LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

TAITAJA2014-TAPAHTUMAN VERKKOSUUNNITELMA

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2013
Juha-Pekka Varis

Lahden ammattikorkeakoulu
Tietoliikennetekniikan koulutusohjelma

VARIS, JUHA-PEKKA: Taitaja2014-tapahtuman verkkosuunnitelma

Tietoliikennetekniikan opinnäytetyö, 71 sivua, 14 liitesivua

Syksy 2013

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli laatia verkkosuunnitelma Taitaja2014-tapahtumaan, mikä järjestetään Lahden Messukeskuksessa. Verkkosuunnitelman pohjalta voidaan tehdä tietoverkon toteuttamiseen tarvittavat laite- ja tarvikehankinnat, kaapelointi, verkon aktiivilaitteiden sijoittaminen ja konfigurointi.

Tietoverkko koostuu muun muassa seuraavista aktiivilaitteista: kytkimistä, reitittimistä ja palomuureista. Kytkin yhdistää siihen kytketyt laitteet toisiinsa, ja kytkimen tehtävänä on ottaa vastaan segmentistä tulevia kehyksiä, tallentaa kehykset muistiinsa ja lähettää ne eteenpäin oikeaan segmenttiin. Reitittimeen voidaan kytkeä muita laitteita, ja reitittimen tehtävänä on reitittää eli ohjata liikennettä eri verkkojen välillä. Palomuuri on laite tai ohjelmisto, jolla voidaan estää ulkoverkosta tulevat hyökkäykset yrityksen tai kotikäyttäjän sisäverkkoon joko käyttämällä pakettisuodatinta tai sovellussiltaa.

Verkkosuunnittelu koostuu tarpeiden kartoittamisesta, ennakoimisesta eli laajennusvarasta ja senhetkisten hyvien tapojen ja standardien vaatimusten täyttämisestä. Suunnittelussa voidaan käyttää hyväksi monentyyppisiä suunnitteluprosesseja, kuten hanke-, luonnos- ja toteutussuunnittelua, joka soveltuu yleiskaapelointiin.

Taitaja2014-tapahtumassa tulee olemaan noin 50 lajia, joihin tarvitaan toimitsijoille ja kilpailijoiden käyttöön nykykäsityksen mukaan 138 tietokonetta. Verkkokapasiteetti on suunniteltu 276 tietokoneelle, jotta jokaista oikeaa tarvetta varten olisi yksi varapaikka. Verkkoliikenne jaetaan seitsemään eri verkkoon käyttämällä kytkimissä VLAN:ja, jotka määritellään porttikohtaisesti tarpeen mukaan ja kytkimien oikeista porteista vedetään lajipisteisiin oikeisiin käyttäjiin. Taitaja2014-tapahtuman runkoverkon toteuttamiseen aktiivilaitteita tarvitaan 18 kytkintä ja 1 varajärjestelmällä varmistettu palomuuri ja reititin sekä 803 metriä CAT6-parikaapelia. WLAN-verkkoja tarvitaan ainakin kaksi, yleisölle ja toimitsijoille omat.

Asiasanat: Taitaja2014-tapahtuma, kaapelointi, topologia, verkkosuunnitelma, aktiivilaitteet, WLAN

Lahti University of Applied Sciences
Degree Programme in Information Technology

VARIS, JUHA-PEKKA: Network Plan for the Taitaja2014 Event

Bachelor's Thesis in Information Technology, 71 pages, 14 pages of appendices

Autumn 2013

ABSTRACT

The aim of this Bachelor's thesis was to draw up an information network plan for the Taitaja2014 event, which is held in the Lahti Messukeskus. On the basis of the information network plan, network equipment and supplies acquisitions, cabling and active network device placement and configuration can be carried out.

Among other things, an information network consists of the following active devices: switches, routers, and firewalls. The devices are connected to each other by a switch. The function of a switch is to receive frames from network segments, store the frames in its memory and send them forward to the right network segments. The function of a router is to route, direct, traffic between networks. A firewall is a device or a piece of software that can prevent external network attacks within a company or a home user's network by using either packet filtering or application layer filtering.

Designing a network consists of mapping the needs, anticipating the need for extension and meeting current best practices and the requirements of standards. In designing, many kinds of designing processes can be used, such as project plan, sketch design, and detailed design, which is suitable for general cabling.

The Taitaja2014 event is going to have about 50 events. In these events, it is anticipated that the officials and competitors will need 138 computers. Network capacity is designed for 276 computers, so that for each computer there will be one in reserve. Network traffic is divided into seven networks with VLAN using switches. The VLANs are defined to a switch per port as required, and from each switch there is a cable wired to event point from the appropriate ports to the appropriate user.

To implement the Taitaja2014 event network for active devices there is a need for 18 switches, one back-up system confirmed firewall / router and 803 meters of CAT6 twisted-pair cable. There is a need for at least two separate WLANs, one for the public and one for the officials.

Key words: Taitaja2014 event, cabling, topology, network plan, active devices, wireless LAN

SISÄLLYS

LYHENNELUETTELO

AES Advanced Encryption Standard, salausmenetelmä

CARP Common Address Reduncancy Protocol, palomuurin protokolla, joka sallii useiden isäntien jakaa IP-osoiteryhmän samassa lähiverkossa

CSMA/CA Carrier Sense Multiple Access With Collision Avoidance, WLANin käyttämä siirtotien varausmenetelmä

CSMA/CD Carrier Sense Multiple Access With Collision Detection, ethernetin käyttämä siirtotien varausmenetelmä

CTR Counter, AES-jonosalaajan toimintamuoto

CTS Clear To Send, viesti, jolla laitteelle annetaan lupa lähettää

DHCP Dynamic Host Configuration Protocol, verkkoprotokolla, jonka avulla uudet lähiverkkoon liittyvät asiakaslaitteet voivat pyytää konfiguraatioasetuksia

DNS Domain Name System, Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi

DSSS Direct Sequence Spread Spectrum, suorasekvenssi hajaspektri

FHSS Frequency Hopping Spread Spectrum, taajuushyppely hajaspektri

GHz Gigahertsi, taajuuden yksikkö

IEEE Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö, jonka toimintaa on tietotekniikan standardoiminen

IP-osoite, Internet Protocol osoite, Internetissä tietokoneen tunnistamiseen käytettävä numero

IPsec Internet Protocol Security, joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen

IR Infra Red, infrapuna

ISM Industrial, Scientific and Medical, taajuusalue, jonka käyttö ei vaadi lupaa

LAN Local Area Network, rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko

LED Light-Emitting Diode, hohtodiodi

MAC Media Access Control, verkossa liikennöintiin käytetty järjestelmä

Mbps Megabittiä sekunnissa

NAT Network address translation, menetelmä, jossa sisäverkon IP-osoite käännetään toiseksi ulkoverkossa näkyväksi IP-osoitteeksi

OFDM Orthogonal Frequency-division Multiplexing, monikantoaaltotekniikka

OSI-malli Open Systems Interconnection Reference Model, tiedonsiirtoprotokollien kuvaamiseen käytetty 7-kerroksinen malli

PHKK Päijät-Hämeen Koulutuskonserni, maakunnallinen koulutuksen järjestäjä, kehittäjä ja ylläpitäjä, jonka tulosalueita ovat Koulutuskeskus Salpaus, Lahden ammattikorkeakoulu ja Tuoterengas

RC4 Rivest Cipher 4, jonosalaus

RF Radio Frequency, radioaallot

RSTP Rapid Spanning Tree Protocol, kytkimen protokolla, joka estää useampien samanaikaisten yhteyksien muodostumisen ei-reitittävien aktiivilaitteiden välille

RTS Request To Send, viesti, jolla laite ilmoittaa olevansa valmis lähettämään

SSID service set identifier, langattoman lähiverkon yksilöivä tunniste

STP Shielded Twisted Pair, suojattu kierretty parikaapeli

STP Spanning Tree Protocol, kytkimen protokolla, joka estää useampien samanaikaisten yhteyksien muodostumisen ei-reitittävien aktiivilaitteiden välille

UTP Unshielded Twisted Pair, suojaamaton kierretty parikaapeli

VLAN Virtual LAN, virtuaalinen lähiverkko

VPN Virtual Private Network, virtuaalinen erillisverkko

VTP Virtual Trunking Protocol, kytkimen protokolla, jolla laitteet voivat muodostaa oman VTP-verkon

WEP Wired Equivalent Privacy, 802.11:n WLAN:n salausmenetelmä

WLAN Wireless Local Area Network, langaton lähiverkko

WPA Wi-Fi Protected Access, 802.11:n WLAN:n salausmenetelmä

WPA2 Wi-Fi Protected Access 2, 802.11:n WLANin salausmenetelmä

1 JOHDANTO

1.1 Työn tausta ja tavoitteet

Tämän työn tavoitteena on tehdä Taitaja2014-tapahtumaan verkkosuunnitelma, jonka perusteella voidaan tehdä tietoverkon toteuttamiseen tarvittavat laite- ja tarvikehankinnat, kaapelointi, verkon aktiivilaitteiden sijoittaminen ja konfigurointi. Pelkän teoreettisen suunnittelun varaan pohjautuva uusi verkko voi kohdata yllättäviä ongelmia, joten suunnitelman testaus on tärkeää. Testaamiseen ei käytetä mitään valmista suunnittelumallia, vaan testisuunnitelmaa laaditaan kohta kohdalta edellisten tulosten pohjalta.

Laite- ja verkkotestaukset suoritetaan LAMK:n tietoliikennelaboratorion tiloissa. Verkon testaaminen laboratorio-olosuhteissa tuo omat haasteensa, sillä on hankalaa luoda kooltaan, liikennemäärältä, asiakaslaitemäärältään ja liikenteen monimuotoisuudelta vastaavaa verkkoa kuin todellisuudessa. Nämä haasteet pyritään selvittämään hyvällä alkusuunnittelulla Taitaja2014-tapahtuman tarpeista ja tilojen ominaisuuksista, jotta pystytään simuloimaan mahdollisimman hyvin varsinaista Taitaja2014-tapahtumassa käytettävän verkon rakennetta ja toimintaa.

Työn teoriassa keskitytään verkkosuunnitelmassa tarvittavien komponenttien ominaisuuksiin, kuten kaapelointiin, verkon aktiivilaitteisiin ja ohjelmistoihin sekä langattomaan lähiverkkoon. Kaapeloinnissa tutustutaan eri kaapelityyppeihin ja kaapeloinnin suunnitteluun. Verkon aktiivilaitteet ja ohjelmistot tulevat pitämään sisällään kytkimen, reitittimen ja palomuurin ominaisuuksia sekä virtuaalisen lähiverkon ja pfSense-ohjelmiston esittelyn. Langattoman lähiverkon teoriassa keskitytään eri standardien vertailuun ja salaukseen.

1.2 Taitaja2014-tapahtuma

Taitaja on Skills Finland ry:n vuosittain organisoima ammatillisen koulutuksen suurtapahtuma ja nuorten alle 20-vuotiaiden ammatillisessa koulutuksessa olevien ammattitaidon SM-kilpailu. Ensimmäinen Taitaja-kilpailu pidettiin vuonna 1989, ja siinä kilpailijoita oli kolmisenkymmentä kahdessa lajissa. Nykyään Taitaja-kilpailu on alansa suurin tapahtuma. Ennen finaalia Taitaja-kilpailusta järjestetään

kymmeniä semifinaaleja ja niihin osallistuu yli tuhat kilpailijaa. (Skills Finland ry 2013.)

Vuoden 2014 Taitaja-kilpailun finaalin järjestää Koulutuskeskus Salpaus Taitaja2014-tapahtumassa, ja se pidetään 8.–10.4.2014 Lahden Messukeskuksessa ja sen lähellä sijaitsevissa Koulutuskeskus Salpauksen tiloissa. Tapahtumassa kilpailee noin 400 opiskelijaa noin 45 ammattialalla. Näiden lisäksi tapahtumassa on kaksi näytöslajia sekä yksi ammattinäytös. Tapahtumaan ei ole sisäänpääsymaksua, ja sen kokonaiskävijämääräksi odotetaan jopa 40 000 ihmistä. Mainoskuva tapahtumasta on kuviossa 1. (Taitaja2014 2013.)

KUVIO 1. Taijaja2014-tapahtuman mainoksia (Taitaja2014 2013)

2 KAAPELOINTI

2.1 Yleiskaapelointi

Yleiskaapeloinnin lähtökohtana on ollut ajatus, että tietoliikennekaapelointi on osa rakennusten perusjärjestelmää ja palvelee useita sovelluksia, perinteisen sovelluskohtaisen verkon sijaan. Yleiskaapeloinnin tärkeimmät ominaisuudet ovat seuraavat:

- rakennuksen valmistumisen yhteydessä asennettava sovelluksista riippumaton tietoliikennekaapelointi
- kaapeloinnin vaatimien tilojen ja johtoteiden huomioiminen rakennussuunnitelmissa
- kaapelointijärjestelmä helposti ja edullisesti muunneltavissa käyttäjien tarpeiden mukaisesti
- standardoidut rakenneosat, joiden laatu ja suorituskyky on määriteltyjä
- rakenneosien kilpailuttamisen mahdollisuus
- kaapelointijärjestelmän tuki nykyisille tietoliikennetekniikan tuotteille ja järjestelmille ja näiden tuotekehitykselle.

(SFS-käsikirja 167 2004, 7 - 8.)

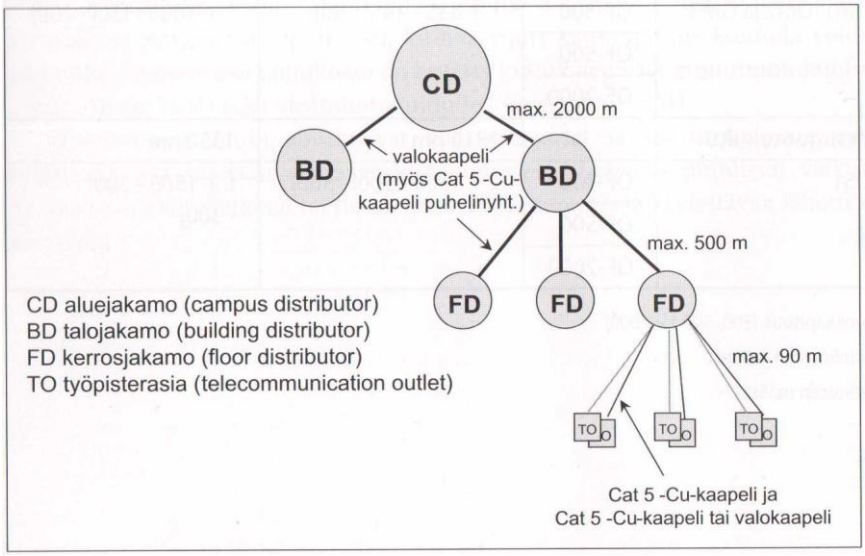
Nykyaikainen uudisrakennusten kaapelointi perustuu yleiskaapelointistandardeihin, joita ovat eurooppalainen EN 50173 ja kansainvälinen ISO/IEC 11801. Standardisarja EN 50173 sisältää neljä omaa standardia eri käyttöympäristöille: toimistoille, teollisuudelle, kodeille ja datakeskuksille. Standardeissa määritetään kaapeloinnin rakenne ja kokoonpano, toteutusvaihtoehdot ja suorituskykyvaatimukset. Yleiskaapelointi mahdollistaa yhtenäisen lähiverkkokokonaisuuden rakentamisen, jolloin verkon laajentaminen, hallinta ja vikojen paikallistaminen on helppoa. (Koivisto 2009b, 57; Tietosähkö 2013.)

Yleiskaapelointi koostuu kolmesta osajärjestelmistä, jotka ovat aluekaapelointi, nousukaapelointi ja kerroskaapelointi taulukon 1 ja kuvion 2 mukaisesti. Standardissa EN 50173-1 on määritelty kiinteistötyypistä riippumaton

runkokaapelointi, johon kuuluvat aluekaapelointi ja nousukaapelointi. (Yleiskaapelointijärjestelmät 2008, 44 - 45.)

TAULUKKO 1. Osajärjestelmien kaapelityypit (Hakala & Vainio 2005, 118)

Osajärjestelmien ensi- ja toissijaiset kaapelityypit		
Osajärjestelmä	**Kaapeli**	**Käyttötarkoitus**
Aluekaapelointi	Valokaapeli Cat 5–7 -kuparikaapelit	Kaikki sovellukset Puheensiirto
Nousukaapelointi	Valokaapeli, Cat 5–7 -kuparikaapelit	Datansiirto Puheensiirto (A–C-luokat)
Kerroskaapelointi	Cat 5–7 -kuparikaapelit Valokaapeli	Kaikki sovellukset Nopea datansiirto



KUVIO 2. Yleiskaapeloinnin osajärjestelmät ja niihin liittyvät kaapelipituudet (Hakala & Vainio 2005, 120)

Aluekaapelointiin sisältyy aluejakamosta talojakamoon ulottuva kaapelointi ja sen päätteet sekä aluejakamon ristikytkennät, joilla kytketään yhteen kaikki saman alueen rakennukset. Aluekaapelointi on toteutettava valokuidulla, ja sen

maksimipituus ei saa ylittää 2000:ta metriä. (Jaakohuhta 2005, 57; Schneider Electric 2013, 52.)

Nousukaapeloinnilla tarkoitetaan talojakamosta kerrosjakamoon tai -jakamoihin asti ylettyvää kaapelointia. Siihen sisältyvät nousukaapelit, niiden päätteet talo- ja kerrosjakamoissa sekä talojakamossa sijaitsevat ristikytkennät. Nousukaapelointi suositellaan toteuttavaksi valokuidulla, mutta myös korkealuokkaisen kierretyn parikaapelin käyttö on mahdollista. Nousukaapelin maksimipituus on 500 metriä. (Jaakohuhta 2005, 50, 57; Yleiskaapelointijärjestelmät 2008, 45.)

Kerroskaapelointi yhdistää yhden kerrosjakamon ja työpisterasiat. Lisäksi kerroskaapelointi kattaa kerrosjakamoissa sijaitsevat kerroskaapeloinnin päätteet ja ristikytkennät. Isoihin ja raskaisiin dataverkkoihin suositellaan käytettäväksi valokuitua. Pienemmille kuormituksille sopii suojattu tai suojaamaton parikaapeli. Kerroskaapeloinnin sallittu enimmäispituus on 90 metriä. (Jaakohuhta 2005, 55; Schneider Electric 2013, 52.)

Yleiskaapeloinnin siirtotiessä toimivat sovellukset on jaettu kuuteen luokkaan kaistanleveyden perusteella sekä optiseen luokkaan. Määriteltäessä yleiskaapeloinnissa käytettävää sovellusta tulee ottaa huomioon sovelluksen luokka ja luokalle soveltuva kaapelityyppi. Sovellusten luokat on esitelty taulukossa 2. (Hakala & Vainio 2005, 116 - 117.)

TAULUKKO 2. Kanavien ja siirtoteiden luokat sekä niiden sovellusvaihtoehdot (Hakala & Vainio 2005, 117)

Siirtoteiden luokat	
Luokka	**Käyttö (sovellukset)**
A (= 100 kHz)	Analogiset puhelimet (POTS, PSTN), X.21
B (= 1 MHz)	ISDN perus- ja järjestelmäliittymä
C (= 16 MHz)	10BaseT,100BaseT2, 100BaseT4, 4 Mb/s TokenRing
D (= 100 MHz)	100BaseT, 1000BaseT 16 Mb/s TokenRing, ATM-TP, CDDI
E (= 250 MHz	1000BaseTx, ATM LAN 1,2 Gb/s
F (= 600 MHz)	FC-100TP
Optinen	10BaseFL, 10BaseFB, 100BaseFX, 1000BaseSX, 1000BaseLX, 10GbaseSR/SW, 10GbaseLR/LW, 10GbaseER/EW, 10GbaseLX4/ LW4, FDDI, ATM

2.2 Kaapelityypit

Tiedonsiirron nopeus ja luotettavuus perustuu suurimmilta osin kaapelityyppeihin, jotka voidaan tietoverkoissa luokitella kolmeen pääryhmään: koaksiaali-, perikierrettyihin ja optisiin kuitukaapeleihin. Joitakin näistä kaapelityypeistä voidaan käyttää myös muualla kuin tietokoneverkoissa. (Meyers 2003, 71.)

Nykyaikainen rakennusten sisäkaapelointi toteutetaan useimmiten parikaapeleilla ja valokuitua käytetään runkoverkoissa. Vanhemmissa verkoissa saattaa olla käytössä myös koaksiaalikaapelia. Kaapelityypin valinnassa on huomioitava seuraavat seikat:

- kaapeleiden käyttö ja asennettavuus
- kaapeleiden etäisyydet ja siirtonopeudet
- kaapeleiden häiriösuoja ja hinta.

(OAMK 2013.)

2.2.1 Koaksiaalikaapeli

Koaksiaalikaapeli on vanhin lähiverkoissa käytetty kaapelityyppi, jota on aikoinaan käytetty hyvien signaalinsiirto-ominaisuuksiensa vuoksi. Koaksiaalikaapeli koostuu kuvion 3 mukaisesti keskijohtimesta, sitä suojaavasta eristeestä, punotusta ulkojohtimesta ja kaapelin muovivaipasta. Joissakin kaapeleissa on ulkojohtimen ja eristekerroksen välissä foliokerros, joka estää ulkopuolisten häiriöiden summautumista siirrettävään signaaliin. Ulkojohtimen ja keskijohtimen välissä oleva eristekerros on tärkein osa koaksiaalikaapelia, sillä sen ominaisuuksista riippuu hyvin pitkälti kaapelin laatu. Koaksiaalikaapelin keski- ja ulkojohdin ovat johtavaa materiaalia, joiden avulla signaali välittyy. (Sähkötieto ry 2008, 111; Kompo 2010.)

KUVIO 3. Koaksiaalikaapelin rakenne (Wikipedia 2013b)

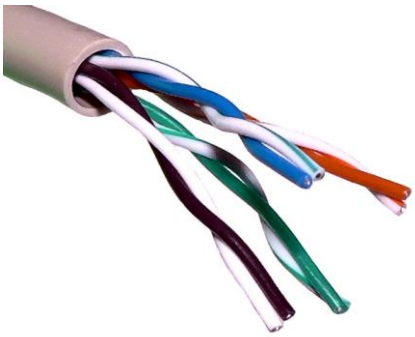
Verkoissa on käytetty aikojen saatossa kolmea eri koaksiaalikaapelityyppiä RG-58, RG-6 ja RG-8. Paksu ethernet-kaapelijärjestelmä 10Base5 perustui RG-8-tyyppiseen koaksiaalikaapeliin, joka on vanhin ja vähiten käytetty. Termi 10Base5 tarkoittaa 10 Mbps nopeudella toimivaa ethernet-verkkoa, jossa kaapelien enimmäispituus on 500 m. Suosituin ja edullisin koaksiaalikaapelityyppiin RG-58 perustuva ethernet-kaapelijärjestelmä on ohut ethernet 10Base2. Molempien ethernetien heikkoutena on haavoittuvuus, sillä väylän katkeaminen pudottaa kaikki samassa segmentissä olevat työasemat pois verkosta. Nykyään

koaksiaalikaapelin yleisimmät sovellukset ovat kaapelitelevisio- ja tukiasemajärjestelmät sekä antennikaapelit. (Meyers 2003, 72 - 74, 98 - 99, 103.)

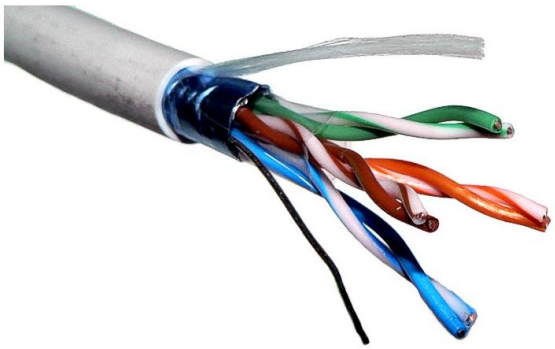
2.2.2 Parikaapeli

Parikaapeli eli symmetrinen kaapeli on käytetyin kaapelityyppi nykyaikaisissa verkoissa. Parikaapeli koostuu yhdestä tai useammasta eristetystä ja kierretystä metallijohdinparista, jotka on kierretty toistensa ympärille. Parikaapelin etuna muihin kaapelityyppeihin ovat edullisuus, keveys, joustavuus ja helppo asennettavuus. Lisäksi parikaapelilla voidaan saavuttaa huomattavasti suuremmat nopeudet kuin esimerkiksi koaksiaalikaapelilla. (Teleasennusopas 2005, 12; Dulaney & Harwood 2011, 215.)

Parikaapelit voivat olla kokonaan tai osittain (osa johdinpareista) sähköisesti suojattuja. Suojatuissa kaapeleissa kaapelit tai johdinparit voidaan suojata erillisellä maadoitetulla vaipalla, joka vähentää kaapelista lähtevää ja siihen tulevaa elektromagneettista säteilyä parantaen sen suorituskykyä ja turvallisuutta. Kuvion 4 mukaiset suojaamattomat parikaapelit (UTP, Unshielded Twisted Pair) ovat yleisempiä kuin kuvion 5 mukaiset suojatut parikaapelit (STP, Shielded Twisted Pair) halvemman hintansa vuoksi. Jos ympäristöissä esiintyy paljon sähkömagneettista häiriötä, käytetään yleensä suojattua parikaapelia. (Granlund 2007, 44.)



KUVIO 4. Suojaamaton kierretty parikaapeli (UTP) (Wikipedia 2013f)



KUVIO 5. Suojattu kierretty parikaapeli (STP) (Wikipedia 2013h)

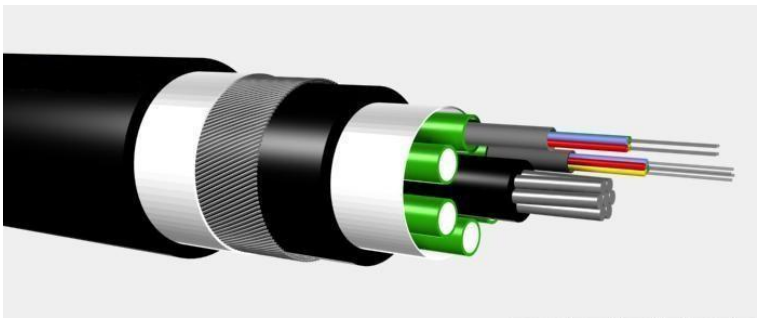
Parikaapelit jaetaan suojaustyyppien lisäksi eri kategorioihin siirtonopeuksien perusteella taulukon 3 mukaisesti. Vuodesta 2002 lähtien on Suomessa käytetty yleiskaapeloinnissa kategoria 6:n (Cat 6) kaapelointia, jossa päästään 1000 Mbps:n maksiminopeuteen. Myös kategoria 6a:n parisuojattu kaapelointi on käytössä. (Wikipedia 2013f.)

TAULUKKO 3. Parikaapeleiden kaapeliluokat (Wikipedia 2013f)

Kategoria	Kaistanleveys	Sovellukset
Cat1	0,4 MHz	Puhe ja modeemiyhteyksiin
Cat2	? MHz	Vanhemmissa päätejärjestelmissä, esimerkiksi IBM 3270
Cat3	16 MHz	10BASE-T ja 100BASE-T4 Ethernet
Cat4	20 MHz	16 Mbit/s Token Ring
Cat5	100 MHz	100BASE-TX & 1000BASE-T Ethernet
Cat5e	100 MHz	100BASE-TX & 1000BASE-T Ethernet
Cat6	250 MHz	1000BASE-T Ethernet
Cat6e	250 MHz	10GBASE-T (kehitteillä) Ethernet
Cat6a	500 MHz	10GBASE-T (kehitteillä) Ethernet
Cat7	600 MHz	Ei sovelluksia vielä.
Cat7a	1000 MHz	Puhelin, CATV, 1000BASE-T samassa kaapelissa.
Cat8	1200 MHz	Kehitteillä, ei sovelluksia vielä.

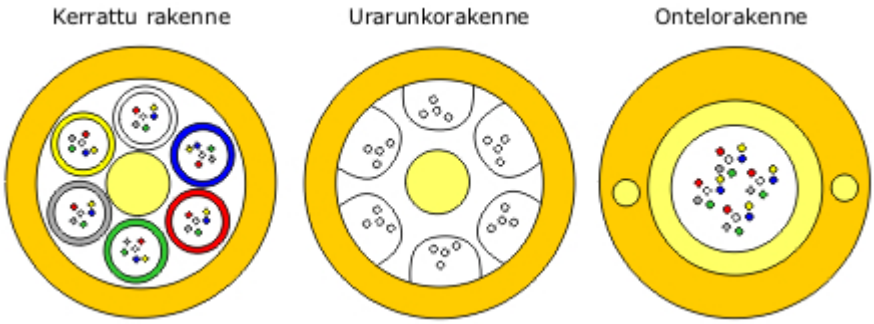
2.2.3 Valokaapeli

Valokaapeli eli optinen kuitu koostuu viidestä osasta eli kuiduista suojuksineen, kaapelisydämestä, veto- ja lujite-elementistä sekä vaipasta kuvion 6 mukaan. Yksi valokuitukaapeli koostuu useasta optisesta kuidusta. Valokuidussa alun perin sähköinen signaali muutetaan siirron ajaksi valopulsseiksi, jolloin tieto etenee valon muodossa. Valoimpulssit etenevät kuidussa kokonaisheijastumisen ansiosta seinämästä seinämään. Valokuituyhteys muodostuu kahdesta samanlaisesta kuidusta, joita toista pitkin lähetetään ja toista pitkin vastaanotetaan signaalia. (Sähkötieto ry 2008, 130.)



KUVIO 6. Valokaapelin rakenne (Wikipedia 2013e)

Kaapelisydämen rakenteena voi olla kerrattu rakenne, urarunkorakenne tai ontelorakenne kuvion 7 mukaisesti. Kerratussa rakenteessa toisiopäällystetyt kuidut tai kuituryhmät on kerrattu samankeskisesti vetoelementtinä toimivan keskielementin ympärille. Kerrattu rakenne on perinteinen ja vanhin valokaapelirakenne. Urarunkorakenteessa kaapelin sydän muodostuu pituussuuntaisia uria sisältävästä muovitangosta. Urarunkorakenteen etuna on hyvä puristuslujuus, rakenteen selkeys asennuksen kannalta ja käyttömahdollisuus sekä sisä- että ulkotiloissa. Ontelorakenteessa kaapelin sydän muodostuu yhdestä putkesta, jonka sisällä ovat ensiöpäällystetyt kuidut. Ontelorakenteella on hyvä puristuslujuus, ja kuidut on ryhmitelty sopivasti niiden tunnistamiseksi. (Koivisto 2009a, 8 - 9.)



KUVIO 7. Valokaapeleiden sydänrakenteet (Kuituinfo 2013)

Yleiskaapeloinnin valokuidut jaetaan niiden toiminnan perusteella yksimuotokuituihin ja monimuotokuituihin. Monimuotokuidussa LED-lähettimellä syötetty valo etenee useassa eri muodossa, mikä aiheuttaa valoimpulssin levenemistä kuidussa ja siten rajoittaa kuidun kaistanleveyttä. Tämän vuoksi monimuotokuitua käytetäänkin lähinnä vain lyhyillä matkoilla eli lähiverkoissa, koska useat valonsäteet heikentävät signaalia. Pidemmillä välimatkoilla käytetään yksimuotokuitua, jossa Laser-lähettimellä syötetty valo etenee vain yhtä reittiä ja antaa siten paremman signaalin. Tämän vuoksi kalliimpaa yksimuotokuitua käytetään runkoverkoissa. (i&i Solutions 2006, 5; Granlund 2007, 48 - 50.)

Valokaapelin suurin ero parikaapeliin verrattuna on tiedon lähetys valoimpulssien avulla, mikä vähentää ulkoisista lähteistä syntyviä häiriötekijöitä. Valokaapelin etuina ovat suuri tiedonsiirtokyky ja kaistanleveys, tietoturvallisuus ja kaapeleiden keveys. Valokuidun monista eduista huolimatta sen käyttö on edelleen melko vähäistä verrattuna parikaapeliin kalliin hinnan ja vaikean asennettavuuden vuoksi. Lähiverkossa valokuituja käytetään lähinnä runkoverkossa ja datakeskusyhteyksissä. (Granlund 2007, 53.)

2.3 Kaapeloinnin suunnittelu ja asennus

Kaapeloinnin suunnittelussa lähdetään liikkeelle kohteen tarpeiden kartoittamisesta, ennakoimisesta eli laajennusvarasta ja senhetkisten hyvien tapojen ja standardien vaatimusten täyttämisestä. Suunnittelussa voidaan käyttää hyväksi monentyyppisiä suunnitteluprosesseja, kuten hanke-, luonnos- ja toteutussuunnittelua, joka soveltuu yleiskaapelointiin. Näissä suunnitteluprosesseissa ei käydä läpi pelkästään kaapeloinnin suunnittelua vaan yleiskaapelointia ja kokonaisen tietoverkon suunnittelua, mutta niiden vaiheita pystyy soveltamaan myös pelkän tietoverkonkaapeloinnin suunnitteluun. Tässä työssä tarkastellaan lähemmin Hämeen-Anttilan Tietoliikenteen perusteet -kirjassa tietoverkkojen rakentamisessa läpikäytyä mallia. (Hämeen-Anttila 2003, 86; Hakala & Vainio 2005, 114.)

2.3.1 Tietoverkkojen rakentaminen - suunnitteluvaihe

Tietoverkkojen rakentamisen suunnitteluvaihe koostuu tarvekartoituksesta ja ennakoivasta tietojen hankinnasta sekä verkon suunnitelmasta. Kohteen tarvekartoituksessa ja ennakoivassa tietojen hankinnassa mietitään, mitä palveluita verkossa tullaan käyttämään ja mitä palveluita tullaan tarjoamaan. Käyttäjien nykyiset tarpeet selvitetään kartoittamalla käyttäjien käyttämät työvälineet, sovellukset ja verkkopalvelut sekä arvioidaan niiden kriittisyys yrityksen toiminnan kannalta. Tarvittaessa verkon palveluiden toiminnan takaamiseksi voidaan palvelut asettaa tärkeysjärjestykseen kriittisyyden perusteella. Tärkeysjärjestys auttaa hyödyntämään verkon kapasiteetin järkevästi, jolloin kapasiteetin loppuessa palveluista tinkiminen aloitetaan vähemmän kriittisistä alueista tai palveluista. Esimerkiksi käyttäjien kotimaisten iltapäivälehtien verkkojulkaisujen selailu ei pitäisi olla niin tärkeätä kuin sähköpostin kulkeminen ja videoneuvottelupuheluiden pitäminen. Tarvekartoituksessa selviää verkkokapasiteetin vaatimukset, verkossa liikkuvan tiedon kriittisyys ja tiedon vaatima tietoturva. (Hämeen-Anttila 2003, 86.)

Verkon suunnittelu voidaan aloittaa tarvekartoituksen jälkeen, koska silloin on tiedossa käyttäjien tarpeet ja verkon fyysiset puitteet, kuten tilan rakennusmateriaali, koko ja muoto sekä huoneiden ja kerrosten määrä. Verkkosuunnitelmia kannattaa tehdä useampia variaatioita, ja niistä kannattaa pyytää tarjouspyyntöjä useammalta taholta. Tarjouspyynnöt kannattaa lähettää etenkin tahoilla, joilla on aiempaa kokemusta samantyylisten (kokoluokka, käytetyt teknologiat, laitteet, kaapelit) verkkojen toteuttamisesta. Verkon suunnittelun yhteydessä on tärkeää tehdä käyttöönottosuunnitelma ja hankintasuunnitelma. Näiden avulla voidaan hankinnat tehdä porrastetusti oikeaan aikaan ja varmistaa verkkokomponenttien saatavuus ajoissa. (Hämeen-Anttila 2003, 86 - 87.)

2.3.2 Tietoverkkojen rakentaminen - toteutusvaihe

Suunnitteluun liittyvien vaiheiden jälkeen siirrytään toteuttamisvaiheeseen, joka koostuu hankinnan toteuttamisesta, asennuksesta ja käyttöönotosta, kaapeloinnista

ja koulutuksesta. Isojen verkkojen hankinnat kannattaa tehdä harkitusti portaittain, sillä verkkokomponenttien hinnat elävät kovasti, teknologia vanhenee nopeasti ja uusia malleja kehitetään jatkuvalla tahdilla. Aikaisemmassa vaiheessa tehty verkkosuunnitelma on hyvä työkalu hankintojen porrastamiseen, sillä siitä selviää, mitä hankitaan, missä aikataulussa ja missä järjestyksessä. (Hämeen-Anttila 2003, 87.)

Hankinnan toteutusta seuraavat asennus ja käyttöönottaminen, joissa mennään jo varsinaiseen konkreettiseen tekemiseen, kuten työasemien asennukseen. Tilanteesta riippuen verkon asentaminen voidaan tehdä kokonaan kohdeyrityksen oman henkilökunnan toimesta, ulkoistaa rutiiniasennusten osalta tai kokonaan. Se mikä näistä vaihtoehdoista on järkevin, riippuu monesta seikasta, ja jokaisessa vaihtoehdossa on hyvät ja huonot puolensa. Mikäli verkon asennusta ei ulkoisteta kokonaan, verkon asentaminen vaatii joka tapauksessa oman henkilökunnan työpanosta ja tutustumista asentajien tekemään verkkoon. Jos esimerkiksi verkko asennettaisiin toimivaan kuntoon, mutta käyttäjien tarpeiden mukainen optimointi jäisi tekemättä, niin henkilökunnan taitojen salliessa voisi olla järkevää tehdä koko verkon asennus itse. Toisaalta tilanteessa, jossa verkko on tarkoin määritelty ja dokumentoitu ja henkilökunta on ollut mukana aikaisemmissa vaiheissa, rutiiniasennusten ulkoistaminen voisi olla hyvinkin järkevää. Tällä tavalla henkilökunnan työresursseja jäisi vapaaksi muihin asioihin. Mikäli asennettava verkko sisältää verkkovastaaville tuntemattomia verkko-ohjelmistoja, palvelinkäyttöjärjestelmiä tai laitteistoja, on niihin tutustumiseen ja hallinnointiin on varattava riittävästi omaa aikaa. (Hämeen-Anttila 2003, 87.)

Hankintojen tapaan on järkevää porrastaa verkkopalveluiden käyttöönottoa. Aloitetaan käyttäjien tarpeiden kannalta olennaisimmista asioista ja siirrytään sitten vähemmän tärkeisiin. Kun kaikki verkkopalvelut on saatu valmiiksi ja toimimaan, voidaan aloittaa verkon monitorointi, keskittyä verkkopalveluiden laadun syventämiseen ja koko verkon toiminnan optimointiin. (Hämeen-Anttila 2003, 88.)

Kaapelointi kerrosjakamon ja työpisteen välillä voidaan toteuttaa esimerkiksi ajanmukaisella parikaapelilla, ja kerrosjakamot voidaan yhdistää toisiinsa

nopeammalla kuituverkolla. Aikaisemmin käytetty, nykyään jo hylätty, vaihtoehto oli toteuttaa kaapelointi ohuella ethernetillä. Jos ohueen ethernet-segmenttiin tuli vika, niin kaikki siinä segmentissä olleet työasemat jäivät ilman verkkoyhteyttä, mikä oli yksi tämän kaapelityypin heikkouksista. Parikaapelin kohdalla vika yleensä vaikuttaa vain yhteen kohteeseen. Parikaapelin etuja aikaisempiin käytettyihin kaapeleihin nähden ovat parempi vikasietoisuus ja muiden tiedonsiirtotekniikoiden tukeminen. Lisäksi parikaapelia voidaan käyttää muuhunkin kuin tietoverkon liikenteeseen, kuten puhelinliikenteeseen. (Hämeen-Anttila 2003, 88.)

Koulutus on tärkeä osa uutta verkkoa, eikä uudella verkolla ja sen palveluilla ole käyttöarvoa, jos verkon käyttäjät eivät osaa käyttää sitä tai hyödyntää sen tarjoamia hienouksia. Koulutuksessa pitää huomioida käyttäjien osaamisen eritasoisuus ja huolehtia, että kaikki saavat heille riittävän koulutuksen verkkoon, sen käyttöön ja palveluihin. Uudenlaisen verkkopalvelun mahdollisuuksien testaamisessa on parempi käyttää testiryhmänä osaa tulevasta käyttäjäryhmästä. Tämä testiryhmä pystyy paikantamaan virheitä, antamaan parannusehdotuksia ja palautetta käyttökokemuksista, joiden perusteella on mahdollista korjata verkon vikoja, tehdä parannuksia verkkoon tai varautua tuleviin ongelmatilanteisiin lopullisen käyttöönoton kohdalla. Palvelusta luopuminen on halvempaa pienen testiryhmän testausvaiheessa kuin täysivaltaisen käyttöönoton jälkeen. (Hämeen-Anttila 2003, 88 - 89.)

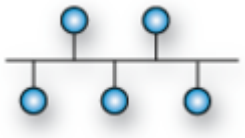
2.4 Verkon topologiat

Verkkotopologia kuvaa tapaa, jolla verkon laitteet on kytketty toisiinsa, ja sitä, millaisen rakenteen ne muodostavat joko fyysisesti tai loogisesti. Fyysinen topologia kuvastaa kirjaimellisesti, miten laitteet on kytketty toisiinsa. Loogisessa topologiassa verkon laitteiden rakenne hahmotellaan niiden toiminnan perusteella eli miten paketit siirtyvät verkossa. (Meyers 2003, 65, 69.)

Verkon topologiat voidaan jakaa kaksi- ja monipisteyhteydellisiin topologioihin. Kaksipisteyhteys muodostetaan nimensä mukaisesti kahdesta laitteesta ja niitä yhdistävästä siirtotiestä. Monipisteyhteydet muodostavat monimutkaisempia

topologioita, jotka taas voidaan jakaa neljään perusverkkotopologiaan: tähti-, rengas-, väylä- ja mesh-topologia. Nykyaikana verkkojen topologiat yleensä ovat yhdistelmiä, koska ne eivät koostu vain yhdestä topologiasta vaan useamman eri perustopologian yhdistelmästä. (Granlund 2007, 77.)

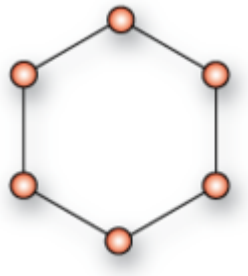
Väylätopologia on vanhin käytössä olevista topologioista, ja siinä kaikki verkon laitteet ovat yhden kaapelin varrella kuvion 8 mukaisesti. Kaapeli päätetään sovitusvastuksella, joka estää signaalien heijastumiset. Väyläkytkennässä laitteet ovat samanarvoisia ja kanavanvaraus perustuu kilpavarausmenettelyyn. Verkkoa voi käyttää vain yksi laite kerrallaan, sillä jos toinen laite yrittää liikennöidä verkossa samaan aikaan, aiheuttaa toinen laite törmäyksen ja ruuhkauttaa verkkoa. Tämä tarkoittaa rajattua laitteiden määrää, mutta väyläverkon rakentamisen yksinkertaisuus ja edullisuus ovat lisänneet sen suosiota esimerkiksi koaksiaalikaapeliverkoissa. Väylätopologiassa yhden laitteen vikaantuminen ei aiheuta koko verkon hajoamista vaan siitä muodostuu yksittäisiä segmenttejä, joiden sisällä liikenne yhä toimii. (Hämeen-Anttila 2003, 29; Granlund 2007, 79.)



KUVIO 8. Väylätopologia (Wikipedia 2013i)

Rengastopologiassa verkon laitteet muodostaa renkaan eli jonon, joka yhdistyy itseensä ja sillä ei ole alkamis- eikä loppumispistettä kuvion 9 mukaisesti. Tässä verkon toiminta vaatii kaikkien laitteiden ja kaapeleiden toimintaa. Jos yksikin laite tai kaapeli rikkoontuu, koko verkko lakkaa toimimasta. Rengastopologiassa lähettämisvuoro kiertää renkaan jokaisella solmulla, ja jos laitteella ei ole mitään lähetettävää, laite antaa vuoron seuraavalla laitteelle. Rengastopologiaa käytetään esimerkiksi verkkoratkaisuissa, joissa tähden muodostaminen on hankalaa ja

kallista pitkien matkojen takia tähden alkuun jokaisen kytkimen luota. (Hämeen-Anttila 2003, 30.)

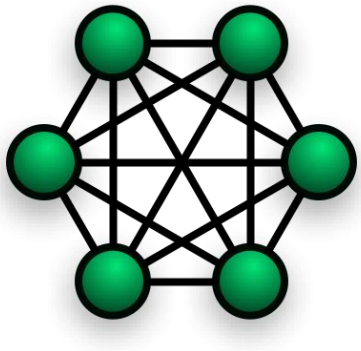


KUVIO 9. Rengastopologia (Wikipedia 2013i)

Nykyaikaisissa lähiverkkokaapeloinneissa on käytössä useimmiten tähtitopologia, jossa laitteet on kytketty aktiivilaitteen porttiin, jonka kautta ne ovat yhteydessä toisiinsa kuvion 10 mukaisesti. Tähtitopologiassa yhden ei-keskuslaitteen rikkoontuessa ja tietoverkkoyhteyden katketessa katoaa yhteys ainoastaan vikaantuneen laitteen perässä oleviin laitteisiin. Mutta keskuslaitteen vikaantuessa hajoaa myös koko verkko, eikä mikään verkon laitteista saa yhteyttä minnekään. (Hämeen-Anttila 2003, 30 - 31.)

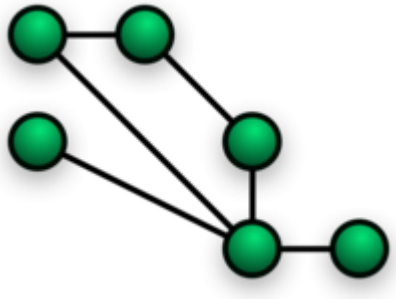
KUVIO 10. Tähtitopologia (Wikipedia 2013i)

Full mesh -topologiassa kaikki verkon laitteet on kytketty toisiinsa erillisillä kaapeleilla kuvion 11 mukaisesti. Tässä topologiassa käytetään eniten kaapelia, mutta toisaalta full mesh -topologia on myös vikasietoisin topologia. Verkon laitteiden tai kaapelien rikkoutuminen ei vaikuta muiden välisiin yhteyksiin, ainoastaan itseensä. Kalleutensa ja hankaluutensa vuoksi full mesh -topologiaa käytetään esimerkiksi korkeaa käytettävyyttä vaativissa verkoissa. (Meyers 2003, 65; Wikipedia 2013d.)



KUVIO 11. Full mesh-topologia (Wikipedia 2013i)

Mesh-topologia (kuvio 12) on periaatteeltaan samantyylinen kuin full mesh -topologia, mutta siinä on ainoastaan jokaisella verkon kriittisillä laitteilla erillinen yhteys toisiinsa, ei kaikilla. Tällä saadaan aikaiseksi vikasietoisuutta ensisijaisen reitin vikaantuessa ja yhteyden katketessa passiivisena ollut yhteys alkaa toimia ja liikenne vaihtuu kulkemaan sen kautta. (Wikipedia 2013f.)



KUVIO 12. Mesh-topologia (Wikipedia 2013d)

Nykyaikana yleisin verkkotopologia on hybriditopologia, jolloin käytetään väylä-, tähti-, rengas- ja mesh-topologioita tarkoitukseen sopivalla tavalla yhdistettyinä. Samalla perusverkkotopologiat sellaisenaan ovat kadonneet käytöstä lähes kokonaan. Esimerkkeinä hybriditopologioista ovat tähtiväylätopologia, jossa useampi tähtitopologiaan perustuva verkko on liitetty yhteen lineaariseen runkoväylään, ja tähtirengastopologia. Hybridiverkot sisältävät siis samankaltaisuuksia kahden tai useamman eri topologiamallin kanssa, mutta tätä verkkoa ei voida kuitenkaan luokitella minkään yksittäisen mukaan. (Meyers 2003, 67, 70.)

3 VERKON AKTIIVILAITTEET JA OHJELMISTOT

3.1 Kytkimet

Kytkin on verkossa toimiva aktiivilaite, joka yhdistää siihen kytketyt laitteet toisiinsa, kytkimeen voidaan yhdistää laitteita, kuten tietokoneita, tulostimia ja palvelimia. Kytkimellä tehty verkko muodostaa loogisen ja fyysisen tähtitopologian ja toimii topologian keskipisteenä, keskuksena. Kytkimet toimivat OSI-mallin tasolla 2, siirtoyhteystasolla. Kerroksen tehtävänä on määritellä lähettävän ja vastaanottavan laitteen fyysiset osoitteet eli MAC-osoitteet ja muodostaa datasta siirrettäviä yksiköitä, kuten kehyksiä. (Hakala & Vainio 2005, 139; Odom 2005, 109 - 110.)

Käytännössä kytkin on moniporttinen silta, joka on useista porteista koostuva laite kuvion 13 mukaisesti. Kytkimen tehtävänä on ottaa vastaan segmentistä tulevia kehyksiä, tallentaa kehykset muistiinsa ja lähettää ne eteenpäin oikeaan segmenttiin. Tilanteessa, jossa kehys ei ole päässyt perille, on tapahtunut törmäys ja kytkin lähettää kehyksen uudestaan. Samassa portissa olevalle kohteelle tarkoitettua kehystä ei lähetetä muihin portteihin eikä tallenneta muistiin. Kytkin pitää kirjaa siihen yhteydessä olevista laitteista, minkä portin takana laitteet ovat, niiden MAC-osoitteista ja muodostaa tiedoista taulukon. Taulukon perusteella kytkin osaa ohjata kehykset oikeisiin portteihin. Mikäli fyysistä osoitetta ei osoitetaulusta löydy, lähettää kytkin sen ulos kaikista porteista (broadcast). (Hakala & Vainio 2005, 84.)

KUVIO 13. Ciscon Catalyst 2960 sarjan 48-porttinen kytkin (Cisco 2013a)

Kytkinten hankinnassa kannattaa kiinnittää huomiota kytkimen osoitemuistin suuruuteen, kapasiteettiin ja tukeen varayhteyksille sekä tuettaviin ominaisuuksiin. Hyödyllisiä ominaisuuksia ovat seuraavat:

- STP (Spanning Tree Protocol) on protokolla, joka estää haitallisten silmukoiden syntymistä ei-reitittävien aktiivilaitteiden välille. STP mahdollistaa myös automaattisten varayhteyksien ylläpidon. Käytännössä tämä tarkoittaa, että aktiivisen linkin mennessä alas STP korvaa sen varayhteydeksi määrätyllä linkillä.
- RSTP (Rapid Spanning Tree Protocol) on samankaltainen protokolla kuin STP, mutta parannetuilla vasteajoilla ja päivitetyillä ominaisuuksilla.
- VTP (Virtual Trunking Protocol) on protokolla, jolla laitteet voivat muodostaa oman VTP-verkon, jossa yksi osapuoli on VTP-palvelimen (server) roolissa ja muut asiakkaiden (client) rooleissa. VLAN-tietokannan hallinnointi tapahtuu VTP-palvelimissa, josta ne päivittyvät automaattisesti asiakasroolissa oleviin osapuoliin.

(Hakala & Vainio 2005, 105; Cisco 2013b; Cisco 2013c.)

3.2 Reitittimet

Reititin on verkon aktiivilaite, johon voidaan kytkeä muita laitteita. Reitittimen erikoispiirre on, että reititin osaa reitittää eli ohjata liikennettä eri verkkojen (osoiteavaruuksien) välillä. Reititin toimii OSI-mallin tasolla 3, verkkokerroksella. Verkkokerroksen tehtävänä on määritellä datapakettien reititys eri verkkojen välillä, priorisoida liikennettä ja lisätä paketteihin loogiset osoitteet. (Hämeen-Anttila 2003, 47; Hakala & Vainio 2005, 139.)

Reitittimet käyttävät joko staattista tai dynaamista reititystä. Staattisessa reitityksessä verkkojen osoitteet syötetään manuaalisesti reititystauluun, ja dynaamisessa reitityksessä reitittimet saavat tietoja verkon osoitteista toisilta reitittimiltä. Reititin ei tiedä, missä laitteet tai kohteet sijaitsevat verkossa, sillä tietäminen olisi epäkäytännöllistä ja tilaa vievää. Sen sijaan reititin tietää, mihin suuntaan liikenne kannattaa ohjata, seuraavalla taholle, joka ei välttämättä

vieläkään tiedä, missä kohde tarkalleen on. Reititin tietää vain seuraavan tahon, joka on kohdetta lähempänä. Tehtävien hoitamisesta huolehtivat tarkoitukseen suunnitellut protokollat, joista lähiverkoissa käytetään lähinnä IP-protokollaa (Internet Protocol). Reitittimeen voidaan yhdistää myös useita palomuurin tehtäviä, kuten kohde- ja lähdeosoitteidenperusteella tapahtuva pakettisuodatus. (Hämeen-Anttila 2003, 47; Odom 2005, 267 - 268.)

DHCP (Dynamic Host Configuration Protocol) on verkkoprotokolla, jonka avulla uudet lähiverkkoon liittyvät asiakaslaitteet voivat pyytää konfiguraatioasetuksia. Näitä konfiguraatioasetuksia ovat muun muassa IP-osoite, oletusyhdyskäytävä (default gatewayn) ja DNS-palvelimen (Domain Name System) osoite. IP-osoitteen pyytäminen on DHCP:n käytetyin ja tärkein ominaisuus. (Meyers 2003, 38.)

IP-osoite eli Internet Protocol address on osoite, jonka avulla voidaan yksilöidä IP-verkon laite. Samassa verkossa ei saa olla kahta samaa IP-osoitteen laitetta eli laitteen osoite pitää olla ainutkertainen. IP-osoitteen avulla laite voi lähettää ja etenkin vastaanottaa IP-verkon liikennettä. IP-osoite on 32-bittinen binääriluku, joka ryhmitetään neljään kahdeksanbittiseen lukuun, oktettiin. Helppouden vuoksi IP-osoitteen oktetit kirjoitetaan desimaalimuotoon ja ne erotetaan toisistaan pisteillä, esimerkiksi 192.168.0.254. (Hakala & Vainio 2005, 211; Odom 2005, 212.)

DHCP:n antama IP-osoite voi olla ylläpitäjän etukäteen määrittelemältä IP-osoiteavaruusalueelta. Annettu IP-osoite on voimassa määrätyn ajan, jonka jälkeen sen jatkokäyttöön tarvitsee pyytää lisää aikaa. Annetut IP-osoitteet voidaan myös antaa osoitetta pyytävän laitteen MAC-osoitteen perusteella, jolloin kyseisellä laitteella olisi siinä verkossa aina sama IP-osoite. (Meyers 2003, 327; Hakala & Vainio 2005, 211 - 212.)

Oletusyhdyskäytävä (default gateway) kertoo asiakaslaitteelle, mihin sen pitää lähettää liikenne, jolle asiakaslaite ei tiedä reititystä. DNS-palvelimen osoite on tärkeä Internet-sivujen selaamisessa, sillä ilman DNS-palvelinta olisi pakko käyttää numeromuodossa olevia IP-osoitteita nimien sijaan. (Meyers 2003, 327; Hakala & Vainio 2005, 240.)

3.3 Palomuuri

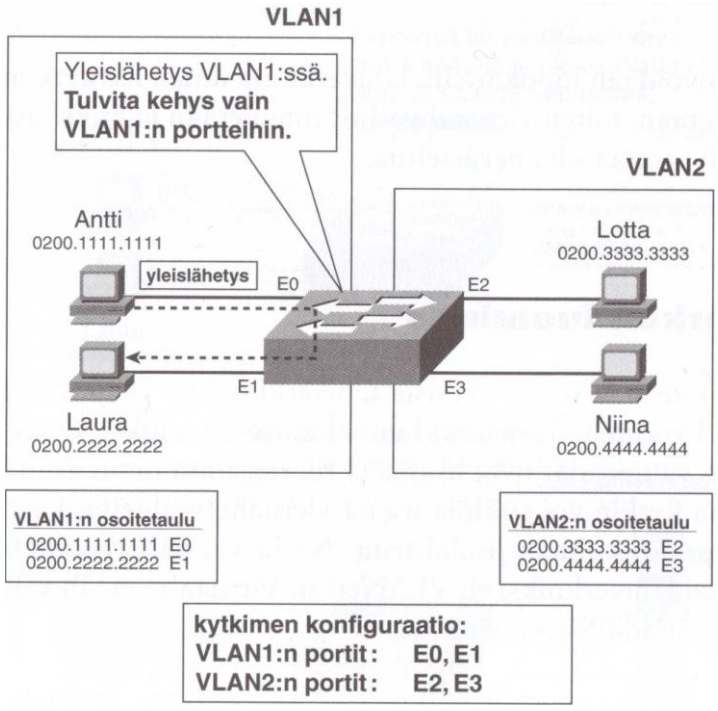
Palomuuri on laite tai ohjelmisto, jolla voidaan estää ulkoverkosta tulevat hyökkäykset yrityksen tai kotikäyttäjän sisäverkkoon. Palomuurit voidaan jakaa kahteen eri perustyyppiin toimintansa perusteella, jotka ovat pakettisuodatin ja sovellussilta. Pakettisuodattimet ovat yleisimpiä ja edullisimpia ratkaisuja, jotka perustuvat yleensä reitittimiin. Pakettisuodattimet vertaavat pakettien käyttämiä porttinumeroita ja IP-osoitteita palomuurille annettuihin määräyksiin ja tarpeen mukaan hylkäävät paketin. Sovellussilta toimii kahden sovelluksen välissä, joista toinen on suojatussa verkossa ja toinen sen ulkopuolella. Sovellussilta analysoi kaiken lävitseen kulkevan liikenteen paketti paketilta ja poistaa seasta vahingolliset paketit. Näiden palomuurien lisäksi on olemassa hybridipalomuureja, joissa on sekä pakettisuodattimen että sovellussillan ominaisuuksia. (Hämeen-Anttila 2003, 81 - 83; Vainio & Hakala 2005, 347.)

CARP (Common Address Reduncancy Protocol) on protokolla, joka sallii useiden isäntien jakaa IP-osoiteryhmän samassa lähiverkossa. CARP:n avulla voidaan luoda laiteklusteri, joka näkyy muille verkossa olijoille yhtenä laitteena. Tämä on hyödyllistä etenkin palomuurien ja reitittimien kohdalla, koska laiteklustereilla voidaan saada muun muassa vikasietoisuutta ja kuorman tasausta. Laiteklusterissa voi esimerkiksi olla yksi aktiivinen päälaite ja loput varalla olevia laitteita, jotka päälaitteen syystä tai toisesta lopettaessa toimintansa jatkavat päälaitteen roolissa. CARP:n avulla varalaitteet voivat jatkaa päälaitteen tekemää tehtävää, jopa niin nopeasti, ettei vaihdos haittaa liikennöintiä tai osapuolet eivät huomaa mitään katkosta. (Countersiege 2013; Wikipedia 2013c.)

3.4 VLAN

VLAN (Virtual LAN) eli virtuaalilähiverkko on kytkimissä ja reitittimissä käytetty tekniikka, jolla yksittäiseen fyysiseen verkkoon voidaan tehdä loogisesti toisistaan erillään olevia verkkoja, yleislähetysalueita (broadcast domain). Yleislähetysalueella olevat laitteet vastaanottavat kaikki toistensa lähettämät yleislähetykset. Yleislähetysalueen sisällä olevat laitteet eivät näe muihin alueisiin eivätkä voi vuorovaikuttaa muihin verkkoihin ilman liikenteen reititystä verkosta

toiseen. Suurissa lähiverkoissa yleislähetysten (broadcast) määrä saattaa kasvaa niin suureksi, että määrä alkaa vaikuttaa verkon toiminnallisuuteen ja ruuhkauttaa kaistaa. Kokonaisverkon toiminnallisuutta ja kaistaa saadaan parannettua jakamalla lähiverkon laitteet VLAN:lla pienempiin verkkoihin, mitä on kuvattu kuviossa 14. (Hakala & Vainio 2005, 93 - 94.)



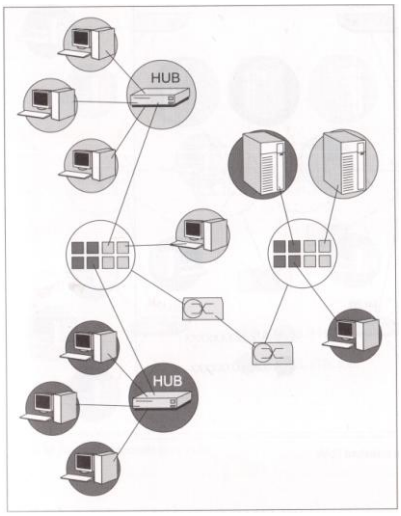
KUVIO 14. Yleislähetyksen kuuluminen VLAN-verkossa (Odom 2005, 138)

Yleislähetys on lähetys, joka ethernetissä lähetetään MAC-kohdeosoitteella FF:FF:FF:FF:FF:FF. Yleislähetyksellä ei ole tiettyä kohdetta, vaan yleislähetys yrittää tavoittaa kaikkia lähiverkon laitteita. Kytkimet ja toistimet jakavat yleislähetyksen kaikkiin portteihin eli jokaiselle, joka on niissä kiinni. Yleislähetyksellä voidaan muun muassa selvittää erinäisiä tietoja verkossa olevista laitteista. (Odom 2005, 132; Wikipedia 2013k.)

VLANeja voidaan käyttää jakamaan verkkoa eri käyttötarkoituksiin ja eri kohderyhmille. Tilapäiset vierailijat voivat esimerkiksi tarvita pääsyä lähiverkosta Internetiin ja lähiverkon joihinkin palveluihin, mutta vierailijoiden ei kuitenkaan

yleensä tarvitse päästä kaikkialle lähiverkossa. Tällaisessa tilanteessa tietoturvallisuuden kannalta on hyvä rajata vierailijat eri verkkoon, mikä onnistuu helposti VLAN:lla. Muita kohderyhmiä VLAN-verkoiksi ovat esimerkiksi tuotanto, hallinto, intranet, WLAN ja ekstranet. (Wikipedia 2013j.)

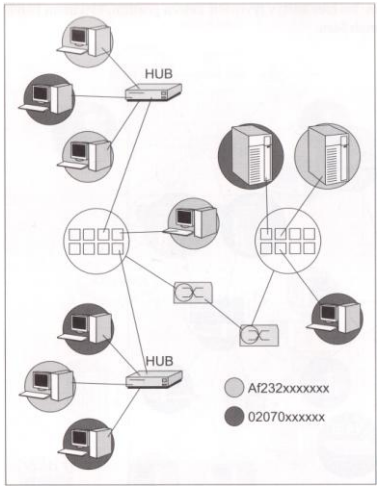
Asiakaslaitteiden VLAN-verkkoihin kuuluminen voidaan määritellä neljällä eri perusteella: kytkimen portin perusteella, MAC-osoitteen perusteella, verkkokerroksen palveluiden perusteella tai Policy-määritysten avulla. Porttiperusteisessa VLAN:ssa (port based VLAN) VLAN:iin kuuluminen määräytyy sen perusteella, mihin kytkimen porttiin laite kytketään ja mihin VLAN:iin portti on määritelty (kuvio 15). VLAN:sta toiseen vaihtaminen on helpoimmillaan johdon vaihtamista kytkimen portista toiseen. Kukin portti voi kuulua kerrallaan vain yhteen VLAN-verkkoon. Porttiperusteinen VLAN on helppoa ja nopeaa pienen työmääränsä vuoksi, sillä laitteista itsestään ei tarvitse tietää mitään, vaan riittää tietää, mihin VLAN:iin laitteen tarvitsee olla yhteydessä. (Hakala & Vainio 2005, 96 - 99.)



KUVIO 15. Porttiperustainen VLAN (Hakala & Vainio 2005, 97)

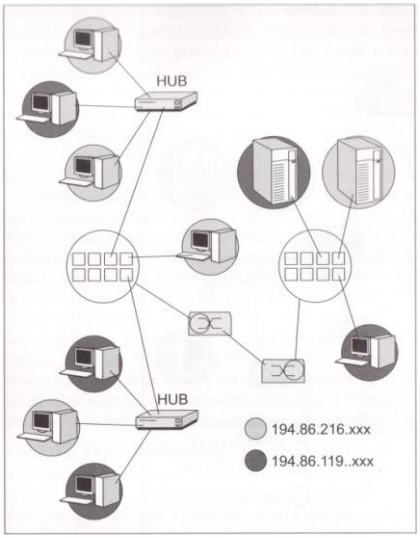
MAC-osoitteeseen perustuva VLAN (MAC-based VLAN) toimii siten, että kytkimiin ja reitittimiin määritellään, mitkä MAC-osoitteet kuuluvat mihinkin

VLAN:eihin (kuvio 16). MAC-osoite voi kuulua useampaan VLAN:iin. MAC-osoitteen perustuva VLAN on työläämpi vaihtoehto kuin esimerkiksi porttiperustainen VLAN, sillä ylläpidon tarvitsee määritellä yksittäisille laitteille VLAN:t, joihin laite kuuluu. Määrittelyjen jälkeen kytkimet voivat dynaamisesti huolehtia VLAN:n uudelleenmäärittelystä laitesiirtojen yhteydessä. (Jaakohuhta 2005, 157.)



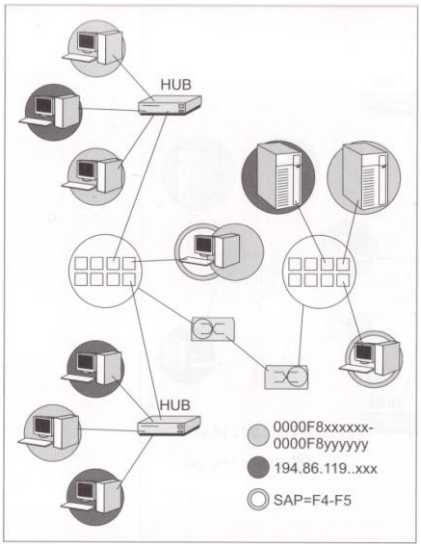
KUVIO 16. MAC-osoitteeseen perustuva VLAN (Hakala & Vainio 2005, 98)

Kolmas tapa toteuttaa VLAN perustuu OSI-mallin verkkokerrokseen (layer 3 based VLAN) ja vaatii käytettäviltä kytkimiltä reititysominaisuuden (kuvio 17). Reititysominaisuuden avulla VLAN:ja voidaan muodostaa aliverkkojen tai IPX-verkkonumeron perusteella. Kytkimen portissa voi olla yksi tai useampi aliverkko ja aliverkko voi olla useammassa kuin yhdessä portissa. (Hakala & Vainio 2005, 98.)



KUVIO 17. Aliverkon perusteella luotu VLAN (Hakala & Vainio 2005, 99)

Policy-perusteinen VLAN (policy based VLAN) antaa mahdollisuuden ryhmitellä VLAN:eihin kuuluvat käyttäjät useilla eri perusteilla (kuvio 18). Käytettävissä olevat ryhmittelyn perusteet ovat verkko-osoite (MAC-osoite tai OSI-mallin 3-tason osoite), protokollan tyyppi tai protokollien otsikoissa olevat muut tiedot ja kohdat. (Hakala & Vainio 2005, 99.)



KUVIO 18. Useiden kriteerien perusteella luotu VLAN (Hakala & Vainio 2005, 100)

Jos verkossa on useita eri kytkimiä kattavia VLAN:ja, tarvitaan kytkimien välille trunking-protokolla, joka lisää jokaiseen kehykseen lisäotsikon, ennen trunk-yhteyden kautta lähetystä. Trunking-protokollan avulla vastaanottava kytkin tietää, mihin VLAN:iin kyseinen kehys kuuluu ja mihin kehys tulee välittää. (Odom 2005, 144 - 146.)

VLAN:n käytölle on useita tärkeitä merkityksiä. Virtuaaliverkkojen avulla voidaan parantaa tietoturvaa rajaamalla eri VLAN:ssa olevien käyttäjien pääsyä fyysisesti samassa verkossa sijaitseviin toisiin laitteisiin. VLAN:lla voidaan rajoittaa levitysviestialuetta pienemmäksi isoissa verkoissa ja siten vähentää verkon ruuhkautumista ja kasvattaa lähiverkon tiedonsiirtokapasiteettia. VLAN:lla voidaan helpottaa verkon ylläpitoa käyttäjien siirtyessä lähiverkossa paikasta toiseen. (Jaakohuhta 2005, 157.)

4 LANGATON LÄHIVERKKO

Langattomassa lähiverkossa siirtotienä käytetään yleensä radiotietä ethernet-verkoissa käytettävän kaapeloinnin sijaan. Radiotien ohella langattomissa lähiverkoissa käytetään joskus valosignaalia. Koska WLAN toimii ISM-taajuuksilla (Industrial Scientific Medical) eli radiotaajuuksilla, joilla voidaan toimia ilman erillistä lupaa, WLAN on altis muiden lähteiden aiheuttamille häiriöille. Häiriötekijöitä ovat esimerkiksi mikroaaltouuni ja päällekkäin olevat WLAN-lähetykset. Häiriöiden lisäksi langattoman lähiverkon suorituskyky on ethernet-verkkoa pienempi, ja suorituskyky jää usein 30 - 60 %:iin langattomien verkkojen bittinopeudesta. (Geier 2005, 69, 76; Puska 2005, 21; Granlund 2007, 294, 299.)

Langattoman lähiverkon toiminta määritellään IEEE 802.11 -standardikokoelmalla, josta käytetään nykyään lyhennettä WiFi (Wireless Fidelity). WiFi-sertifikaatti on WiFi Alliance -organisaation myöntämä sertifikaatti, jolla varmistetaan langattomien 802.11-lähiverkkotuotteiden, kuten tukiasemien ja eri radiokorttien, minimivaatimukset sekä yhteensopivuus muiden laitteiden kanssa. (Geier 2005, 130; Granlund 2007, 293.)

4.1 Standardien vertailu

Langatonta lähiverkkoa suunniteltaessa on mietittävä tarkkaan, valitseeko 2,4 GHz:n vai 5 GHz:n kaistan, sillä järjestelmät eivät ole suoraan yhteensopivia keskenään. Standardeista 802.11b ja 802.11g toimivat 2,4 GHz:n kaistalla, 802.11a 5 GHz:n kaistalla ja 802.11n käyttää molempia kaistoja hyväkseen. Suomessa saa käyttää kansallisten määräysten mukaan kaikkia standardeja ilman käyttölupaa, kunhan laitteet täyttävät standardien määräykset ja asetettuja lähetystehoja ei ylitetä. Valintaa tehtäessä on kiinnitettävä huomiota ainakin seuraaviin asioihin.

- Maantieteellinen sijainti: 2,4 GHz:n langattomat lähiverkot on hyväksytty lähes kaikkialla maailmassa, mutta 5 GHz:n käyttöä langattomissa lähiverkoissa on rajoitettu.

- Suorituskyky: 2,4 GHz:n kaista mahdollistaa vain kolme ei-päällekkäistä kanavaa, kun taas 5 GHz:n kaistalla on mahdollista saada 12 ei-päällekkäistä kanavaa.
- Tilojen laajuus: 2,4 GHz:n kaistalla on pitempi kantavuus ja kaista vaatii pienemmän tukiasemien määrän kuin huonomman kantaman omaava 5 GHz:n kaista. Tosin joissakin tilanteissa 5 GHz:n kaistalla voi olla yhtä hyvä kantama kuin 2,4 GHz:n kaistalla.
- Häiriöt: 2,4 GHz:n kaistalla langattomiin lähiverkkoihin saattaa kohdistua häiriöitä esimerkiksi langattomista puhelimista ja mikroaaltouuneista, jotka heikentävät verkon suorituskykyä. 5 GHz:n kaista on melko vapaa häiriöistä.
- Yhteensopivuus: 2,4 GHz:n ja 5 GHz:n järjestelmät eivät ole suoraan yhteensopivia, mutta nykyään uudemmat laitteet on usein varustettu kaksikaistaisella verkkokortilla, joka voi käyttää molempia järjestelmiä.
- Tietoturva: 2,4 Ghz:n järjestelmässä on enemmän tietoturvaongelmia kuin 5 Ghz:n järjestelmässä pidemmän kantaman vuoksi.

(Geier 2005, 128 - 129.)

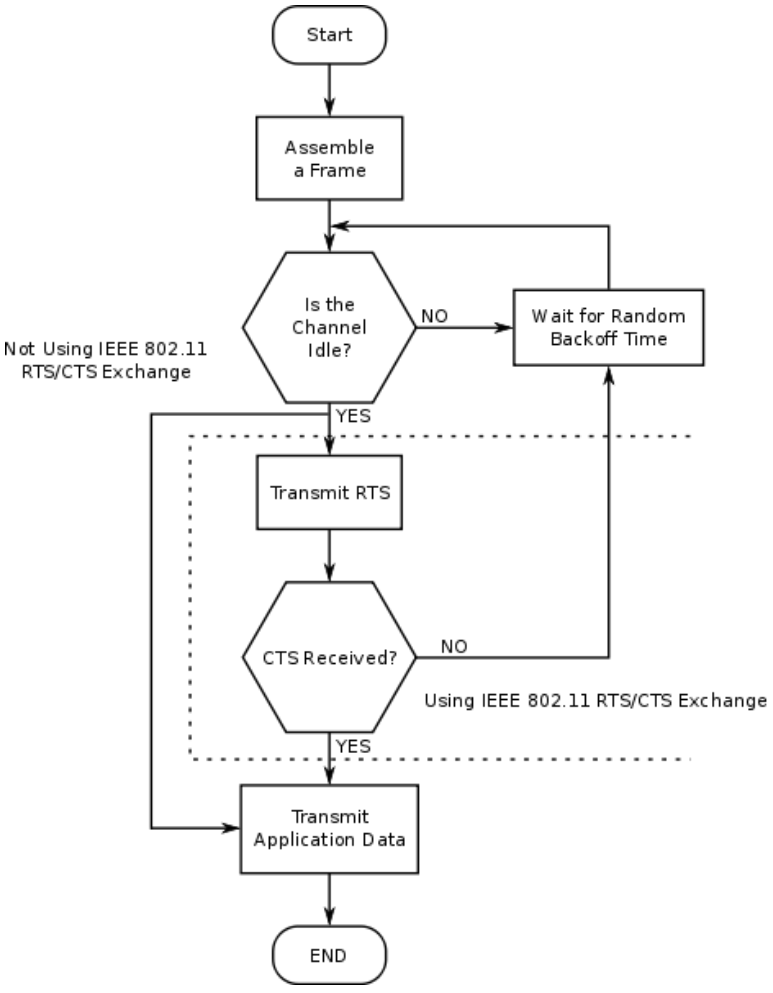
Taulukossa 4 on esitetty yhteenvetona eri 802.11-standardien tietoja. EIRP-teho tarkoittaa suurinta sallittua tehoa.

TAULUKKO 4. Eri 802.11-standardien tiedot (Puska 2005, 46)

Standardi	**802.11**	**802.11b**	**802.11a**	**802.11g**	**802.11n**
Ratifioitu	1997	1999	1999	2003	2009
Mediat	IR, RF	RF	RF	RF	RF
Hajaspektri-tekniikka	FHSS, DSSS	DSSS	OFDM	OFMD	OFDM
Teoreettinen bittinopeus	1 ja 2 Mbit/s	1, 2, 5,5 ja 11 Mbit/s	6 - 54 Mbit/s	1 - 54 Mbit/s	600 Mbit/s
Taajuus-alue	RF: 2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 ja 5 GHz
Kanavia yhteensä	DS: 14	14	12	12	
Ei-päällekkäisiä kanavia	3	3	12	3	
EIRP-teho	100 mW	100 mW	200 mW	100 mW	100 ja 200 mW
Käyttökohteet	sisä- ja ulkotiloissa		vain sisätiloissa	sisä- ja ulkotiloissa	

4.2 CSMA/CA

Siirtotien varaaminen on siirtoyhteyskerroksen toiminto, jossa protokollat määräävät laitteiden datalähetysten järjestyksen. Yleinen siirtotien varausprotokolla sekä lankaverkossa että langattomassa verkoissa on CSMA, jossa jokainen langaton verkkokortti osaa havaita muiden laitteiden tekemät lähetykset. CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) on langattoman tietoliikenteen siirtotien varausmenetelmä, jossa kuvion 19 mukaisesti lähettämistä aikova osapuoli ensin kuuntelee, onko siirtotie vapaana, kysyy lupaa tiedonsiirron aloittamiseen (RTS-viesti (Request to Send)) ja vasta luvan saatuaan aloittaa tiedonsiirron (CTS-kuittaus (Confirm to Send). (Geier 2005, 59; Granlund 2007, 315.)



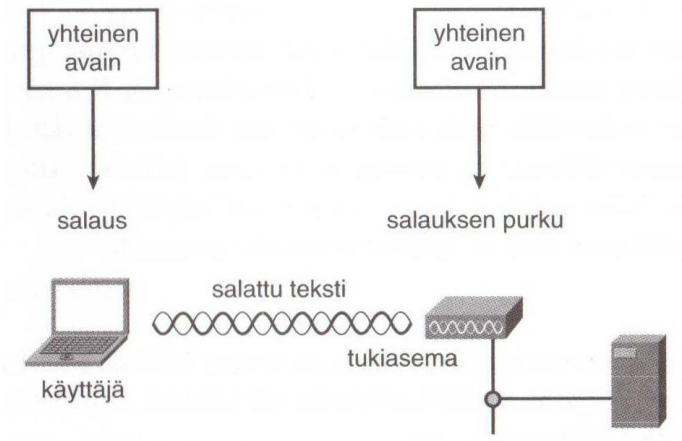
KUVIO 19. CSMA/CA:n toimintaperiaate (Wikipedia 2013a)

CSMA/CA-varausmenetelmässä siis varotaan tekemästä törmäyksiä. Lankaverkoissa käytettävässä CSMA/CD-varausmenetelmässä (Carrier Sense Multiple Access With Collision Detection) ainoastaan kuunnellaan, onko siirtotie vapaa, ja sitten aloitetaan lähettäminen. CSMA/CD-varausmenetelmässä mahdolliset törmäykset yritetään havaita jälkeenpäin. (Puska 2005, 29.)

4.3 Salaus

Langattomat lähiverkot toimivat radiosignaaleilla, joiden kuuluvuutta on vaikea rajoittaa tietylle alueelle ja tietyille kuulijoille (Puska 2005, 79). Jotta langattomiin lähiverkkoihin saadaan samanlainen suoja kuin perinteiseen kiinteään lähiverkkoon, radiotiellä kulkeva tieto salataan (Granlund 2007, 317). IEEE:n 802.11 -standardeissa on määritelty salausmenetelmät: WEP (Wired Equivalent Protocol), WPA (Wi-fi Protected Access) ja WPA2 (Wi-fi Protected Access 2). WEP-salaus on todettu epäturvalliseksi, WPA-salaus oli tarkoitettu väliaikaiseksi ratkaisuksi WPA2-salauksen valmistumisen asti. Nykyaikana suosituin ja suositelluin salaus on WPA2.

WEP-salaus oli ensimmäinen IEEE 802.11 -standardissa vuonna 1999 määritelty salausmenetelmä, joka käyttää RC4-jonosalausta (Rivest Cipher 4). WEP-salaus on sittemmin hylätty yleisestä käytöstä helpon murrettavuuden takia, joka johtuu WEP-salauksessa käytettävästä symmetrisestä, kiinteästä avaimesta. Symmetrisyys tarkoittaa, että salattu teksti puretaan samalla avaimella kuin se salataan kuvion 20 mukaisesti. WEP-salaus ei tarjoa riittävää tietoturvaa useimmille yrityksille. Toisaalta käyttämällä WEP-salausta voidaan estää ulkopuolisten langattomien lähiverkkojen vahinkokäyttö, joka on avoimien langattomien lähiverkkojen ongelma. (Geier 2005, 131; Puska 2005, 80.)



KUVIO 20. Symmetrinen salaus (Geier 2005, 179)

WPA-salaus oli WiFi-allianssin pikaisesti tehty tilapäiseksi tarkoitettu ratkaisu paikkaamaan WEP-salauksessa havaittuja puutteita. WPA-salaus ei pohjautunut olemassa oleviin standardeihin, vaan sen toivottiin luovan suuntaviivat valmisteilla olevalle IEEE 802.11i-standardille. Kiireen vuoksi WPA suunniteltiin sellaiseksi, että sen pystyi ottamaan vanhoissa laitteissa käyttöön pelkällä ohjelmistopäivityksellä eli päivitys ei edellyttänyt uusien laitteiden ostoa. (Granlund 2007, 320.)

WPA2 on IEEE 802.11i -standardin vuonna 2004 valmistunut salausmenetelmä. Toisin kuin WPA, WPA2 vaati laitekannan uudistuksen eli WPA2 ei päivity ohjelmistopäivityksellä. WPA2-salauksessa käytetään vuonna 2002 standardoitua AES-jonosalaajaa (Advanced Encryption Standard). AES-jonosalaajalla on viisi eri toimintamuotoa, ja WPA2 käyttää toimintomuotoa CTR (Counter), eli AES CTR-jonosalaajaa. WPA2-salauksessa ei ole havaittu huolestuttavia heikkouksia, ja sitä suositellaan käytettävän IEEE 802.11 -standardin vaihtoehdoista. (Granlund 2007, 317, 320 - 321.)

5 PALOMUURIOHJELMISTOT

5.1 SmoothWall Express 3.0

SmoothWall Express on yksi tunnetuimmista Linux-käyttöjärjestelmään pohjautuvista ilmaisista palomuuriohjelmistoista, joka on suunniteltu kotikäyttöön sekä pienille yrityksille. SmoothWall Expressistä on myös maksullinen versio, jossa on enemmän ominaisuuksia kuin ilmaisversiossa.

SmoothWall Expressin asentaminen on tehty helpoksi, eikä asentaminen vaadi tuntemusta Linuxista. SmoothWall Expressin käyttäminen on helppoa selainkäyttöliittymällä ja SmoothWall Expressin on suunniteltu toimimaan hitaammilla ja vanhemmilla tietokoneilla. SmootWall Expressillä voidaan muun muassa kontrolloida verkkoliikennettä, sisään tulevaa ja uloslähtevää sekä sisäistä liikennettä. (Meredith 2010; SmoothWall 2013a.)

5.2 Zentyal 3.0

Zentyal on avoimen lähdekoodin ilmainen ohjelmisto, joka ei ole pelkästään palomuuriohjelma vaan tekijät kuvailevat Zentyalia Linux-palvelimeksi, joka on tarkoitettu pienille tai keskikokoisille yrityksille. Zentyal on tekijöidensä mielestä vastine Windows Server -palvelinohjelmistolle. Zentyal pohjautuu Ubuntu-jakeluun, ja Zentyal voidaan jälkiasentaa Ubuntu-käyttöjärjestelmän asennukseen tai asentaa kokonaan itsenäisesti omilta asennuslevyiltä. (Zentyal 2013c; Wikipedia 2013l.)

Zentyal on palomuuriin liittyvien asioiden lisäksi muuan muassa web-palvelin, sähköpostipalvelin, tiedostopalvelin, pikaviestipalvelin, RADIUS-palvelin ja Voice over IP -palvelin. Zentyalissa on helppokäyttöinen selainkäyttöliittymä. (Wikipedia 2013l.)

5.3 pfSense 2.0.3

pfSsense on ensisijaisesti avoimen lähdekoodin palomuuri- ja reititinohjelma, joka pohjautuu Unixin kaltaiseen käyttöjärjestelmään, ja siinä on selainkäyttöliittymä.

pfSensen perusjakelu sisältää valmiiksi paljon ominaisuuksia, ja niitä on mahdollista laajentaa erikseen asennettavilla lisäosilla (kuten snort). pfSenseä käytetään yleensä reunapalomuurina, reitittimenä, WLAN-tukiasemana, DHCP-palvelimena ja VPN- päätepisteenä. (Electric Sheep Fencing LLC 2013c; Electric Sheep Fencing LLC 2013a; Wikipedia 2013g.)

pfSensen version 1.2.x minimivaatimukset laitteistolle ovat 100 MHz:n Pentium-tasoinen prosessori ja 128 MB käyttömuistia. Lisäksi kovalevyasennukseen vaaditaan CD-asema ja 1 GB kovalevytilaa. Laitteiston vaatimukset riippuvat myös käytöstä ja esimerkiksi palomuuri- ja reititinkäytössä liikenteen määrästä, nopeudesta ja tyypistä. pfSensen tilavaatimuksiin vaikuttaa myös se, asennetaanko siihen perusosan lisäksi lisäosia, logitetaanko liikennettä ja kuinka suuren tilataulun liikenne aiheuttaa. (Electric Sheep Fencing LLC 2013d.)

pfSense on ominaisuuksiltaan kilpailukykyinen kaupallisten palomuurien kanssa, ja joissakin tapauksissa siinä on jopa enemmän ominaisuuksia. pfSensen palomuuri on tilallinen, ja sillä voi suodattaa TCP- ja UDP-liikennettä lähde- ja kohdeIP:n perusteella, IP-protokollan perusteella ja lähde- ja kohdeportin perusteella. pfSensen muita ominaisuuksia ovat seuraavat:

- tilataulu
- NAT (Network address translation)
- CARP
- kuorman tasaus
- VPN
- IPsec (Internet Protocol Security)
- OpenVPN
- historialliset raportointigraafit ja tosiaikaiset monitorointigraafit
- dynaaminen DNS
- DHCP-palvelin ja -relay.

(Electric Sheep Fencing LLC 2013b.)

5.4 Palomuuriohjelmistojen vertailu

SmoothWall-, Zentyal- ja pfSense-palomuuriohjelmistojen vertailu on rajattu Taitaja2014-tapahtuman verkkosuunnitelman olennaisiin ominaisuuksiin. Vertailtavissa palomuuriohjelmistoissa ja palomuuriohjelmistoissa on ylipäätään olemassa paljon muitakin ominaisuuksia. Taulukossa 6 vertaillaan palomuuriohjelmistojen vähimmäisvaatimuksia, jotka asennettava ohjelmisto vaatii järjestelmältä. Taulukosta 5 selviää, että pfSense on vähimmäisvaatimuksiltaan hyvin samankaltainen kuin SmoothWall Express ja että Zentyal vaatii erikoisen paljon prosessoria, muistia ja kovalevyä muihin vertailtaviin palomuureihin nähden. Zentyalin vähimmäisvaatimukset selittyvät sillä, että Zentyal on enemmän kuin palomuuriohjelmisto ja Zentyal luokittelee itsensä palvelinohjelmistoksi. Taitaja2014-tapahtuman verkkoliikenteen määrää ei etukäteen tiedetä tarkkaan, ja koska palomuuriohjelmiston suorituskyky sekä skaalautuvuus ovat täysin riippuvaisia vähimmäisvaatimuksista yli jäävistä resursseista, vaikuttaa Zentyal vähimmäisvaatimusten osalta huonoimmalta vaihtoehdolta.

TAULUKKO 5. Vertailtavien palomuuriohjelmistojen vähimmäisvaatimukset (Electric Sheep Fencing LL 2013d; SmoothWall 2013b; Zentyal 2013a)

Vähimmäisvaatimukset	**Zentyal 3.0**	**SmoothWall Express 3.0**	**pfSense 2.0.3**
Prosessori	Pentium 4 tai vastaava	Pentium 200 MHz	Pentium 100 MHz
Muisti	2GB	64 MB	128 MB
Kovalevy	80GB	1 GB	1 GB

Taulukossa 6 vertaillaan palomuuriohjelmistojen ominaisuuksia ja taulukosta nähdään, että SmoothWall Expressistä puuttuu useita testauksen kannalta olennaisia ominaisuuksia, kuten DHCP Relay, VLAN, kuorman tasaus ja vikasietoisuus. Näiden lisäksi myös SmoothWall Expressin uloslähtevän

liikenteen kontrolli on rajoitettu. SmoothWall Expressin puuttuvat ominaisuudet ovat niin merkittäviä, ettei sitä voi harkita käytettäväksi Taitaja2014-tapahtumassa. Zentyalin ominaisuudet DHCP relayta lukuun ottamatta ovat riittävät. Zentyalin ja pfSensen olennaisimmat ominaisuudet ovat lähes samalla viivalla, kuitenkin pfSensen ollessa hiukan parempi. Sekä Zentyal että pfSense sopisivat ominaisuuksiltaan Taitaja2014-tapahtuman palomuuriksi.

TAULUKKO 6. Vertailtavien palomuuriohjelmien ominaisuuksia (Electric Sheep Fencing LLC 2013b; SmoothWall 2013b; Zentyal 2013b)

Ominaisuus	**SmoothWall express**	**Zentyal**	**pfSense**
Tilallinen palomuuri ja tutkiminen	On	On	On
Uloslähtevän liikenteen kontrolli	Rajoitettu	On	On
WebGUI	On	On	On
DHCP	On	On	On
DHCP relay	Ei	Ei	On
NAT	On	On	On
VLAN	Ei	On	On
Vikasietoisuus	Ei	On	On
Kuorman tasaus	Ei	On	On
Intrusion Detection System	On	On	On, lisäpaketti

Testaukseen ei valittu SmoothWall Expressiä, sen puuttuvien ominaisuuksien vuoksi, eikä Zentyalia, koska sen vähimmäisvaatimukset ovat liian isot. pfSense valikoitui reitittimen ja palomuurin rooliin muiden vaihtoehtojen sijaan, koska pfSensestä löytyvät tarvittavat ominaisuudet, pfSense on ilmainen, vähimmäisvaatimukset ovat kohtuulliset ja koska pfSense on tuttu ohjelma Taitaja2014-tapahtuman LAMK:n puolen henkilöstölle. pfSenseä on käytetty LAMK:n käytössä hyvin tuloksin esimerkiksi Salpausselän kisoissa useampana vuotena. pfSense ei vaadi erillisiä laitehankintoja, koska sen ajamiseen ei tarvita kuin perustietokone, ja se saatiin lainaan LAMK:n tietoliikennelaboratoriosta.

6 TIETOVERKON SUUNNITTELU JA TESTAUS

6.1 Taitaja2014-tapahtuman verkkotarpeet ja tilat

Ennen varsinaisen suunnittelun ja testaamisen aloittamista perehdyttiin Taitaja2014-tapahtuman verkkotarpeisiin ja tilaan, jossa tapahtuma järjestetään. Taitaja2014-tapahtuma pidetään Lahden Messukeskuksessa (kuvio 21), ja verkonsuunnittelun kannalta olennaisin osa tapahtumasta tapahtuu enimmäkseen halleissa B, C, D ja E (taulukko 7) sekä Messukeskuksen pääsisäänkäynnin pysäköintialueella. Lisäksi A-hallissa on ajoittain varsinaisesta kilpailuohjelmasta poikkeavaa ohjelmaa.

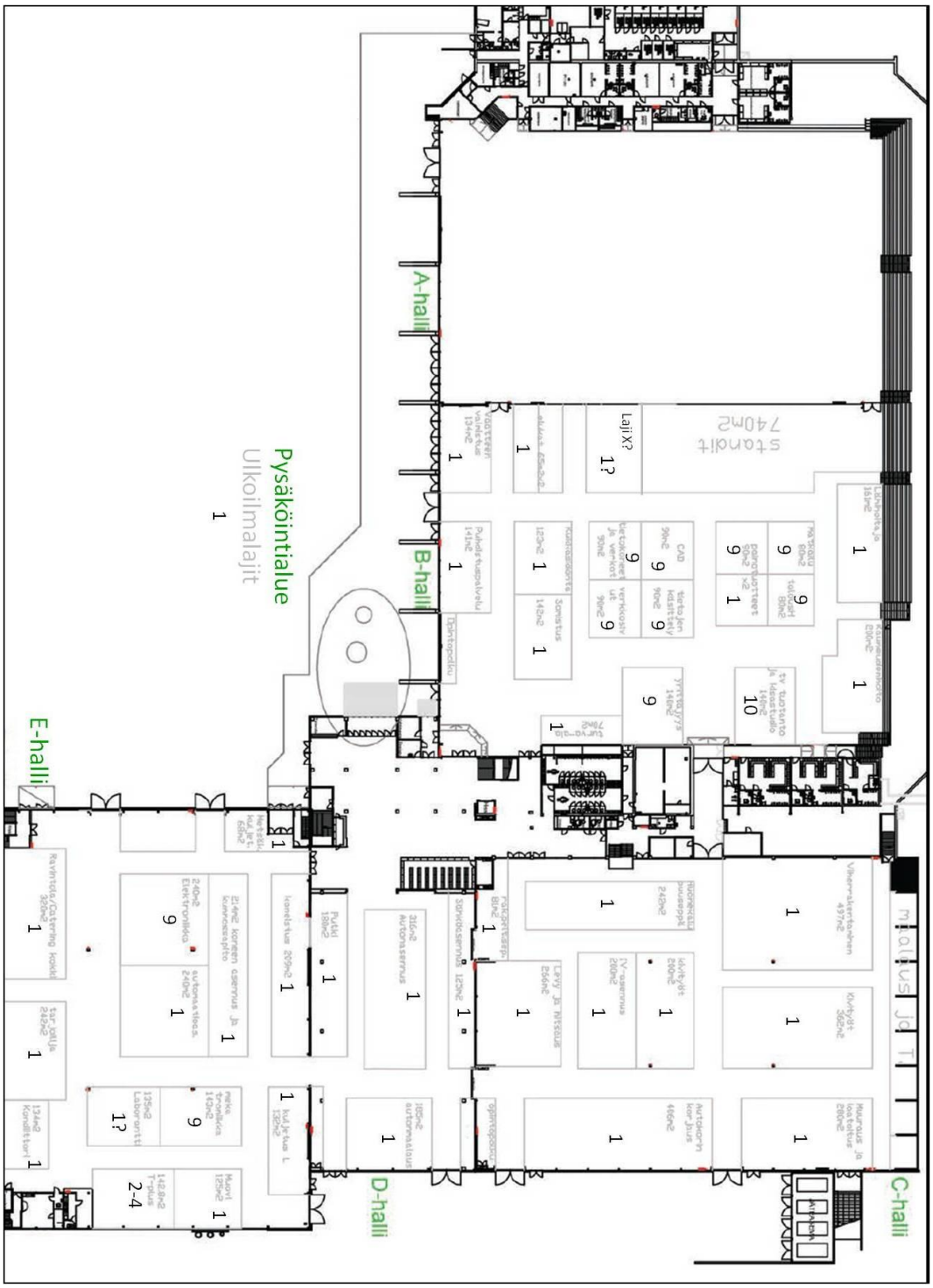
KUVIO 21. Lahden Messukeskuksen ilmakuva vuodelta 2006 (Lahden Messut 2013a)

TAULUKKO 7. Lahden Messukeskuksen tilaisuuksiin käytettävät tilat (Lahden Messut 2013b)

Messukeskuksen halli	**Pinta-ala**
A-halli (Suurhalli Areena)	3 395 m^2
B-halli (Suurhalli Treeni)	4 495 m^2
C-halli (Salpausselkä Halli)	4 085 m^2
D-halli (Vesijärvi Halli)	1 375 m^2
E-halli (Lahti Halli)	3 875 m^2

Verkkosuunnitelman tekemisen kannalta tärkeimmät tiedot olivat työpisterasioiden määrä ja sijainti halleissa. Työpisterasiat sijaitsivat hallien seinissä ja tukipilareissa, ja niiden sijainnit näkyvät kuviosta 22. Tästä poiketen B-hallin pysäköintialueen puoleisen ovien lähellä oleva työpisterasia sijaitsi sähköjohtokourussa, useamman metrin korkeudella lattiasta. Työpisterasiat olivat pääsääntöisesti 2-osaisia, joissakin harvemmissa tapauksissa 4-osaisia.

Verkkosuunnitelman tekemiseen vaikuttivat työpisterasioiden ohella mahdollisuus käyttää kaapeloinnin apuna B-hallissa kolmen metrin korkeudella tukipalkkien suuntaisesti kulkevaa vaijeria. D-hallissa ulkoseinän kahden oven väliseen tilaan tarvittava kaapelointi on vedettävä matalamman oven yli.



KUVIO 22. Pohjakuva Lahden Messukeskuksen tiloista ja Taitaja2014-tapahtuman konepaikkojen tarvemäärästä (Taitaja2014 2013)

Taitaja2014-tapahtuman tietotekniset tarpeet ovat varsin mittavat. Kilpailussa on lähemmäksi 50 lajia, ja jokainen laji vaatii oman toimitsijoille tarkoitetun

tietokoneen sekä vaihtelevan määrän tietokoneita lajin kilpailijoiden käyttöön ja lajin kilpailun toteuttamiseen. Tietokoneiden määrä on suuntaa antava ja tulee elämään vielä tapahtuman aikana. Nykykäsityksen mukaan määrä jakautuu Messukeskuksen tiloihin seuraavasti:

- B-halli: 92 tietokonetta
- C-halli: 9 tietokonetta
- D-halli: 4 tietokonetta
- E-halli: 32 tietokonetta
- Messukeskuksen pysäköintialue: 1 tietokone

Yhteensä 138

Järjestäjätahon linjauksen perusteella verkkokapasiteetti pyritään mitoittamaan niin, että jokaista oikeaa tarvetta kohden on yksi varapaikka. Tämän vuoksi verkko mitoitetaan 276 tietokoneelle laskennallisen arvon 138 sijaan.

Tapahtumassa tarvitaan oma verkko toimitsijoille, kilpailijoille ja yleisölle sekä tietokoneet ja verkot -lajille. Toimitsijoiden pitää päästä langallisesti ja langattomasti sisäverkon pisteenlaskupalvelimille, tulostimiin ja Internetiin. Kilpailijoiden pitää päästä langallisesti Internetiin ja mahdollisesti tulostimiin. Yleisön pitää päästä langattomasti Internetiin. Tietokoneet ja verkot -lajin pitää langallisesti päästä Internetiin muusta kilpailusta fyysisesti ja loogisesti erillään olevan oman verkon ja laitteiston kautta.

WLAN-yhteys Internetiin pitää olla käytettävissä kaikissa Messukeskuksen halleissa, myös hallissa A, jossa ei ole varsinaista kilpailutoimintaa, sekä pysäköintialueella ja Messukeskuksen aulassa. Verkkotulostimia tulee kaksi kappaletta jokaiseen halliin.

6.2 Suunnittelu ja testaus

Ennen verkkosuunnitelman suunnittelun ja testauksen alkamista oli tiedossa, että Taitaja2014-tapahtuman laitteisto kytkimen osalta on Ciscon 2960S. Tämä johtui siitä, että järjestäjätaho (Salpaus/PHKK (Päijät-Hämeen Koulutuskonserni)) on käyttänyt muussa aikaisemmassa käytössä tätä kytkintä, joten sen toimivuus on

käytössä testattu. Järjestäjätaholla ei ole tarpeeksi samanmallisia kytkimiä valmiina, joten niitä hankitaan lisää, ja ne tulevat lainaan Taitaja2014-tapahtumaan. Taitaja2014-tapahtuman jälkeen niitä voidaan hyödyntää muussa käytössä. Ciscon 2960S-kytkin on Taitaja2014-tapahtuman verkkototeutuksen kannalta hyvinkin riittävä teholtaan, kapasiteetiltaan, ominaisuuksiltaan ja luotettavuudeltaan. Verkkototeutus ei vaadi sellaisia ominaisuuksia tai erikoisuuksia, joita valtaosasta peruskytkimistä ei löytyisi.

Laite- ja verkkotestaukset suoritettiin LAMK:n tietoliikennelaboratorion tiloissa. Testauksissa tutustuttiin laitteisiin, niiden ominaisuuksiin ja sitten pystytettiin riittävän kokoinen verkko, jolla voitiin simuloida varsinaisessa Taitaja 2014-tapahtumassa käytettävää verkon rakennetta ja toimintaa olennaisilta osilta.

Verkon suunnittelu ja testaaminen sekä aktiivilaitteiden testaaminen eivät välttämättä ole erillisiä toimenpiteitä, vaan ne voidaan tehdä toisiansa tukien, limittäin. Pelkän teoreettisen suunnittelun varaan pohjautuva uusi verkko voi kohdata yllättäviä ongelmia, joten suunnitelman testaus on tärkeää. Verkon testaamisessa laboratorio-olosuhteissa tuo omat haasteensa, sillä on hankalaa luoda kooltaan, liikennemäärältä, asiakaslaitemäärältään ja liikenteen monimuotoisuudelta vastaavaa verkkoa kuin todellisuudessa. Kuten aikaisemmin todettiin, käytettävän kytkimen malli oli tiedossa jo ennen testauksia ja sen suoriutuminen kenttäolosuhteissa on tuttua, joten testauksissa keskityttiin verkontoteuttamiseen valittujen verkkotekniikoiden ja kytkimien asetuksien testaamiseen.

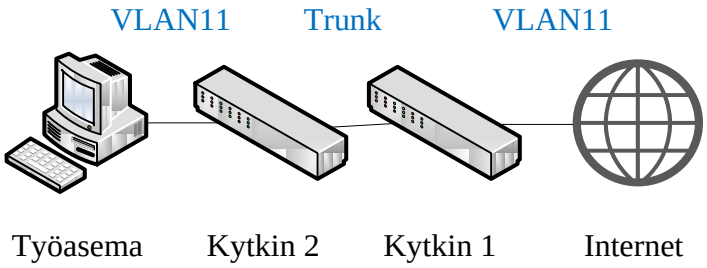
Laite- ja verkkotestauksiin saatiin lainaksi PHKK:lta kaksi kytkintä, jotka ovat hyvin samankaltaisia toiminnaltaan ja ominaisuuksiltaan kuin varsinaisessa Taitaja2014-tapahtumassa todennäköisesti käytettävät kytkimet. Testauksissa käytettävät kytkimet olivat Ciscon 24-porttisia 2960G-mallin kytkimiä (kuvio 23).

KUVIO 23. Ciscon 24-porttiset 2960G-mallin kytkimet

Testaamisessa ei käytetty mitään valmista suunnittelumallia, vaan testisuunnitelmaa laadittiin kohta kohdalta edellisten tulosten pohjalta järkeilyä ja omaa ja opinnäytetyön teknisen puolen ohjaajan harkintakykyä käyttäen. Testiverkon rakentaminen aloitettiin pienestä ja sitä kasvatettiin asteittain.

6.3 Testaus 1: perusverkko, VLAN ja VTP

Ensimmäisen testauksen ideana oli toteuttaa kuvion 24 mukainen verkkotopologia ja saada työasemalle yhteys Internetiin kytkimien läpi. Kytkimissä käytettiin VLAN:ja, ja kytkinten kesken VLAN:ja hallinoitiin VTP:llä. Laitteistona tässä testauksessa oli kaksi kytkintä, työasema ja Internet-yhteys.



KUVIO 24. Testauksen 1 verkkotopologia

VLAN:ien luonnissa kytkimen tietokantaan pitää ensin luoda VLAN, sitten luotu VLAN liitetään tiettyyn liityntään ja lopuksi liitynnän tyyppi määritellään access- tai trunk-tyyppiseksi. Liitynnän access-tyyppiä käytetään yhden VLAN:n liikennöidessä ja trunk-tyyppiä kaikkien VLAN:ien liikennöidessä. Trunk-tyyppiä käytetään liitynnöissä, jotka ovat kiinni toisissa kytkimissä, palomuureissa tai reitittimissä.

Testauksen kytkimet numeroitiin 1 ja 2. Työasema liitettiin kytkimeen 2, joka liitettiin kytkimeen 1 ja kytkin 1 liitettiin Internetiin. Työasema kiinnitettiin kytkimen 2 porttiin, joka oli VLAN:ssa 11. Kytkinten välisessä kytkennässä portit olivat VLAN:n trunk-tilassa eli välittivät kaikkien VLAN:ien liikenteen. Kytkimen 1 Internetiin kiinni oleva portti oli VLAN:ssa 11.

VTP:n idea on, että VLAN:t voidaan luoda kytkimeen, joka toimii VTP-palvelimena, ja verkon muut kytkimet saavat tiedot VLAN:eista VTP-palvelimelta. Kytkin 1 oli verkon reunakytkin ja toimi VTP-palvelimena, kytkin 2 toimi VTP-asiakkaana. VTP luotiin kytkimeen globaalissa konfiguraatiotilassa komennoilla VTP domain/mode/password/version. VTP:lle tarvitsee määritellä ainakin VTP-verkon nimi, johon kytkin kuuluu (domain), VTP:ssä käytetty salasana (password) ja onko kytkin VTP-palvelin vai -asiakas (mode). Testauksessa VTP-palvelimena olevana kytkimellä1 luotiin VLANeja ja tiedot niistä siirtyivät onnistuneesti VTP-asiakkaana olevaan kytkimeen 2.

Vaihtoehdossa, jossa VLAN:a ei olisi käytetty kytkimissä laisinkaan, olisi kaikkien osapuolten välinen liikenne tapahtunut samassa verkossa. Tällöin teoriassa kaikilla osapuolilla olisi ollut mahdollisuus liikennöidä kaikkien verkossa olevien kanssa, mikä olisi ollut tietoturvan kannalta todella huono vaihtoehto. Jos tässä tilanteessa pääsyä olisi haluttu rajoittaa jonnekin, rajoittaminen olisi pitänyt tehdä siinä laitteessa, johon pääsyä ei haluta. Erillisen palomuurin käyttäminen laitteissa, johon pääsyä halutaan rajata, olisi ollut resursseja tuhlaavaa ja joissakin tapauksissa mahdotonta.

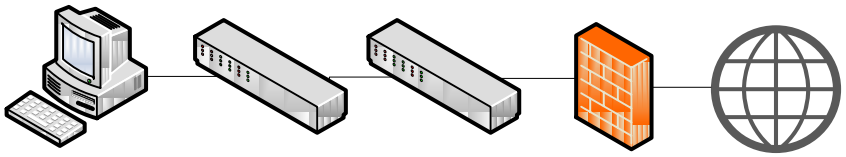
Toinen vaihtoehto liikenteen rajoittamiseen tapauksessa, jossa ei ole käytössä VLAN:a, olisi käyttää reitittimiä, joihin olisi määritelty laitteiden tai verkkojen pääsy toisiin laitteisiin tai verkkoihin. Reitittimien käyttö VLAN:ien sijaan olisi tarkoittanut aivan erilaisen, monimutkaisemman ja enemmän kaapelivetoja tarvitsevan topologian käyttöä. Reitittimet olisi pitänyt sijoittaa topologiassa lähemmäksi verkonkäyttäjiä, ja jokaisessa reitittimen portissa olisi voinut olla vain yhdentyyppisen verkon laitteita, jotka saisivat liikennöidä keskenään. Tämä olisi lisännyt myös kustannuksia, sillä reitittimissä on huomattavasti vähemmän portteja kuin kytkimissä ja reitittimet ovat paljon kalliimpia kuin kytkimet. Lisäksi reitittäminen vaatii enemmän prosessoritehoa kuin kytkimien toiminta, joten verkon toteutuksessa reitittimiä kannattaa määrällisesti käyttää vähemmän kuin kytkimiä.

Jos VLAN olisi ollut MAC-pohjainen, tietoturva olisi ollut parempi ja ainoastaan etukäteen tiedetty laite olisi liitetty tiettyyn VLAN:iin. Haittapuolena MAC-pohjaisessa VLAN:ssa olisi lisääntynyt työnmäärä, sillä pitäisi tietää kaikkien laitteiden MAC-osoitteet etukäteen tai sitten tuntemattomien laitteiden MAC-osoitteet pitäisi lisätä verkon ollessa jo käytössä.

Tässä vaiheessa, kun Taitaja2014-tapahtuman laitteet eivät ole vielä tiedossa, ei voida sitoutua MAC-pohjaiseen VLAN:iin. Toisaalta MAC-pohjainen VLAN on mahdollista ottaa käyttöön tapahtuman aikana, mikäli sen käyttämistä ei koeta olennaisesti rasittavan käytössä olevia resursseja, hidastavan laitteiden käyttöönottoa tai niiden käyttäjiä.

6.4 Testaus 2: palomuuri ja perusverkko

Testauksessa 2 ideana oli konfiguroida perusasetukset palomuuriin, lisätä palomuuri testauksen 1 verkkotopologiaan ja testata palomuurin toimintaa käytännössä. Palomuuria lukuun ottamatta laitteisto oli sama kuin testauksessa 1. Palomuuri sijoittui Internetin ja kytkimen 1 väliin kuvion 25 mukaisesti.



KUVIO 25. Testauksen 2 verkkotopologia

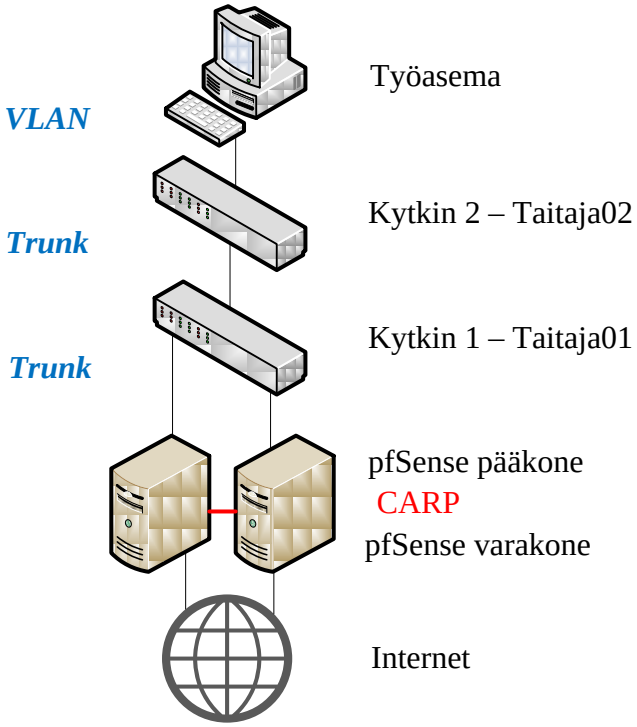
Palomuuriksi valittiin pfSense-ohjelma ja testaus aloitettiin pfSensen asennuksella tyhjään työasemaan. Asennuksessa komentoriviltä määriteltiin, mitkä työaseman verkkokortit toimivat WAN- ja LAN-yhteytenä, ja luotiin VLAN-liityntä LAN-liitynnän alle. Tämän jälkeen pfSenseä oli mahdollista konfiguroida LAN-liitynnässä kiinni olevalla laitteen webselaimella ja sitä kautta tehtiin asennus loppuun sekä konfiguroitiin perusasetukset.

Varsinaisessa testissä pfSenseen luotiin LAN-liitynnän alla olevalle VLAN-liitynnälle palomuurisääntö, joka sallii VLAN:n liikenteen Internetiin. Palomuurisäännön toimivuus testattiin vaihtamalla työasema, jonka pääsyä Internetiin testattiin, eri porttiin ja VLAN:iin kytkin 2:ssa. Pfsensen palomuuri estää oletuksena kaiken liikenteen, ellei sitä ole sallittu. Tästä syystä aina kun työasema oli eri VLAN:ssa kuin salliva palomuurisääntö, yhteyttä Internetiin ei ollut. Palomuurisääntö ja verkko toimivat testissä niin kuin pitikin.

Vaihtoehtona olisi ollut oman, erillisen palomuurin asentaminen jokaiseen laitteeseen, jos verkossa ei olisi ollenkaan käytetty palomuuria eikä reititintä. Merkittävin haitta olisi ollut verkon ulkoapäin tulevan liikenteen täysi pääsy omaan sisäverkkoon. Ilman verkossa olevaa reititintä VLAN-verkkojen käyttämisen hyöty olisi hävinnyt kokonaan ja VLAN-verkkojen välinen liikennöinti ei olisi ollut mahdollista.

6.5 Testaus 3: CARP, VLAN ja DHCP

Testauksessa 3 luotiin kytkimiin VLAN:ja kattamaan Taitaja2014-tapahtuman tarpeet ja pfSensellä testattiin VLAN:ien palomuurisäännöt, CARPia, DHCP:tä ja NAT poolia. Testauksen 2 pfSensen perustoimintojen testauksen jälkeen alettiin tutkia pfSensen vikasietoisuuden parantamista tuomalla rinnalle varakone ja käyttämällä niiden välillä CARP:a (kuvio 26). CARP:n avulla pääkoneen hajotessa varakone ottaa pääkoneen tehtävät lennossa ja jatkaa sen roolissa saman tien. CARP:n käyttö edellyttää, että laitteiden välillä otetaan käyttöön vain CARP:n osapuolten väliseen liikennöintiin tarkoitettu verkkokortti. Verkkokortin liitynnälle annettiin nimi CARPSYNC ja niille luotiin IP-osoitteet: pääkone 192.168.11.11 ja varakone 192.168.11.12. CARP:n osapuolille määriteltiin pfSensestä, onko laite pääkone (master) vai varakone, ja molempiin laitteisiin määriteltiin vastapuolen IP-osoite sekä se, että synkronisointi on päällä. Pääkoneeseen määriteltiin synkronisoitavat asiat ja varakoneen tunnukset, jotka pääkone tarvitsee tietojen synkronisointiin.



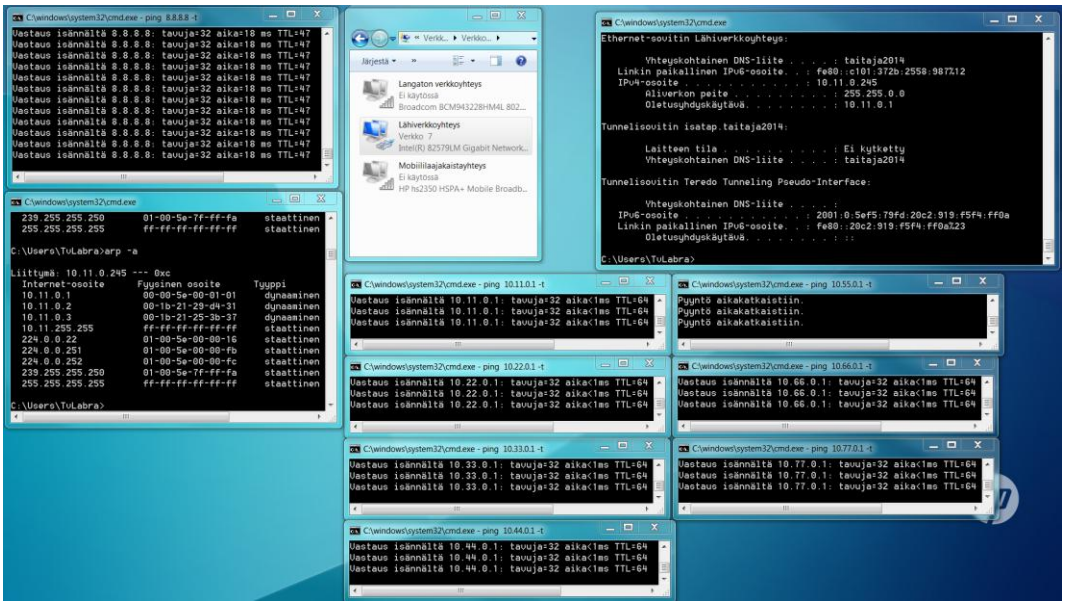
KUVIO 26. Testauksen 3 verkkotopologia

CARP:n toiminta vaatii, että molemmille koneille on luotu jokaiselle VLAN-liitynnälle virtuaali IP. Virtuaali IP on laitteiden yhteinen IP, jona pfSenset näkyvät muulle verkolle yhtenä. CARP:n yhtenä etuna on se, että se synkronoi monia tietoja osapuolten välillä, jolloin hallinnointi ja muutokset esimerkiksi palomuurisääntöihin tarvitsee tehdä vain pääkoneeseen. Mutta kaikkiin osapuoliin on laitettava käsin muuan muassa liitynnät, virtuaali IP:t ja VLAN:t.

Jos CARP:a eli vikasietoisuutta ei olisi käytetty pfSense-laitteiden välillä, niin vikasietoisuuden tuoma lisävakuutus varalaitteesta olisi poistunut vaikuttamatta verkon toiminnallisuuteen. Todennäköisyys, että pfSense-laite olisi lakannut toimimasta kesken tapahtuman, on pieni, eikä verkossa ole muuallakaan panostettu vikasietoisuuteen. CARP:n tuoma lisäkapasiteetti kuorman tasauksen muodossa on arvokas lisä, koska Taitaja2014-tapahtuman verkkoliikenteen määrä tai piikit on tässä vaiheessa arvailujen varassa, eli pienellä rahallisella sijoituksella ja työvaivalla saatu lisäkapasiteetti kannattaa hyödyntää edes varmuuden varaksi. CARP:n suunnittelu, tekeminen ja ylläpitäminen on varsin helppoa ja laitteisto on vaatimuksiltaan pieni.

Vikasietoisuuden parantaminen koko verkossa olisi vaatinut topologiaan silmukoita tai useampia reittejä ainakin verkon avainkohtiin. Vikasietoisessa verkossa olisi voitu käyttää logiikkaa, jossa on pääyhteyksiä varayhteyksineen tai liikenteelle olisi ollut monta reittiä ja useasta reittivaihtoehdosta reitin olisi päättänyt verkon aktiivilaitteet.

CARPin testauksien loputtua luotiin kytkimiin useampia VLAN-verkkoja ja niiden liikennöintiä pyrittiin rajoittamaan pfSensen palomuurisäännöillä niin, että VLAN-verkot pystyivät liikennöimään vain haluttuihin muihin VLAN-verkkoihin sekä joissakin tapauksessa Internetiin. pfSensen VLAN:ien välisten palomuurisääntöjen testaamisessa käytettiin työasemasta jokaiseen VLAN-verkkoon ja Internet-yhteyden virkaa simuloivaa IP-osoitteeseen 8.8.8.8 kohdistuvaa jatkuvaa pingausta (kuvio 27). Pingauksien ollessa päällä vaihdettiin työaseman porttia kytkimessä yksitellen jokaiseen VLAN:iin ja tarkastettiin, että palomuurisäännöt toimivat halutulla tavalla ja jokaisesta VLAN:sta oli yhteys niihin VLAN:eihin, joihin oli tarkoituskin.



KUVIO 27. pfSensen VLAN:ien välisten palomuurisääntöjen testaus pingaamisella

VLAN-verkkojen tekemisessä logiikka, jolla VLAN-verkkoihin kuuluvat laitteet jaotellaan, voi olla hyvinkin erityyppinen. Mitä pienempiin loogisiin osiin laiteryhmät pystytään jakamaan, sen tarkemmin niiden liikennöintiä voidaan pelkällä VLAN-verkkoon kuulumisella rajoittaa ja säädellä. Suurempi määrä VLAN-verkkoja tarkoittaa myös suurempaa määrää palomuurisääntöjä, joilla VLAN-verkkojen välistä liikennöintiä mahdollistetaan ja reititetään.

Myöskään palomuurisäännöissä ei ole yhtä oikeaa ratkaisua, vaan niiden laatiminen on mahdollista monella eri logiikalla ja sama toiminnallisuus voidaan toteuttaa useammalla tavalla. Testatuissa säännöissä noudatetaan järjestäjätahon linjauksia. Vaihtoehtoisesti palomuurisäännöt olisi voitu määritellä paljon tarkemmiksi ja yksityiskohtaisemmiksi käyttämällä säännöissä liikenteen tarvitsemia tarkkoja portteja, verkkoprotokollaa sekä lähde- ja kohdeosoitteita.

Tarkemmat palomuurisäännöt olisivat edellyttäneet tarkempaa tietämystä verkosta, verkon käyttäjistä, laitteista ja verkon käyttötarkoituksista. Taitaja2014-tapahtuman verkon tarkempi verkkoliikenne ei ole tässä vaiheessa tiedossa, mutta palomuurisääntöjä on mahdollista tarkentaa tulevaisuudessa verkon ja sen

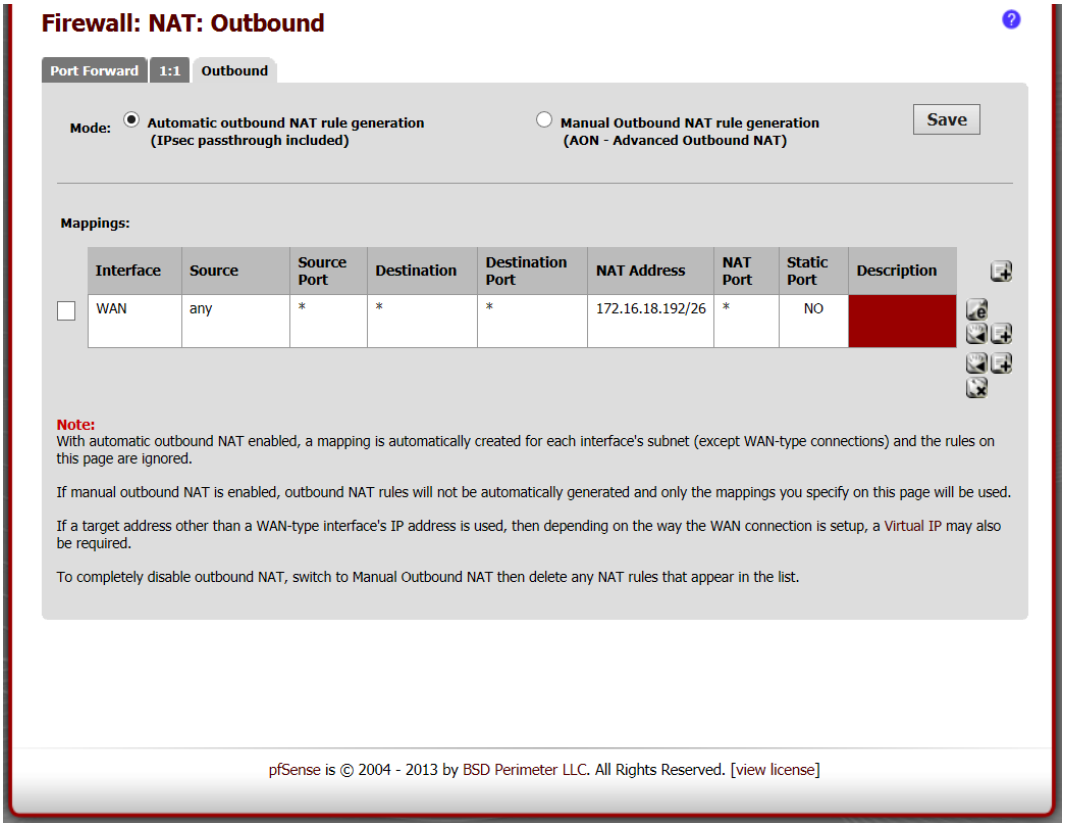
suunnitelman tarkentuessa. Tarkempien palomuurisääntöjen huonona puolena on se, että verkon eläessä ja muuttuessa tulisi helpommin ongelmia verkon toimivuudessa. Taitaja2014-tapahtuman kaltaisessa tapahtumassa toimivuus ja toimintavarmuus ovat ensisijaisia asioita ja tietoturva tulee vasta näiden jälkeen. Lisäksi tarkemmat palomuurisäännöt tarvitsevat perusteellisempaa suunnittelua sekä testaamista, koska näistä tarkemmista säännöistä saatu hyöty häviää, jos verkko ei toimikaan kaikilta osin niin kuin sen tarvitsisi.

VLAN:ien luonnin ja palomuurisääntöjen jälkeen testattiin pfSensen DHCP-palvelinta. Koska Taitaja2014-tapahtumaan oletetaan tulevan väkeä niin paljon, että julkisia IP-osoitteita ei olisi mitenkään ollut tarpeeksi edes kaikille verkon laitteille, tapahtuman vierailijoista puhumattakaan. Verkossa pitää ottaa käyttöön DHCP-palvelin, jonka avulla käyttöön saadaan riittävästi IP-osoitteita. Kukin VLAN on omassa aliverkossa ja siten tarvitsevat DHCP:lle oman erillisen DHCP poolin, IP-avaruuden, josta IP-osoitteita jaetaan VLAN:n laitteille. DHCP:n käyttöönotto pfSensessä oli varsin helppoa; liityntöihin tarvitsi vain laittaa DCHP päälle, määritellä IP-alue, jolta liitynnän laitteet saavat IP:n, määritellä gatewayksi pfSensen yhteinen virtuaali IP. Vaikein asia oli päättää DHCP poolin IP-alueen koko.

Jos DHCP-palvelin olisi ollut käytetyn pfSensen sijaan erillinen laite, pfSensessä olisi käytetty DHCP-relayta. Tällöin IP-osoitteiden hallinta ja jakelu olisi ollut tehokkaampaa, selkeämpää ja käytössä olisi ollut enemmän ja syvällisempiä DHCP:hen liittyviä toimintoja ja asetuksia. Huonoja puolia olisivat kokonaan uuden laitteen hankkiminen, asentaminen, konfigurointi ja käyttöönotto. Tämän työn puitteissa ei erillistä DHCP-palvelinta otettu käyttöön, mutta varsinaisessa Taitaja2014-tapahtumassa erillisen DHCP-palvelimen käyttäminen mahdollista.

Kun verkossa on DHCP ja NAT käytössä kaikki sisäverkon laitteet näkyvät ulkomaailmaan liikennöivän yhdestä IP-osoitteesta ja/tai useammasta portista. NAT poolilla voidaan lisätä ulkoverkon IP-osoitteiden määrää, joina sisäverkon liikenne näkyy. Testauksien 3 aikana WAN-liitynnän IP-osoite täytyi tulla DHCP:n kautta olosuhteiden pakosta, joten NAT poolia ei ollut mahdollista testata kuin teoreettisesti. Testeissä kuitenkin selvisi, mistä pfSensen valikoista ja

miten NAT poolin saa halutessaan tehtyä. Valikosta Firewall:NAT:Outbound voidaan vaihtaa automaattisen NAT-sääntöjen luonnin sijaan manuaalinen sääntöjen luonti. Manuaalisesti voidaan määritellä sääntöjä, kuten mikä aliverkkoavaruus NAT:taan ja mihin ulkoverkon IP-osoitteeseen (kuvio 28).

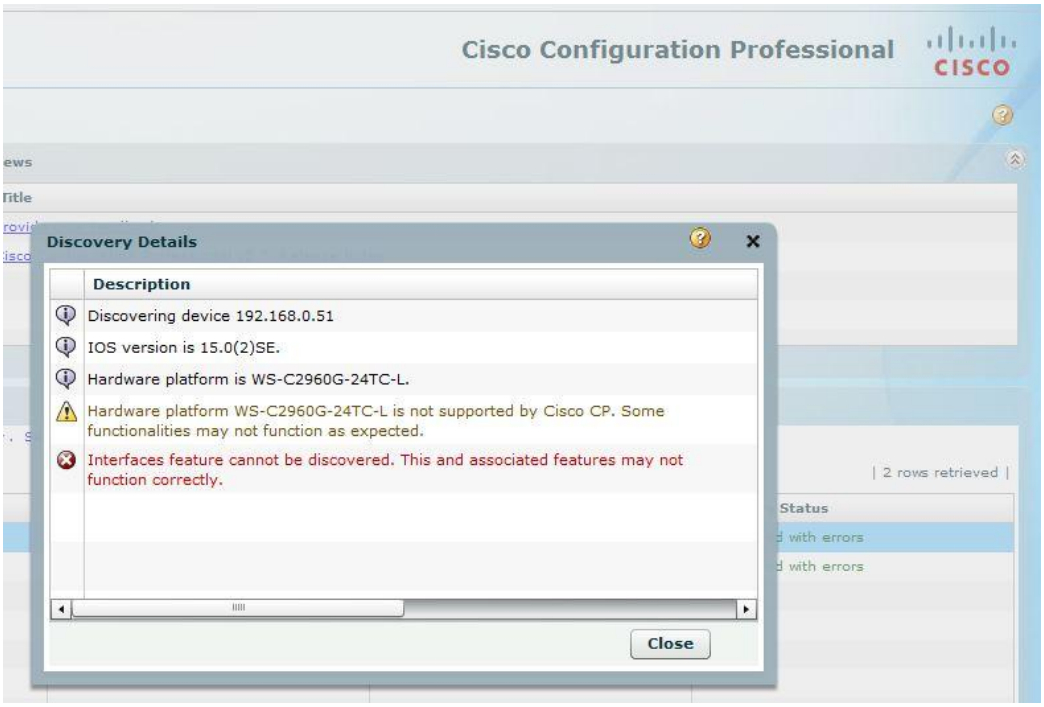


KUVIO 28. NAT ja NAT pool pfSensessä

6.6 Testaus 4: etähallintaohjelmien testaus

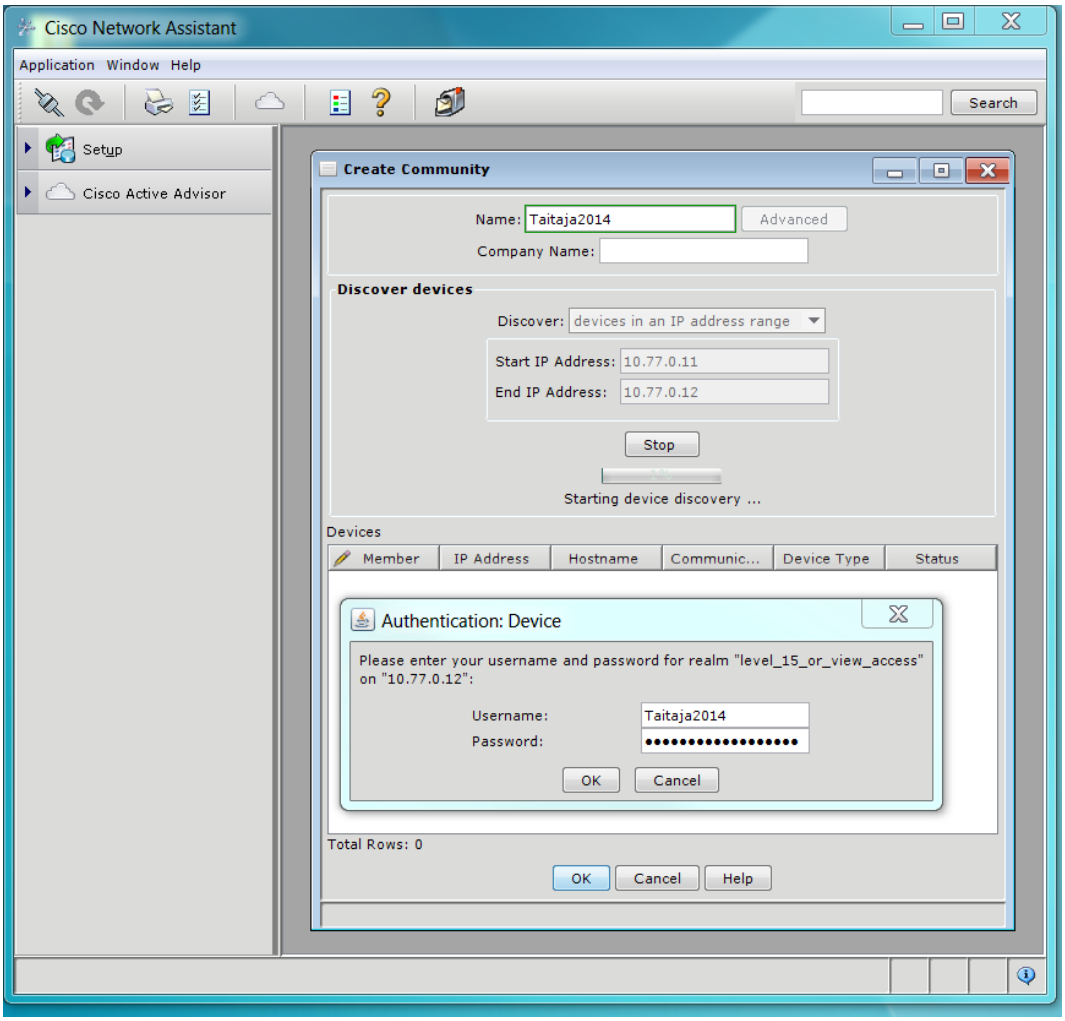
Ison verkon yksittäisten aktiivilaitteiden konfigurointi on hidasta ja työlästä. Tämän vuoksi testattiin myös verkon aktiivilaitteiden etähallintaohjelmia. Ensimmäisenä vaihtoehtona testattiin Cisco Configuration Professional (CP) etähallintaohjelmaa. CP-ohjelman testaus lopetettiin lyhyeen, sillä asennuksen jälkeen ohjelma ilmoitti suoraan, ettei ohjelma tue käytössä olevaan kytkinmallia

(kuvio 29). Vaikkei kytkinmallille ei ollut tukea, niin ohjelmalla saatiin tehtyä joitakin asetuksia kytkimelle, muttei kuitenkaan riittävästi.



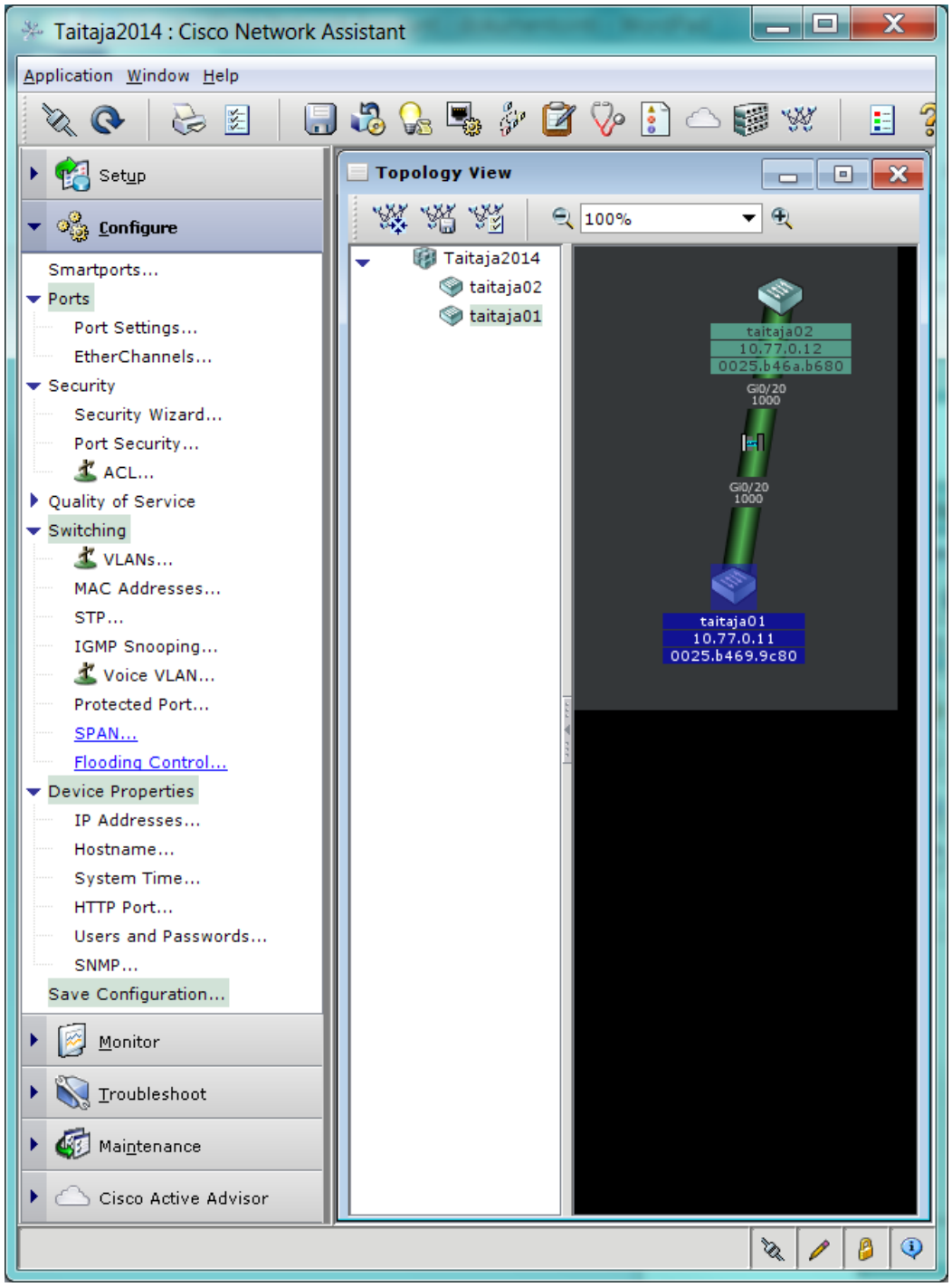
KUVIO 29. Cisco Configuration Professionalin vikailmoitus

Ensimmäisen etähallintaohjelman testauksen ollessa selkeä epäonnistuminen, siirryttiin seuraavaan vaihtoehtoon eli ohjelmaan nimeltä Cisco Network Assistant (NA). Kuvion 30 mukaisesti ohjelmassa luodaan ensin verkon laitteille yhteisö (community) ja nimetään se sekä määritellään ohjelman kommunikointiasetukset ja tapa, jolla ohjelma löytää verkon laitteet. NA-ohjelman löytäessä laitteen tarvitsee löydetyille laitteilla antaa kunkin laitteen käyttäjätunnus ja salasana.



KUVIO 30. Cisco Network Assistant 5.8.7. -yhteisö (community)

Kun yhteisö on luotu ja löydetty, luo ohjelma verkon laitteista topologiakuvan kuvion 31 mukaisesti. Topologiakuvasta voidaan nähdä muun muassa laitteiden loogiset kytkennät toisiinsa nähden, nimet, IP-osoitteet, MAC-osoitteet ja kytkentöjen liityntien porttien numerot ja nopeudet. Muutoksien tekeminen etähallinnalla yhteisöön on helppoa ja huomattavasti nopeampaa kuin konsolipiuhalla jokaiseen laitteeseen kytkeytyen tai pääteohjelmalla yhteyksien ottaminen.



KUVIO 31. Cisco Network Assistant - topologiakuva ja valikot

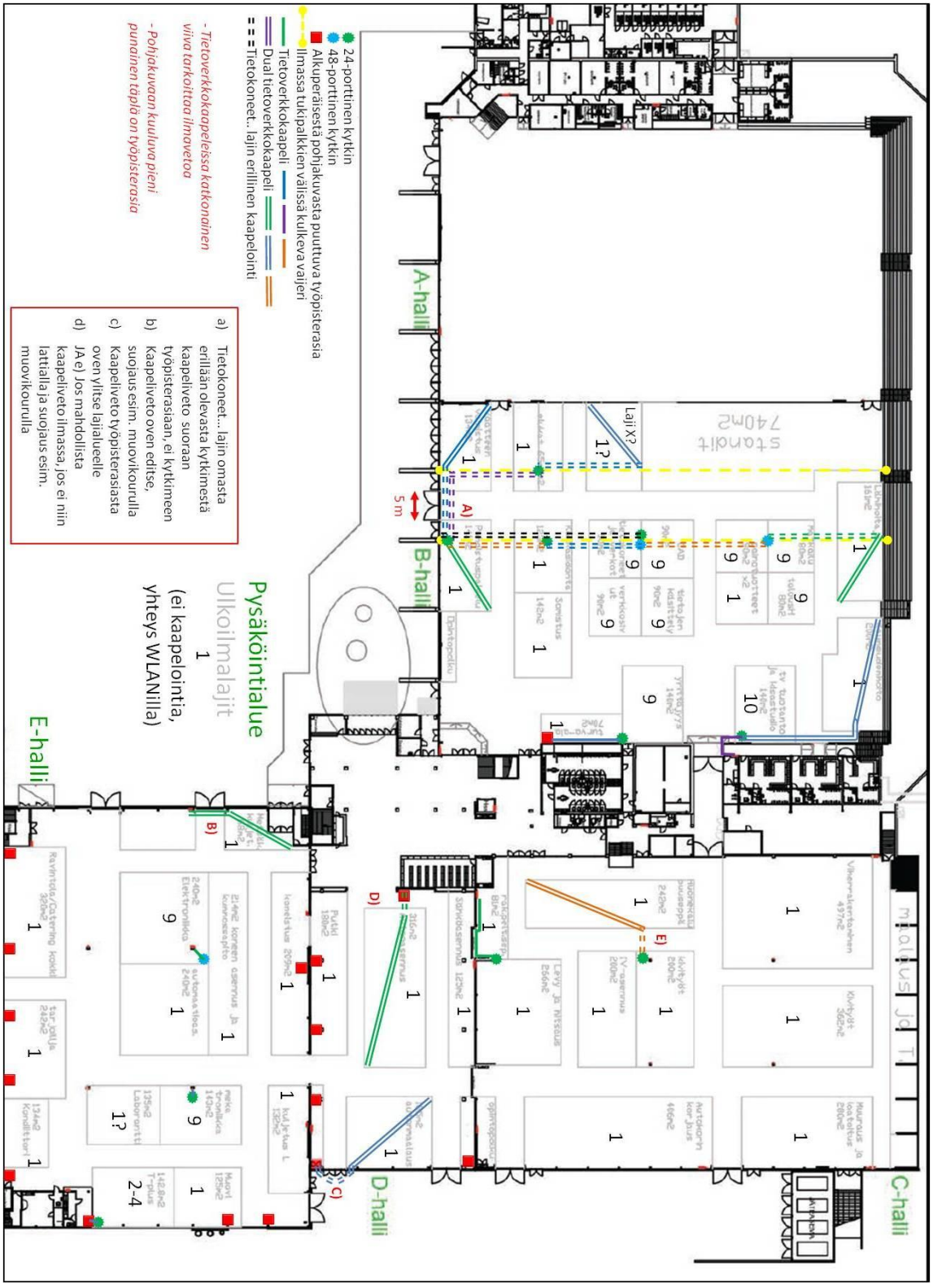
7 TIETOVERKON RAKENNE

Tässä luvussa esitellään luvun 6 testauksien perusteella saadut tulokset ja niiden pohjalta tehdyt valinnat Taitaja2014-tapahtuman verkkosuunnitelmaksi.

7.1 Kytkimien konfiguraatio ja kaapeloinnin ja kytkimien verkkokuva

Taitaja2014-tapahtuman runkoverkossa on kahden tyyppisiä kytkimiä: verkon reunalla oleva pääkytkin, johon kaikki sisäverkon kytkimet ja työpisterasiat ovat yhteydessä, sekä sisäverkon kytkimet, joilla varsinainen sisäverkon runko on toteutettu. Sisäverkon kytkimien konfiguraatiopohja mukautetaan sijoituskohtaisesta, ja pääkytkimen konfiguraatioon muutetaan vain porttien VLAN-määritykset. Pääkytkimen konfiguraatio on liitteessä 1, ja sisäverkon kytkimien konfiguraatiopohja on liitteessä 2.

Taitaja2014-tapahtuman verkon toteuttamiseen aktiivilaitteita tarvitaan 18 kytkintä ja 1 varajärjestelmällä varmistettu palomuuri/reititin. Kytkimien määrät halleja kohden ovat: B-halli 8 kytkintä, C-halli 2 kytkintä, D-halli 0 kytkintä ja E-halli 3 kytkintä. B-, C-, E- ja E-halleilla jokaisella on oma konehuone, jokaiseen konehuoneeseen tarvitaan 1 kytkin, eli yhteensä 4 kytkintä. Konehuoneiden välinen yhteys kulkee pääkonehuoneen kautta, jonne tarvitaan oma kytkin, pääkytkin. Kytkimien sijoitus halleihin ja niiden väliset kaapeloinnin tehdään kuvion 32 verkkokuvan mukaisesti.



KUVIO 32. Taitaja2014-tapahtuman verkkokuva (kaapelointi ja kytkimet)

Verkkokuvan kuvion 32 mukaiseen runkoverkon toteuttamiseen tarvitaan 803 metriä CAT6-parikaapelia, joista 82 metriä on alle 20 metrin kaapeleita ja 721 metriä on yli 20 metrin kaapeleita. Kokonaiskaapelipituudesta dual parikaapelia on 753 metriä ja tavallista parikaalia on 50 metriä.

7.2 VLAN

Verkkoliikenteen erottaminen toisistaan tapahtuu käyttämällä kytkimissä VLAN:ja, jotka määritellään porttikohtaisesti tarpeen mukaan. Kytkimistä vedetään kaapelit lajipisteisiin oikeasta portista oikeaan käyttäjään. Esimerkiksi toimitsijaVLAN:iin kuuluvasta portista vedetään kaapeli lajipisteessä olevaan toimitsija tietokoneeseen. Kytkimet ovat lukollisissa kaapeissa, joten voidaan olettaa, että vain oikeat henkilöt pääsevät lisäämään, muuttamaan ja poistamaan kytkimien porteissa olevia kaapeleita.

VLAN:eille luotiin niiden numeroiden perusteella sitä vastaava aliverkko ja DHCP-alue taulukon 8 mukaan. pfSense-tietokoneiden liityntien IP-osoitteet määriteltiin seuraavasti: virtuaali IP on aliverkon ensimmäinen osoite (10.xx.0.1/16), pääkoneen VLAN-liitynnän IP on aliverkon toinen osoite (10.xx.0.2/16) ja varakoneen VLAN-liitynnän IP on aliverkon kolmas osoite (10.xx.0.3/16). Jokaisen aliverkon IP-alue 10.xx.0.0-10.xx.0.255 on tarkoitettu staattisille osoitteille, esimerkiksi verkon laitteille, jotka muodostavat verkon toiminnallisen rungon ja eivät tule poistumaan verkosta. Tällaisia laitteita ovat esimerkiksi kytkimet, reititin, WLAN-tukiasemat, WLAN-kontrolleri ja tulostinpalvelin. Virtuaali IP on yhteinen ainoa muille näkyvä IP-osoite, johon molemmat pfSense-tietokoneet vastaavat ja käyttävät sitä liikennöidessään. DHCP:n IP-alue on alue, josta aliverkon laitteille jaetaan dynaamisesti IP-osoitteita. Kussakin aliverkossa on jaettavia IP-osoitteita suuruusluokaltaan 60 000 kappaletta, joka on sellainen määrä, ettei IP-osoitteet varmasti lopu kesken.

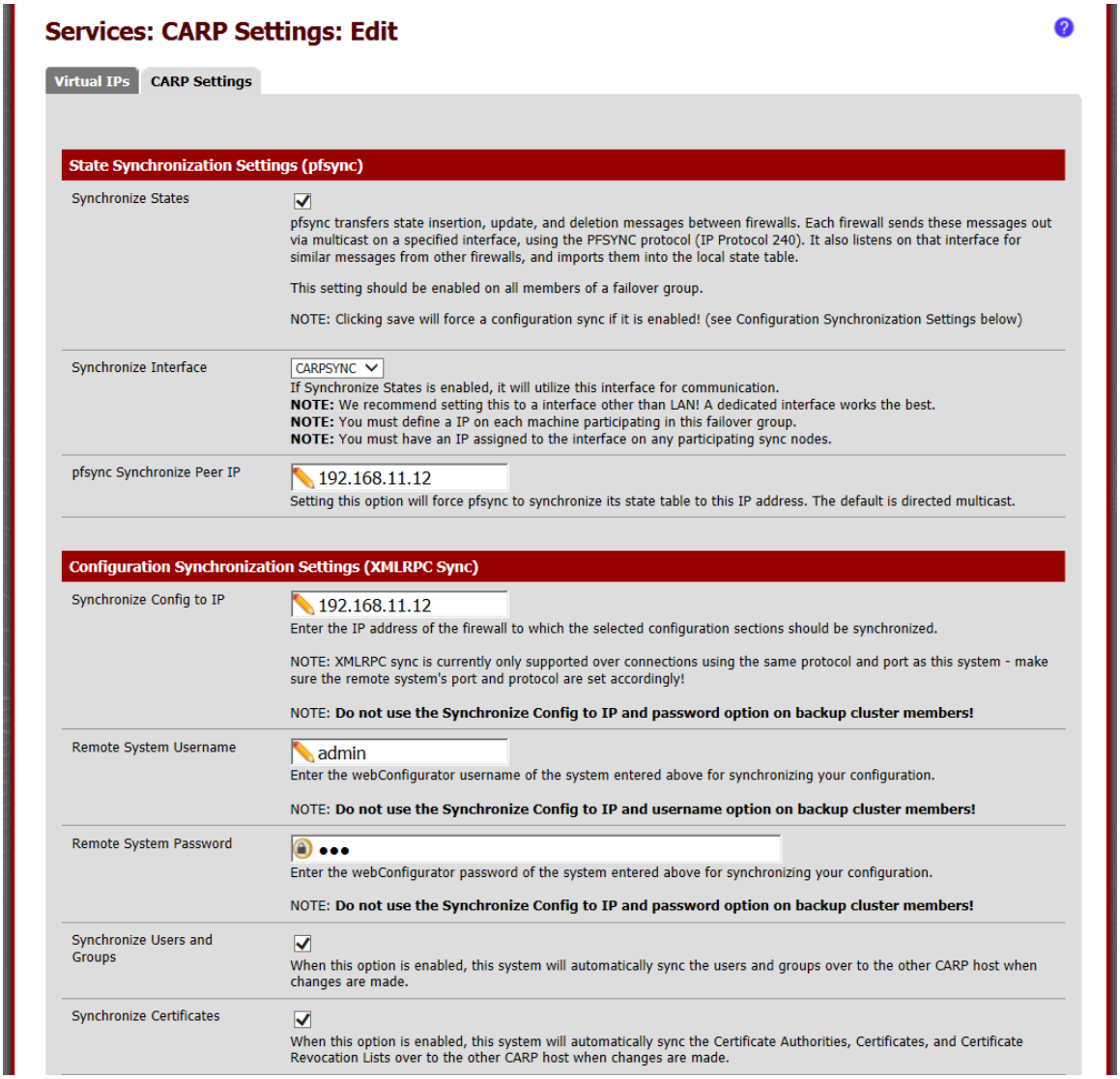
TAULUKKO 8. pfSense-tietokoneiden määritykset: VLAN, DHCP, liityntien IP:t

VLANin numero	VLANin nimi	DHCP:n IP-alue	Liitynnän IP - pää- ja varakone	Virtuaali IP
11	Hallinto	10.11.1.0-10.11.255.254	10.11.0.2/16, 10.11.0.3/16	10.11.0.1/16
22	Toimitsija	10.22.1.0-10.22.255.254	10.22.0.2/16, 10.22.0.3/16	10.22.0.1/16
33	Kilpailija	10.33.1.0-10.33.255.254	10.33.0.2/16, 10.33.0.3/16	10.33.0.1/16
44	Tulostin	10.44.1.0-10.55.255.254	10.44.0.2/16, 10.44.0.3/16	10.44.0.1/16
55	Yleisö	10.55.1.0-10.55.255.254	10.55.0.2/16, 10.55.0.3/16	10.55.0.1/16
66	WLAN	10.66.1.0-10.66.255.254	10.66.0.2/16, 10.66.0.3/16	10.66.0.1/16
77	Aktiivilaite	10.77.1.0-10.77.255.254	10.77.0.2/16, 10.77.0.3/16	10.77.0.1/16

VLAN:t luotiin ja jaoteltiin sisältämiensä laitteiden mukaan seuraavasti:

- Hallinto: verkon hallinnoimiseen tarkoitetut laitteet
- Toimitsija: lajien yhteydessä olevat toimitsijatietokoneet
- Kilpailija: lajeissa olevat kilpailijoille tarkoitetut tietokoneet
- Tulostin: verkkotulostimet ja tulostinpalvelin
- Yleisö: yleisön käyttämät laitteet, esimerkiksi älypuhelimet ja tabletit
- WLAN: WLAN-tukiasemat
- Aktiivilaite: kytkimet ja pfSense-tietokoneet (palomuuri/reititin).

pfSensejen välinen CARP saatiin toimimaan ottamalla koneiden väliset verkkokortit käyttöön IP:eillä pääkone 102.168.11.11 ja varakone 192.168.11.12. CARP-laitteiden välinen liityntä nimettiin CARPSYNC:ksi. Pää- ja varakoneeseen laitettiin synkronisointi päälle, pääkoneeseen siten että synkronisoi kaikki tiedot sekä varakoneen tunnuksen ja salasanan kuvion 33 mukaisesti. Kuvion 33 alaosassa olevat kaikki synkronisointiin liittyvät vaihtoehdot laitettiin päälle.



KUVIO 33. CARPin pääkoneen asetukset

Laboratoriotesteissä pfSensejen WAN-liitynnän IP tuli DHCP:ltä. Itse Taitaja2014-tapahtumassa ei voida käyttää dynaamista IP:tä vaan silloin pitää olla staattinen IP, koska itse tapahtumassa on todella paljon käyttäjiä, jolloin NAT:n kanssa on viisasta käyttää useampaa IP:tä kuin WAN-liitynnän ainutta. NAT pool antaa mahdollisuuden määritellä alueen IP-osoitteita, joita voidaan käyttää NAT:ssa. NAT poolissa voidaan määritellä, että tietty sisäverkon aliverkko NAT:taan tiettyyn ulkoverkon IP-osoitteeseen. Tämä helpottaa liikennöinnin

havainnointia, kun NAT:atusta ulkoverkon IP-osoitteesta verkon ylläpitäjä pystyy päättelemään sisäverkon aliverkon osoitteen.

7.3 Palomuurisäännöt

pfSense on tilallinen palomuuri, joten palomuurisäännöissä tarvitsee vain aukaista lähtevälle liikenteelle tie, koska pfSense osaa itse aukaista paluuliikenteelle tien. pfSense käy läpi palomuurisääntöjä järjestyksessä alusta loppuun, käyttää ensimmäistä täsmäävää sääntöä ja lopettaa sääntöjen läpi käymisen. Tästä syystä sääntölistassa voidaan ensin käyttää sallivaa sääntöä ja sen jälkeen kieltävää sääntöä. Tästä on se etu, että näin sääntöjä on helpompi muokata ja tarkentaa, kun sallivaa sääntöä ei tarvitse luoda tyhjästä. Sallivan säännön ei yleensä ole tarkoitus olla kaiken salliva tiettyyn verkkoon vaan esimerkiksi sallia vain tarvittavat portit, esimerkiksi http-liikenteelle portin 80.

Palomuurisäännöt koottiin tiivistetysti liitteisiin (LIITTEET 3 – 7), joissa on käytetty seuraavia termejä:

- **Enable** = onko palomuurisääntö voimassa
- **Pass/Block/Reject**
    - **Pass** = liikenne sallitaan
    - **Block** = torjutaan liikenne, ei ilmoitusta lähettäjälle
    - **Reject** = kielletään liikenne ja kieltämisestä ilmoitetaan lähettäjälle
- **Proto** = mikä protokolla
- **Source** = mikä kohde
    - *nimi* net, esimerkiksi 11HALLINTO net = 11HALLINTO-verkko
    - *nimi* address, esimerkiksi 11HALLINTO address = 11HALLINTO-verkon liitynnän osoite
        - Port = mikä lähdeportti
- **Destination** = mikä kohde
    - *nimi* net, esimerkiksi 11HALLINTO net = 11HALLINTO-verkko
    - *nimi* address, esimerkiksi 11HALLINTO address = 11HALLINTO-verkon liitynnän osoite
        - Port = mikä kohdeportti
- ***** = any, eli mikä vaihtoehto vaan

Jos liitteissä ei ole muuta mainittu, niin Source/Destination-kohdissa kyseessä on liitynnän aliverkko (net) ja poikkeustapauksessa itse liitynnän osoite (address). Liitynnöissä, jotka sallitaan Internetiin, täytyy toiminnan kannalta sallia myös DNS-liikenne. DNS-liikenteen salliminen tarkoittaa palomuurisääntöä, joka sallii UDP-liikenteen liitynnän aliverkosta liitynnän porttiin 53.

Palomuurisäännöissä käytetyt aliakset on liitteissä merkitty italic fontilla:

- carp11 = 10.11.0.2 ja 10.11.0.3
- carp22= 10.22.0.2 ja 10.22.0.3
- carpXX=10.XX.0.2 ja 10.XX.0.3

Palomuurisäännöt:

- Liityntä WAN (liite 3)
- Liityntä 11HALLINTO (liite 3)
- Liityntä CARPSYNC (liite 4)
- Liityntä 22TOIMITSIJA (liite 4)
- Liityntä 33KILPAILIJA (liite 5)
- Liityntä 44TULOSTIN (liite 5)
- Liityntä 55YLEISO (liite 6)
- Liityntä 66WLAN (liite 6)
- Liityntä 77AKTIIVILAITE (liite 7).

Liitteen 6 liityntä 66WLANin palomuurisäännön, joka on tällä hetkellä pois päältä ja sallii kaiken kohteesta WLAN kohteeseen Hallinto, on tarkoitus olla sääntö, jolla sallitaan VLAN:ssa WLAN olevien WLAN-tukiasemien liikenne Hallinnossa olevaan WLAN-controlleriin. Rajauksena palomuurisäännössä voisi olla WLAN-kontrollerin kanssa tarvittavat tietyt portit ja mahdollisesti laitteen IP-osoite.

7.4 WLAN

Taitaja2014-tapahtuman verkon tarvekartoituksen ja suunnittelun perusteella ehdotetaan tapahtuman WLAN-ratkaisuksi seuraavaa määrittelyä.

Loogisia WLAN-verkkoja tarvitaan ainakin kaksi, yleisölle ja toimitsijoille omat. Tämä voidaan toteuttaa esimerkiksi käyttämällä molemmille omaa SSID:tä (Service Set Identifier) tai käyttämällä yhtä SSID:tä, jossa kirjautumistunnusten perusteella käyttäjät jaettaisiin omiin verkkoihinsa. Käyttäjät yhdistetään omiin jo muualla Taitaja2014-verkossa käytettyihin VLAN:eihin, yleisö VLAN:iin 55 ja toimitsijat VLAN:iin 22. WLAN-tukiasemien hallinnointi ja liikennöinti hoidetaan erillisellä tukiasemakontrollerilaitteella. Tukiasemakontrolleri sijoitetaan VLAN:iin 11Hallinto, sen ja tukiasemien väliselle liikenteelle aukaistaan palomuuriin tarvittavat portit (VLAN:n 66WLAN ja 11Hallinto välillä).

WLAN:n kuuluvuusalue pitää kattaa hallit A, B, C, D ja E sekä Messukeskuksen sisäänkäynnin pysäköintialue ja Messukeskuksen aula. WLAN-tukiasemia tulisi olla seuraavasti:

- vähintään kaksi jokaiseen kilpailussa käytettävään halliin (B, C, E ja D)
- yksi kappale B-hallin pysäköintialueen puoleiseen ikkunaan kattamaan pysäköintialue
- vähintään yksi A-halliin
- vähintään yksi Messukeskuksen aulaan.

Tavoitteena on tarjota 200 - 400 käyttäjälle WLAN-yhteys jokaiseen kilpailussa käytettävään halliin. WLAN-tukiasemien pitäisi olla vähintään 802.11g-tekniikan laitteita ja mahdollisuuksien mukaan tuettaisiin 802.11n-tekniikkaa.

Vaihtoehtona edellä kerrotulle WLAN-ratkaisulle olisi, että langallinen verkko olisi ollut vain runkoyhteys ja varayhteys WLAN:lle, joka olisi toiminut pääyhteytenä koko Taitaja2014-tapahtumalle. Tällä ratkaisulla olisi saatu erilainen

ja yksinkertaisempi topologia, joka olisi voitu rakentaa vähemmällä määrällä kytkimiä, mutta WLAN-tukiasemia olisi tarvittu enemmän. Etuna olisi, ettei verkonkäyttäjien tarkalla sijainnilla olisi väliä, ja verkonkäyttäjät voisivat jopa liikkua eikä kaapelivetoja tarvitsisi niin montaa. Haittapuolena WLAN:n käyttämisenä pääyhteytenä olisi ollut, että verkkoliikenne olisi voinut ruuhkautua ja toimia liian hitaasti WLAN-tekniikoiden huomattavasti pienempien verkkonopeuksien vuoksi kuin langallisissa yhteyksissä. WLAN-tekniikan rajoittamaa liikenteen nopeutta olisi ollut mahdollista nopeuttaa lisäämällä tukiasemien määrää ja jakamalla katettava kuuluvuusalue pienempiin alueisiin. Tästä saatava hyöty olisi riippuvainen myös käyttäjien jakaantumisesta tasaisesti etenkin liikennenopeuden mukaan eri tukiasemien kuuluvuusalueille. WLAN-verkon kuuluvuusalue on vaikea saada kattamaan haluttu alue tasaisesti. WLAN:n käyttämiseen pääyhteytenä ei päädytty, koska siinä koettiin olevan liian paljon tuntemattomia tekijöitä ja epävarmuutta.

8 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tässä opinnäytetyössä laadittiin verkkosuunnitelma Taitaja2014-tapahtumaan, joka pidetään Lahden Messukeskuksessa. Työn teoriaosuudessa tutustuttiin verkkosuunnitteluun tiiviisti liittyviin kokonaisuuksiin, kaapelointiin, verkon aktiivilaitteisiin ja ohjelmistoihin sekä langattomaan lähiverkkoon. Teoriatiedon pohjalta oli mahdollista alkaa miettiä varsinaista verkkosuunnitelman laatimista.

Verkkosuunnitelman kannalta tärkeimmät esitiedot olivat käytettävä kytkinmalli (Ciscon 2960S) sekä työpisterasioiden määrä ja sijainti Taijata2014-tapahtuman pitopaikalla eli Lahden Messukeskuksen halleissa. Järjestäjätahon linjauksen perusteella verkkokapasiteetti mitoitettiin siten, että jokaista oikeaa tarvetta kohden on yksi varapaikka, eli verkko mitoitetaan 276 tietokoneelle laskennallisen arvon 138 sijaan.

Verkon suunnittelu ja testaaminen sekä aktiivilaitteiden testaaminen eivät välttämättä ole erillisiä toimenpiteitä, vaan ne voidaan tehdä toisiansa tukien, limittäin. Testaamisessa ei käytetty mitään valmista suunnittelumallia, vaan testisuunnitelmaa laadittiin kohta kohdalta edellisten tulosten pohjalta. Tuleva Taitaja2014-verkko testattiin laboratorio-olosuhteissa, mikä loi omat haasteensa, sillä on hankalaa luoda kooltaan, liikennemäärältä, asiakaslaitemäärältään ja liikenteen monimuotoisuudelta vastaavaa verkkoa kuin todellisuudessa.

Laboratoriotestausten perusteella laadittiin verkkokuva, jossa näkyvät Taitaja2014-tapahtuman verkon toteuttamiseen tarvittavien aktiivilaitteiden määrät ja sijainnit sekä kaapelivedot. Verkkosuunnitelmassa jaettiin verkkoliikenne seitsemään eri verkkoon käyttäjien mukaan. Verkkoliikenteen jakaminen toteutettiin käyttämällä kytkimissä VLAN:ja, joille luotiin erilaisia palomuurisääntöjä pfSensellä. Verkkosuunnitelman mukaan WLAN-verkkoja tarvitaan ainakin kaksi, yleisölle ja toimitsijoille omat. Tämä voidaan toteuttaa esimerkiksi käyttämällä molemmille omaa SSID:tä tai käyttämällä yhtä SSID:tä, jossa kirjautumistunnusten perusteella käyttäjät jaettaisiin omiin verkkoihinsa.

Nykyiset palomuurisäännöt pohjautuvat PHKK:n linjauksiin verkkosuunnittelusta ja verkkotietoturvallisuudesta. Lähempänä Taitaja2014-tapahtumaa

verkkoliikenteen yksityiskohtien hahmottuessa paremmin voidaan tarkentaa eri VLAN:ien välisiä palomuurisääntöjä.

Hyvän tietoverkon rakentamisen tärkeä osa on verkkosuunnittelu, joka mahdollistaa kustannustehokkaan tietoverkon rakentamisen. Huolellisesti tehdyllä verkkosuunnittelulla voidaan välttää karikot verkon rakentamisvaiheessa ja ennakoida verkon tulevia laajennus- tai muutostarpeita paremmin ja nopeammin. Tulevaisuudessa tietoverkkojen tarve lisääntyy koko ajan ja samalla tietoverkkoa tarvitsevien laitteiden määrä ja erilaisuus lisääntyvät. Tulevaisuudessa työpisterasiat voivat olla yhtä tärkeitä kuin sähkörasiatkin, eikä yksi työpisterasia huonetta tai tärkeitä huoneita kohden tule riittämään.

LÄHTEET

Painetut lähteet

Dulaney, E. & Hardwood, M. 2011. CompTIA Network+ N10-005 Authorized Exam Cram. 4. painos. Indiana: Que Publishing.

Geier, J. 2005. Langattomat perusteet. Helsinki: Edita Prima Oy.

Granlund, K. 2007. Tietoliikenne. Jyväskylä: WSOYpro.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: Docendo Finland Oy.

Hämeen-Anttila, T. 2003. Tietoliikenteen perusteet. Porvoo: Docende Finland Oy.

Jaakohuhta, H. 2005. Lähiverkot - Ethernet. 4. uudistettu painos. Helsinki: Edita Prima Oy.

Koivisto, P. 2009a. Optiset kaapeloinnit kiinteistössä. Espoo: Painokurki.

Koivisto, P. 2009b. Teleasennukset käytännössä 7. 2009. Espoo: Esa Print Oy

Meyers, M. 2003. Verkot + sertifikaatti. Helsinki: Edita Prima Oy.

Odom, W. 2005. Tietoverkot prusteet. Helsinki: Edita Prima Oy.

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Gummerus Kirjapaino Oy.

Schneider Electric. 2013. Actassi-järjestelmä tuoteluettelo 2013. Espoo.

SFS-käsikirja 167. 2004. Tietotekniikan yleiskaapelointi. Helsinki: SFS.

Sähkö- ja teleurakoitsijaliitto STUL ry. 2005. Teleasennusopas. 5. uusittu painos. Espoo: Otavamedia Oy.

Sähkötieto ry. 2008. Yleiskaapelointijärjestelmät. 3. uusittu painos. Espoo: Tammerpaino Oy.

Elektroniset lähteet

Cisco. 2013a. Cisco Catalyst 2960 48 Power over Ethernet (PoE) Switch [viitattu 12.8.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_bulletin_c25-512173.html

Cisco. 2013b. Understanding Rapid Spanning Tree Protocol [viitattu 12.8.2013]. Saatavissa: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

Cisco. 2013c. Understanding VLAN Trunk Protocol (VTP) [viitattu 12.8.2013]. Saatavissa: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

Countersiege. 2013. Firewall Failover with pfsync and CARP [viitattu 30.8.2013]. Saatavissa: http://www.countersiege.com/doc/pfsync-carp/

Electric Sheep Fencing LLC. 2013a. Common Deployments [viitattu 27.8.2013]. Saatavissa: http://www.pfsense.org/index.php@option=com_content&task=view&id=71&Itemid=81.html

Electric Sheep Fencing LLC. 2013b. Features [viitattu 27.8.2013]. Saatavissa: http://www.pfsense.org/index.php@option=com_content&task=view&id=40&Itemid=43.html

Electric Sheep Fencing LLC. 2013c. Home [viitattu 27.8.2013]. Saatavissa: http://www.pfsense.org/index.php@option=com_frontpage&Itemid=1.html

Electric Sheep Fencing LLC. 2013d. Minimum Hardware Requirements [viitattu 27.8.2013]. Saatavissa: http://www.pfsense.org/index.php@option=com_content&task=view&id=45&Itemid=48.html

i&i Solutions. 2006. Lähiverkon tekniikka [viitattu 17.7.2013]. Saatavissa http://www.esp.fi/attachments/filebank/19.pdf

Kompo2010. Koaksiaalikaapeli [viitattu 17.7.2013]. Saatavissa: http://kompo2010.wikispaces.com/Koaksiaalikaapeli

Kuituinfo. 2013. Kaapelirakenne [viitattu 17.7.2013]. Saatavissa: http://www.kuitu.net/portal/fi/kuituinfo/optinen_liityntaverkko/valokuitu/rakenne

Lahden Messut. 2013a. Ilmakuva [viitattu 16.8.2013]. Saatavissa: http://press.lahdenmessut.fi/downloadable_material/Ilmakuva1210hr.jpg

Lahden Messut. 2013b. Tilat [viitattu 16.8.2013]. Saatavissa: http://www.lahdenmessut.fi/tilat/

Meredith, M. 2010. PfSense, Smoothwall Express, Smoothwall Advanced [viitattu 9.9.2013]. Saatavissa: http://www.techradar.com/news/software/applications/7-of-the-best-linux-firewalls-697177/2#articleContent

OAMK. 2013. Kaapelityypit [viitattu 17.7.2013]. Saatavissa: http://www.ratol.fi/opensource/lahiverkot/fin/kaapelointi/kaapelityypit.htm

Skills Finland ry. 2013. Skills Finland [viitattu 3.7.2013]. Saatavissa: http://www.skillsfinland.fi/

SmoothWall. 2013a. About [viitattu 9.9.2013]. Saatavissa: http://www.smoothwall.org/about/

SmoothWall. 2013b. Feature Comparison Chart [viitattu 9.9.2013]. Saatavissa: http://www.smoothwall.org/about/feature-comparison-chart/

Taitaja2014. 2013. Taitaja2014. [viitattu 3.7.2013]. Saatavissa: http://www.taitaja2014.fi/

Tietosähkö. 2013. Lähiverkkojen rakentaminen [viitattu 15.7.2013]. Saatavissa: http://www.tietosahko.fi/pdf/parikaapelointi.pdf

Wikipedia. 2013a. Carrier sense multiple access with collision avoidance [viitattu 30.8.2013]. Saatavissa: http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance

Wikipedia. 2013b. Coaxial cable [viitattu 17.7.2013]. Saatavissa: https://en.wikipedia.org/wiki/Coaxial_cable

Wikipedia. 2013c. Common Address Redundancy Protocol [viitattu 30.8.2013]. Saatavissa: http://en.wikipedia.org/wiki/Common_Address_Redundancy_Protocol

Wikipedia. 2013d. Network topology [viitattu 10.8.2013]. Saatavissa: http://en.wikipedia.org/wiki/Network_topology

Wikipedia. 2013e. Optical Fiber [viitattu 17.7.2013]. Saatavissa: https://en.wikipedia.org/wiki/Optical_fiber

Wikipedia. 2013f. Parikaapeli [viitattu 17.7.2013]. Saatavissa: http://fi.wikipedia.org/wiki/Parikaapeli

Wikipedia. 2013g. pfSense [viitattu 30.8.2013]. Saatavissa: http://en.wikipedia.org/wiki/PfSense

Wikipedia. 2013h. Twisted Pair [viitattu 17.7.2013]. Saatavissa: https://en.wikipedia.org/wiki/Twisted_pair

Wikipedia. 2013i. Verkkotopologia [viitattu 10.8.2013]. Saatavissa: http://fi.wikipedia.org/wiki/Verkkotopologia

Wikipedia. 2013j. Virtual LAN [viitattu 10.8.2013]. Saatavissa: http://en.wikipedia.org/wiki/Virtual LAN

Wikipedia. 2013k. Yleislähetys [viitattu 10.8.2013]. Saatavissa: http://fi.wikipedia.org/wiki/Yleisl%C3%A4hetys

Wikipedia. 2013l. Zentyal [viitattu 9.9.2013]. Saatavissa: http://en.wikipedia.org/wiki/Zentyal

Zentyal. 2013a. Installation [viitattu 9.9.2013]. Saatavissa: http://doc.zentyal.org/en/installation.html

Zentyal. 2013b. Server [viitattu 9.9.2013]. Saatavissa: http://www.zentyal.org/server/

Zentyal. 2013c. Zentyal, the Linux Small Business Server [viitattu 9.9.2013]. Saatavissa: http://www.zentyal.org/

LIITTEET

TAITAJA01 kytkin

```
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname taitaja01
!
boot-start-marker
boot-end-marker
!
!
username Taitaja2014 privilege 15 secret 4

VGf7JtZBJ7C88bUZBx9PMSYhn4OsolIS4fEY0EPqmaE
no aaa new-model
clock timezone EET 2 0
system mtu routing 1500
!
!
!
!
crypto pki trustpoint TP-self-signed-3026820224
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3026820224
 revocation-check none
 rsakeypair TP-self-signed-3026820224
!
!
crypto pki certificate chain TP-self-signed-3026820224
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101

05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D

43657274
  69666963 6174652D 33303236 38323032 3234301E 170D3933 30333031

30303031
  31305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504

03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33

30323638
  32303232 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030
```

```
81890281
  8100B047 969312EF 4F9815DF 99A3C4A8 07BAB807 331481E6 FDD0C1BE

8181B9AA
  FB40E38C C9877F95 36799765 18AF2B80 48C8B421 5A8F6C1D 398C8B48

405A4AFA
  27EFA0CE 5CD28A26 74991433 3B9CC7CC 94A838E1 74C56101 1F3F407B

C1FBE07F
  C3DB4CA9 44282C11 E8190714 7ECABBA9 6C7284EB BF1E2289
28DCC0DC

2087F1C1
  C16B0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF

301F0603
  551D2304 18301680 149F8200 D67B854C 08A360A1 15ADEC91 448570B4

B5301D06
  03551D0E 04160414 9F8200D6 7B854C08 A360A115 ADEC9144 8570B4B5

300D0609
  2A864886 F70D0101 05050003 818100A8 801D09B4 2765EB63 20A144A4

B3D9E8B8
  D171C79B CA07E533 E4357FB8 F5731CC5 E40A993A 3F03ADA3
14DE6F0C

70D97885
  EED15ABA FE29036A BABA67D9 B5CA1F5D 3F75014D F9BA5918
A1421D0E

F261762E
  497ADFAA E52683B5 3B652280 83455C17 D8689073 851CE905 3C817CA1

39BB20FE
  5E54D008 28E91520 774898F4 74059C
       quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
```

```
!
!
!
!
!
interface GigabitEthernet0/1
 switchport access vlan 11
 switchport mode access
!
interface GigabitEthernet0/2
 switchport access vlan 22
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 33
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 44
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 55
 switchport mode access
!
interface GigabitEthernet0/6
 switchport access vlan 66
 switchport mode access
!
interface GigabitEthernet0/7
 switchport access vlan 77
 switchport mode access
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
 switchport trunk allowed vlan 11,22,33,44,55,66,77
 switchport mode trunk
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
 switchport trunk allowed vlan 11,22,33,44,55,66,77
 switchport mode trunk
```

```
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface Vlan1
 no ip address
!
interface Vlan77
 ip address 10.77.0.11 255.255.0.0
!
ip default-gateway 10.77.0.1
no ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
line con 0
 login local
 transport preferred ssh
 transport output ssh
line vty 0 4
 privilege level 15
 login local
 transport input ssh
 transport output ssh
line vty 5 15
 privilege level 15
 login local
 transport input ssh
```

```
 transport output ssh
!
ntp server 10.77.0.1 prefer
end

taitaja01(config-if)#
```

TAITAJA02 kytkin

```
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname taitaja02
!
boot-start-marker
boot-end-marker
!
!
username Taitaja2014 privilege 15 secret 4
VGf7JtZBJ7C88bUZBx9PMSYhn4OsolIS4fEY0EPqmaE
no aaa new-model
clock timezone EET 2 0
system mtu routing 1500
!
!
!
!
crypto pki trustpoint TP-self-signed-3026892416
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3026892416
 revocation-check none
 rsakeypair TP-self-signed-3026892416
!
!
crypto pki certificate chain TP-self-signed-3026892416
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 33303236 38393234 3136301E 170D3933 30333031
30303031
  31305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33
30323638
  39323431 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100E938 716575A2 FCEA2D6D 4326BC07 C5BD2D89 0982F47A
7F9BA29C 18C88FBD
  E1B799C9 F021BBF8 83F277D6 FE6ECD58 56CC08CA E9E5924A
7F25656F 9740C5E6
```

```
  31ACD7FB E1142261 4EE5353F A8EB6A54 758DC1E0 41821FCA
9A462350 9EAB2A47
  1A498AA8 515E0404 96CF6362 DBC01057 F9A735EC 7819CC6B F578C50E
0545502F
  30770203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 14410457 A527F47B 6AA22B94 6B773117 908F18AF
4E301D06
  03551D0E 04160414 410457A5 27F47B6A A22B946B 77311790 8F18AF4E
300D0609
  2A864886 F70D0101 05050003 81810095 B37B4505 0E543FB8 F4F2E6E0
8CD57BCD
  C5F2195C 376492C3 2B618491 49E797CB D6ABDF53 307AED0A
98F6FB66 E9216D02
  D1116FD4 8767A83B 8117B50A 483F0162 3B746839 6C6900B6 B4C97EB7
EFA932EA
  4600B585 4F71DD26 DCE9156F 429A24FE 993ACA39 89DAE175
58A05AC2 185D02C2
  7F0CC743 84F37C0C 3792A154 98E27E
      quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface GigabitEthernet0/1
 switchport access vlan 11
 switchport mode access
!
interface GigabitEthernet0/2
 switchport access vlan 22
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 33
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 44
```

```
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 55
 switchport mode access
!
interface GigabitEthernet0/6
 switchport access vlan 66
 switchport mode access
!
interface GigabitEthernet0/7
 switchport access vlan 77
 switchport mode access
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
```

```
interface Vlan1
 no ip address
!
interface Vlan77
 ip address 10.77.0.12 255.255.0.0
!
ip default-gateway 10.77.0.1
no ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
line con 0
 login local
line vty 0 4
 privilege level 15
 login local
 transport input ssh
 transport output ssh
line vty 5 15
 privilege level 15
 login local
 transport input ssh
 transport output ssh
!
end

taitaja02(config-if)#
```

Palomuurisääntö - liityntä WAN

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 11HALLINTO

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*	*	Hallinto Address	443, 80	*
X	Pass	*	*carp11*	*	*carp11*	*	*
X	Pass	*	Hallinto	*	10.11.0.1	UDP	53
X	Block	*	Hallinto	*	Hallinto	*	*
X	Pass	*	Hallinto	*	Toimitsija	*	*
X	Block	*	Hallinto	*	Toimitsija	*	*
X	Pass	*	Hallinto	*	Kilpailija	*	*
X	Block	*	Hallinto	*	Kilpailija	*	*
X	Pass	*	Hallinto	*	Tulostin	*	*
X	Block	*	Hallinto	*	Tulostin	*	*
X	Block	*	Hallinto	*	Yleisö	*	*
X	Pass	*	Hallinto	*	WLAN	*	*
X	Block	*	Hallinto	*	WLAN	*	*
X	Pass	*	Hallinto	*	Aktiivilaite	*	*
X	Block	*	Hallinto	*	Aktiivilaite	*	*
X	Pass	*	Hallinto	*	*	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä CARPSYNC

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	Carpsync	*	Carpsync	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 22TOIMITSIJA

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*carp22*	*	*carp22*	*	*
X	Block	*	Toimitsija	*	Hallinto	*	*
X	Pass	*	Toimitsija	*	10.22.0.1	UDP	53
X	Block	*	Toimitsija	*	Toimitsija	*	*
X	Block	*	Toimitsija	*	Kilpailija	*	*
X	Pass	*	Toimitsija	*	Tulostin	*	*
X	Block	*	Toimitsija	*	Tulostin	*	*
X	Block	*	Toimitsija	*	Yleisö	*	*
X	Block	*	Toimitsija	*	WLAN	*	*
X	Block	*	Toimitsija	*	Aktiivilaite	*	*
X	Pass	*	Toimitsija	*	*	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 33KILPAILIJA

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*carp33*	*	*carp33*	*	*
X	Block	*	Kilpailija	*	Hallinto	*	*
X	Block	*	Kilpailija	*	Toimitsija	*	*
X	Pass	*	Kilpailija	*	10.33.0.1	UDP	53
X	Block	*	Kilpailija	*	Kilpailija	*	*
X	Pass	*	Kilpailija	*	Tulostin	*	*
X	Block	*	Kilpailija	*	Tulostin	*	*
X	Block	*	Kilpailija	*	Yleisö	*	*
X	Block	*	Kilpailija	*	WLAN	*	*
X	Block	*	Kilpailija	*	Aktiivilaite	*	*
X	Pass	*	Kilpailija	*	*	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 44TULOSTIN

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*carp44*	*	*carp44*	*	*
X	Block	*	Tulostin	*	Hallinto	*	*
X	Block	*	Tulostin	*	Toimitsija	*	*
X	Block	*	Tulostin	*	Kilpailija	*	*
X	Block	*	Tulostin	*	Tulostin	*	*
X	Block	*	Tulostin	*	Yleisö	*	*
X	Block	*	Tulostin	*	WLAN	*	*
X	Block	*	Tulostin	*	Aktiivilaite	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 55YLEISO

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*carp55*	*	*carp55*	*	*
X	Block	*	Yleisö	*	Hallinto	*	*
X	Block	*	Yleisö	*	Toimitsija	*	*
X	Block	*	Yleisö	*	Kilpailija	*	*
X	Block	*	Yleisö	*	Tulostin	*	*
X	Pass	*	Yleisö	*	10.55.0.1	UDP	53
X	Block	*	Yleisö	*	Yleisö	*	*
X	Block	*	Yleisö	*	WLAN	*	*
X	Block	*	Yleisö	*	Aktiivilaite	*	*
X	Pass	*	Yleisö	*	*	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 66WLAN

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*carp66*	*	*carp66*	*	*
	Pass	*	*WLAN*	*	*Hallinto*	*	*
X	Block	*	WLAN	*	Hallinto	*	*
X	Block	*	WLAN	*	Toimitsija	*	*
X	Block	*	WLAN	*	Kilpailija	*	*
X	Block	*	WLAN	*	Tulostin	*	*
X	Block	*	WLAN	*	Yleisö	*	*
X	Block	*	WLAN	*	WLAN	*	*
X	Block	*	WLAN	*	Aktiivilaite	*	*
X	Block	*	*	*	*	*	*

Palomuurisääntö - liityntä 77AKTIIVILAITE

Enable	Pass/Block/ Reject	Proto	Source	Port	Destination	Port	Gateway
X	Pass	*	*carp77*	*	*carp77*	*	*
X	Block	*	Aktiivilaite	*	Hallinto	*	*
X	Block	*	Aktiivilaite	*	Toimitsija	*	*
X	Block	*	Aktiivilaite	*	Kilpailija	*	*
X	Block	*	Aktiivilaite	*	Tulostin	*	*
X	Block	*	Aktiivilaite	*	Yleisö	*	*
X	Block	*	Aktiivilaite	*	WLAN	*	*
X	Block	*	Aktiivilaite	*	Aktiivilaite	*	*
X	Block	*	*	*	*	*	*