.255.255.248
 default-router 192.168.1.201
ip dhcp pool VLAN20
 network 192.168.1.112 255.255.255.240
 default-router 192.168.1.113
ip dhcp pool VLAN30
 network 192.168.1.32 255.255.255.224
 default-router 192.168.1.33
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.201 255.255.255.248
 ip nat inside
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.113 255.255.255.240
 ip nat inside
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.1.33 255.255.255.224
 ip nat inside
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

LIITE 4(2).

Reitittimen R2 asetukset

```
interface Serial0/0/0
 ip address 192.168.1.218 255.255.255.252
 encapsulation ppp
 ip nat inside
!
interface Serial0/0/1
 ip address 192.168.1.225 255.255.255.252
 encapsulation ppp
 ip nat inside
 clock rate 64000
!
interface Serial0/1/0
 ip address 101.202.40.44 255.255.252.0
 encapsulation ppp
 ip nat outside
!
interface Serial0/1/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.1.32 0.0.0.31 area 0
 network 192.168.1.112 0.0.0.15 area 0
 network 192.168.1.200 0.0.0.7 area 0
 network 192.168.1.216 0.0.0.3 area 0
 network 192.168.1.224 0.0.0.3 area 0
 default-information originate
!
ip nat inside source list 1 interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
line con 0
line vty 0 4
 login
!
end
```

LIITE 5(1).

Reitittimen R3 asetukset

```
Current configuration : 1540 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
ip dhcp excluded-address 192.168.1.209 192.168.1.211
ip dhcp excluded-address 192.168.1.65
ip dhcp excluded-address 192.168.1.129
!
ip dhcp pool VLAN10
 network 192.168.1.208 255.255.255.248
 default-router 192.168.1.209
ip dhcp pool VLAN20
 network 192.168.1.128 255.255.255.240
 default-router 192.168.1.129
ip dhcp pool VLAN30
 network 192.168.1.64 255.255.255.224
 default-router 192.168.1.65
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.209 255.255.255.248
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.129 255.255.255.240
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.1.65 255.255.255.224
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.1.222 255.255.255.252
 encapsulation ppp
```

LIITE 5(2).

Reitittimen R3 asetukset

```
!
interface Serial0/0/1
 ip address 192.168.1.226 255.255.255.252
 encapsulation ppp
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 192.168.1.64 0.0.0.31 area 0
 network 192.168.1.128 0.0.0.15 area 0
 network 192.168.1.208 0.0.0.7 area 0
 network 192.168.1.220 0.0.0.3 area 0
 network 192.168.1.224 0.0.0.3 area 0
!
ip classless
!
line con 0
line vty 0 4
 login
!
end
```

LIITE 6.

Reitittimen R4 asetukset

```
Current configuration : 595 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R4
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 101.202.40.1 255.255.252.0
 encapsulation ppp
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
line con 0
line vty 0 4
 login
!
end
```

LIITE 7(1).

Kytkimen R1S1 asetukset

```
Current configuration : 1518 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1S1
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 99
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
```

```
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet1/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface GigabitEthernet1/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.1.146 255.255.255.240
!
ip default-gateway 192.168.1.145
```

```
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

LIITE 8(1).

Kytkimen R1S2 asetukset

```
Current configuration : 2073 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1S2
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/5
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 30
!
```

```
interface FastEthernet0/12
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/19
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/21
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/24
```

```
 switchport access vlan 30
 shutdown
!
interface GigabitEthernet1/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface GigabitEthernet1/2
 switchport trunk native vlan 99
 switchport mode trunk
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.1.147 255.255.255.240
!
ip default-gateway 192.168.1.145
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

LIITE 9(1).

Kytkimen R1S3 asetukset

```
Current configuration : 2073 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1S3
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/5
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 30
!
```

```
interface FastEthernet0/12
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/19
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/21
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/24
```

```
 switchport access vlan 30
 shutdown
!
interface GigabitEthernet1/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface GigabitEthernet1/2
 switchport trunk native vlan 99
 switchport mode trunk
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.1.148 255.255.255.240
!
ip default-gateway 192.168.1.145
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```