Ville Aakko

Verkkolaitteiden päivitys Philips Oy:lle

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan Koulutusohjelma
Insinöörityö
23.4.2013

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Ville Aakko Verkkolaitteiden päivitys Philips Oy:lle 51 sivua + 8 liitettä 23.4.2013
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Yliopettaja Janne Salonen IS-Support Manager Jere Mäkelä

Tämän opinnäytetyön tavoitteena oli päivittää asiakasyrityksen verkon laitteita sekä suunnitella uusi verkkotopologia, jossa käytetään virtuaalisia lähiverkkoja tietomyrskyjen minimoimiseksi. IP-osoitteiden jakaminen järkeistettäisiin samalla käyttäen virtuaalisia lähiverkkoja. Asiakasyrityksenä oli Philips Oy, jonka yhden toimipisteen verkolle piti tehdä edellä mainitut päivitykset.

Verkkoon suunniteltiin yhteensä kuusi erilaista tapaa jakaa IP-osoiteavaruus. Viisi suunnitelmaa oli tarkoitettu nykyisen verkon päivitysvaihtoehdoiksi ja yksi tulevaisuutta varten. Tässä työssä näistä viidestä suunnitelmasta käsitellään kolmea, sillä kahden muun vaihtoehdon eroavaisuudet muihin olivat hyvin pieniä. Tämän lisäksi suunniteltiin myös kaksi erilaista verkkotopologiaa, joista toinen oli tarkoitettu olemassa olevan verkon korvaajaksi ja toinen tulevaisuutta varten. Myös verkkolaitteissa olevia erilaisia mielenkiintoisimpia komentoja käytiin läpi, sekä joitain verkkotekniikoita, joita tarvitaan nykyaikaisen verkon pystyttämiseksi ja ylläpitämiseksi.

Käytännön työ jäi kesken johtuen yhtiön sisäisestä hyväksyntäprosessista. Philipsin toimipiste voi kuitenkin käyttää suunnitelmia tulevaisuudessa joko suoraan, tai sitten pohjana omalle versiolleen.

Avainsanat	Cisco, VLAN, FlexStack, StackWise, EtherChannel

Metropolia

Abstract

Author Title Number of Pages Date	Ville Aakko Upgrading network devices for Philips Oy. 51 pages + 8 appendices 23 April 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data networks
Instructors	Janne Salonen, Principal Lecturer Jere Mäkelä, IS-Support Manager

The purpose of this thesis was to upgrade the network devices of a client company, design a new network topology and virtual local area networks to minimize broadcast storms. One aim was to improve the distributing of IP-addresses by using virtual local area networks. This study was carried out for one of the branch offices of Philips Oy.

Altogether there were six different designs for dividing IP address space. Five of those were meant be possible designs to updating the current design and one was for future use. Out of the five designs this thesis covers three, because the differences of the other two were minimal compared to the other designs. There were also designs for network topology, from which one was to replacing the current topology and the other one was for future use. In addition, some of the more interesting commands in the network devices were explored as were some of the network technologies which are needed to build maintain modern day networks.

The practical part of the thesis was not completed due to internal approval process of the company. The branch office of Philips is still able to use the designs in the future as is, or modify them accordingly if needed.

Keywords	Cisco, VLAN, FlexStack, StackWise, EtherChannel

Sisällys

Lyhenteet

Mbps	megabittiä sekunnissa, tiedonsiirtonopeuden mittayksikkö tietoverkoissa.
Gbps	gigabittiä sekunnissa, tiedonsiirtonopeuden mittayksikkö tietoverkoissa. Noin tuhatkertainen Mbps:iin verrattuna.
MBps	megatavua sekunnissa, Mt/s, tiedonsiirtonopeuden mittayksikkö tietoverkoissa.
LAN	Local Area Network, tiedonsiirtotapa informaation siirtoon verkkolaitteiden välillä.
WLAN	Wireless LAN, langaton LAN, kts. LAN.
VLAN	Virtual LAN, tekniikka jolla verkkolaitteissa voidaan jakaa verkko eri segmentteihin (alueisiin).
SNMP	Simple Network Management Protocol, verkkolaitteiden hallintaprotokolla.
MAC	Media Access Control, jokaisen verkkosovittimen identifioiva yksilöllinen ja fyysinen osoite.
EUI	Extended Unified Identifier, IEEE:n antama MAC-osoitteen virallinen nimitys.
OUI	Organizationally Unique Identifier, IEEE:n myymä 24-bittinen tunniste ostavalle yritykselle
IP-osoite	Internet Protocol-osoite, jokaiselle verkkolaitteelle annettava yksilöllinen ”virtuaalinen” osoite Internetin ja / tai suljetun sisäverkon käyttöä varten.
DHCP	Dynamic Host Configuration Protocol, protokolla IP-osoitteen automaattiseksi jakamiseksi verkon asiakaskoneiden verkkolaitteille.
IEEE	Institute for Electrical and Electronics Engineers, maailmanlaajuinen teknologioiden kehitystä, standardeja ja leviämistä edistävä järjestö.

IETF	Internet Engineering Task Force, organisaatio jonka tarkoituksena on kehittää sekä standardoida Internet-protokollia.
LACP	Link Aggregation Control Protocol, avoin tekniikka (protokolla) jolla voidaan monta fyysistä verkkoliitäntää yhdistää yhdeksi virtuaaliseksi verkkoliitännäksi.
PAgP	Port Aggregation Protocol, Ciscon omistama ja ylläpitämä suljettu versio LACP-standardista.
LEAP	Lightweight Extensible Authentication Protocol, Ciscon kehittämä ja patentoima WLAN:n autentikointimetodi.
RADIUS	Remote Authentication Dial In User Service, verkkoprotokolla jonka avulla voidaan hoitaa keskitetysti käyttäjän tunnistaminen ja oikeuksien myöntäminen verkon käyttöön.
SSID	Service Set Identification, käyttäjille näkyvä langattoman verkon nimi.
WPA	Wi-Fi Protected Access, langattoman verkon tunnistautumisprotokolla.
STP	Spanning Tree Protocol, verkkoprotokolla jolla estetään että, tietopaketit eivät jää kiertämään verkkoon.
PSK	Pre-Shared Key, termi tavalle jolla verkkoa käyttävälle laitteelle jaetaan verkon salasana.
MRI	Magnetic Resonance Imaging. Kuvantamistekniikka ihmisruumiin läpikuvaamiseksi.
MR-HIFU	Magnetic Resonance-High Intensity Focused Ultrasound. Philipsin kehittämä tekniikka jolla voidaan poistaa kasvaimia ilman leikkausta.
MR-Linac	Magnetic Resonance-Linear Accelerator. Philipsin ja Elektan kehittämä tekniikka jolla pyritään yhdistämään MRI sekä sädehoito.

1 Johdanto

Opinnäytetyön aiheen löytäminen aiheutti ongelmia, sillä valinnanvaraa aiheissa oli paljonkin, enkä toisaalta halunnut tehdä työtä koululle. Aiheena tälle työlle oli asiakasyrityksen olemassa olevan verkon päivittäminen. Tähän kuului verkkotopologian uudelleensuunnittelu, IP-osoiteavaruuden suunnitteleminen uudestaan sekä laitteiston vaihto-/asennustyöt. Vaikka pääasiallinen työni asiakasyrityksessä olikin lähituen työ, oli koulusta saatu verkkopuolen koulutus herättänyt kiinnostusta lähiverkkojen (LANien) ja langattomien lähiverkkojen (WLANien) toimintaan, suunnitteluun ja toteuttamiseen. Valitsin tämän työn, koska asiakasyrityksen yhdessä toimipisteessä oli ajankohtaisena asiana verkon laitteiston, sekä verkkolaitteiden konfiguraation päivittäminen uudempaan ja koska omat verkkolaiteopinnot olivat samaan aikaan menossa. Nämä olivat määrääviä asioita tämän opinnäytetyön aiheen valitsemiseksi.

Tässä opinnäytetyössä on kaksi osaa. Ensimmäisessä osassa käyn läpi vanhaa verkkoa, sen laitteita ja topologiaa. Sitten on uuden suunnitellun verkon topologiaa, uusia laitteita sekä viimeisimpänä mahdollinen topologia joka tulisi nyt suunnitellun jälkeen. Toisessa osassa käyn sitten läpi eri verkkoteknologioita sekä sitä, että mihin niitä käytetään ja miten.

Asiakasyritys

Asiakasyrityksenä oli Philips Oy, joka toimii niin sairaalalaitepuolella, viihde- ja päivittäiselektroniikan kuin kuluttaja- ja ammattivalaistuksen markkinoilla. Philips on perustettu vuonna 1891 Anton ja Gerard Philipsin toimesta. [1.] Philipsin tuotevalikoimaan kuuluvat erinäiset äänen ja kuvan toistoon tarkoitetut laitteet, kauneus- ja terveystuotteet, kodinhoitotuotteet, valaisimet sekä erilaiset lisälaitteet ja tarvikkeet. [2.]

Äänen ja kuvan osioon kuuluvat esimerkiksi televisiot, Blu-Ray- ja DVD-soittimet, kuulokkeet sekä erilaiset äänentoiston tuotteet. Kauneus- ja terveystuotteet sisältävät esi-

merkiksi parranajokoneet, sähköhammasharjat sekä hiustenhoitolaitteet. Äitiys- ja lastenhoitotarvikkeiksi lasketaan tutit, pulloruokintavälineet, rintapumput yms. Kodinhoitotuotteita ovat kahvinkeittimet, vedenkeittimet, ruoanlaittovälineet, imurit jne. Valaistuksessa sekä valaisimet että lamput kuuluvat sekä kuluttaja- että ammattivalaistuspuolelle, mutta ammattivalaistuksen puolelle kuuluvat myös erilaiset valaistusratkaisut, joilla saadaan vaikkapa seinään tehtyä erilaisia kuvioita siihen tarkoitukseen suunnitellulla valoseinällä. PC-tuotteet ja puhelimet sisältävät nimensä mukaisesti PC:n näytöt, kaiuttimet, langattomat kotipuhelimet jne. Lisätarvikkeet ovat puolestaan esimerkiksi erilaisia kaapeleita ja liittimiä, sähköhammasharjojen päitä jne. [2.] Myös sairaaloiden magneettikuvauslaitteet (MRI) kuuluvat Philipsin valikoimiin, ja erityisesti siihen toimipisteeseen Suomessa, jossa olin tätä opinnäytetyötä tekemässä. Kyseinen toimipiste on tuotekehitysyksikkö, ja siellä kehitetään ja rakennetaan fokusoituun ultraääneen perustuvien hoitolaitteiden (MR-HIFU) prototyyppejä. Uutena lisänä on tullut sädehoidon tuotealue (MR-Linac), jossa pyritään yhdistämään magneettikuvaus sädehoitoon.

2 Verkkoteknologioita

Tässä luvussa käsittelen niitä verkkoteknologioita, joita tässä opinnäytetyössä on käytetty, sekä yleisellä tasolla joitain niistä tekniikoista, jotka olennaisesti liittyvät IP-verkkoihin. Teknologioita ja protokollia on käytössä tällä hetkellä todella monta. Aikojen saatossa niitä on ollut vähintäänkin saman verran.

2.1 MAC-osoite

MAC-osoite on IEEE 802 -standardin osa. Käyn MAC-osoitteesta läpi lähinnä miten se muodostuu, kuinka pitkä se on ja miten sitä voidaan hyödyntää. MAC-osoite on jollekin verkkoa tiedonsiirtoon käyttävälle laitteelle, kuten matkapuhelimelle, verkkotulostimelle, tietokoneen langalliselle ja/tai langattomalle sovittimelle luotu yksilöllinen, ns. ”fyysinen” osoite. Tämän osoitteen avulla esimerkiksi voidaan DHCP-palvelimelta jakaa IP-osoitteet tietylle laitteelle, tai kytkimissä ja reitittimessä sallia tai estää tiedon kulkeminen. MAC-osoite voidaan nykyisissä laitteissa kuitenkin vaihtaa, ja sitä käytetäänkin paljon esimerkiksi verkkouhkien testaamisessa. Tälle menetelmälle on termi ”MAC spoofing”. [3.]

EUI-48

EUI-48 tarkoittaa MAC-osoitteen 48-bittistä versiota. Sen pituus ilmaistaan kuutena kahden merkin ryhmänä, jotka on eroteltu joko viivalla tai kaksoispisteellä. Eli pituus on yhteensä kaksitoista merkkiä. MAC-osoite ilmoitetaan ns. heksadesimaaleina, eli numeroiden ja kirjainten yhdistelmänä. Numeroista käytössä ovat 0 – 9 ja kirjaimista A – F, eli esimerkiksi 01-23-45-67-89-ab. EUI-48-muotoista merkintätapaa käytetään, kun puhutaan IPv4-verkoissa toimivista MAC-osoitteista. EUI-64 on taas IPv6-verkossa käytettävistä osoitteista. Koska EUI-48 on 48-bittinen, tarkoittaa se, että IPv4-verkkojen MAC-osoitteita voi olla 2^{48} eli 281,474,976,710,656 kappaletta. Näiden osoitteiden ei odoteta loppuvan ennen vuotta 2100. EUI-48 koostuu 24-bittisestä OUI:sta sekä 24-bittisestä yrityksen itse laitteelleen antamasta tunnuksesta. [3.] OUI on lyhenne sanois-

ta Organizationally Unique Identifier, ja yritys voi ostaa sen IEEE:lta. OUI on tunniste, jolla tunnistetaan verkkolaitteen valmistaja. [4.]

EUI-64

EUI-64 on IEEE:n käyttämä nimitys 64 bittisille MAC-osoitteille. EUI-64 muodostuu 24-bittisestä OUI:sta sekä 40 bittisestä yrityksen itse laitteelleen antamasta tunnuksesta. Heksadesimaalimuodossa se on pituudeltaan 16 merkkiä, ja osoite jaotellaan kahdeksaan kahden heksadesimaalin ryhmiin, ja erottimena välissä on EUI-48:n tapaan joko viiva tai kaksoispiste. Eli esimerkiksi 12:34:56:78:90:ab:cd:ef. Samoin kuin EUI-48, myös tämä ostetaan IEEE:lta. EUI-64:stä on olemassa muokattu versio (nk. Modified EUI-64), jota käytetään IPv6-verkoissa. [4.]

2.2 IP-osoite

IP-osoite on verkkoa käyttävälle laitteelle annettu yksilöllinen osoite. Tämä osoite voidaan joko manuaalisesti määrittää käytettävässä käyttöjärjestelmässä, tai sitten jakaa se automaattisesti DHCP-palvelimen avulla. Näitä osoitteita voidaan jakaa kahdella tapaa DHCP-palvelimessa; joko niin että luodussa osoiteavaruudessa annetaan osoitteet järjestyksessä pyytäville laitteille tai sitten MAC-osoitteen perusteella määrittää jokin tietty IP-osoite laitteelle. IP-osoitteita on nykyään käytössä kahdenlaisia: vanhempia IPv4-osoitteita sekä uudempia IPv6-osoitteita. Vaikka IP-osoite onkin teoriassa yksilöllinen, voi laitteen IP-osoite vaihtua jostain syystä. Syy voi olla esimerkiksi että verkkolaite on ollut pois päältä tai ulkona verkosta DHCP-palvelimen määrittämään lainaajan (lease time) aikana, jolloin alun perin jollekin laitteelle annettu osoite onkin sitten annettu toiselle. Tämä tosin ei päde, mikäli käytetään MAC-osoitteeseen sidottuja IP-osoitteita.

2.2.1 IPv4-osoite

IPv4-osoitteisto on neljäs versio IP-verkoista ja tällä hetkellä yleisempi kuin IPv6-osoitteisto, ja se onkin pitänyt valtapaikkaa näihin päiviin asti. Tällä hetkellä maailmassa on niin paljon erilaisia laitteita jotka käyttävät Internetiä ja siten IP-osoitteita, että IPv4-osoitteet ovat päässeet loppumaan. Tämän osoitteiden loppumisen takia on kehitetty erilaisia keinoja, joiden avulla IPv4-osoitteiden käyttöikää on pystytty jatkamaan.

IPv4-osoite muodostuu 32-bittisestä osoitteesta ja se jaetaan neljään 8 bitin kokoiseen palaseen, oktettiin. Tämä mahdollistaa, että jokainen neljästä tavusta saa numeraaliset arvot väliltä 0 ja 255. Eli mahdollisia lukuarvoja voi yhteensä olla 256 kappaletta yhtä oktettia kohden. Tämä taasen tarkoittaa sitä, että IPv4-osoitteita on maailmassa käytettävissä 2^{32}, eli yhteensä 4 294 967 296 kappaletta kokonaisuudessaan. [5.]

Otetaanpa esimerkki IPv4-osoitteesta. Se voisi olla vaikkapa 128.64.32.1. Tämän osoitteen 32-bittinen esitystapa on pelkästään numeroista yksi ja nolla muodostuva lukujono. Tarkoittaa siis sitä, että kun IP-osoite muutetaan bittien esitystapaan, on siinä yhteensä 32 numeroa, jotka ovat ykkösiä ja/tai nollia. Edellä mainittu IP-osoite näyttäisi bittimuodossaan tältä: 10000000010000000010000000000001. Kun tämä lukujono jaotellaan neljään kahdeksan bitin kokonaisuuteen, eli tavuun, näyttäisi se tältä: 10000000.01000000.00100000.00000001. Otetaanpa ensimmäinen oktetti (kahdeksan bitin jono); bitteinä se on 10000000. Vastaava numeraalinen arvo kymmenjärjestelmässä on 128. Vasemmalta lukien ensimmäinen ykkösbitti vastaa puolta (128 kpl) koko tavun mahdollisten vaihtoehtojen määrästä, joita siis on 256 kpl. Seuraava ykkösbitti on puolet jäljellä olevasta 128 mahdollisuudesta, eli 64. Otetaan taas seuraava ykkösbitti, joka on jälleen puolet edellisestä, eli 32. Eli seuraavan ykkösbitin numeroarvo on aina puolet edellisen ykkösbitin numeroarvosta. Tämän seurauksen seuraavan ykkösbitin numeroarvo on 16, sitten tulee 8, 4, 2 ja viimeisenä on vain 1. Nyt koko oktetti on pelkästään numerosta yksi koostuva, eli 11111111. Kun jokainen oktetin biteistä on arvoltaan yksi, lasketaan niitä vastaavat numeroarvot yhteen, ja saadaan 255. Esimerkkinä bittisarja 11101111 vastaa numeroarvoa 239 (128 + 64 + 32 + 0 + 8 + 4 +2 +1). Eli kun bitti on yksi, se lasketaan mukaan oktettiin, jos bitti on nolla, sitä ei lasketa mukaan.

Teoriassa minkä tahansa IP-osoitteen väliltä 0.0.0.1 – 255.255.255.254 voi määrittää verkkolaitteelle, ja sisäverkossa tämä pitääkin paikkansa muutamin pienin poikkeuksin, mutta julkisen Internetin osalta tässä on suurempia rajoituksia. Erinäiset IP-osoitteet ovat varattuja yksityiseen sisäverkkokäyttöön, jolloin Internet-liikennettä ei voi kyseisiin osoitteisiin reitittää (ohjata) suoraan. Kuitenkin näiden osoitteiden takana on koneita joille pitäisi saada siirrettyä tietoa. Tähän ongelmaan käytetään osoitteenmuunnosta. Sitten on muita verkko-osoitteita jotka ovat varattuja esimerkiksi IETF:n käyttöön. [6.]

Taulukko 1. Joitain varattuja IP-osoitteita joita ei käytetä julkisessa verkossa. [6.]

IP-osoitealue	Osoitteita	Reititys Internetistä	Tarkoitus
172.16.0.0 – 172.31.255.255	1048576	Ei	Sisäverkon IP-osoitealue.
169.254.0.0 – 169.254.255.255	65536	Ei	Verkkolaitteen automaattinen osoite.
127.0.0.0 – 127.255.255.255	16777216	Ei	Takaisinkytkentäosoitteet verkkolaitteelle.

Taulukko 1 kuvaa kolmea eri verkkoaluetta, joista kahta ei kannata käyttää kotiverkossa. Ensimmäisen rivin osoiteavaruutta voidaan käyttää kotiverkossa tai yrityksen sisäisessä verkossa, eikä siihen voida suoraan reitittää tietoliikennettä Internetistä. Siihen pitää käyttää NAT-tekniikkaa. Toisen rivin osoitteisto on käytössä silloin, kun asiakaslaite ei saa IPv4-osoitetta DHCP-palvelimelta tai kun sitä ei ole manuaalisesti verkkosovittimelle määritetty. Kolmas osoitteisto on sitten takaisinkytkentäosoiteavaruus (loopback address space). Tällä määritetään, että kun esimerkiksi selaimen osoiteriville laitetaan 127.0.0.1, päästään paikallisella koneella olevaan, vaikkapa sitten verkkosivua pyörittävään palvelimeen. Näin päästään nettisivulle ilman, että liikenteen pitää kulkea lähiverkon tai Internetin kautta.

IPv4-osoitteen muodostumisen ymmärtäminen on hyvin tärkeää vielä pitkän aikaa, vaikka IPv6-osoitteisto onkin valtaamassa tilaa IPv4-osoitteistolta. Tämä johtuu siitä, että IPv4-osoitteita käyttäviä laitteita ja ohjelmistoja, jotka eivät ymmärrä IPv6-osoitteita, on hyvin paljon vielä niin kotona, operaattoreilla, kuin teollisuudessakin käytössä. Myös yritysten verkot käyttävät hyvinkin usein IPv4:n sisäverkkoihin varattuja osoitteita, jolloin yrityksillä ei ole kiirettä siirtyä IPv6:n käyttöön. IPv6-verkkoon ollaan kuitenkin siirtymässä, ja ennen pitkää koko IPv4-verkko jää pois käytöstä. Tälläkin het-

kellä markkinoilla on laitteita, jotka tukevat joko eivät ollenkaan, osittain tai täysin IPv6-osoitteistoa. Kestää vielä jonkin aikaa, ennen kuin kaikki valmistajat saavat kaikkiin laitteisiinsa edes osittaisen tuen.

2.2.2 Aliverkon peite IPv4-verkossa

Aliverkon peite (englanniksi subnet mask) on olennainen osa IP-verkkoja ja niiden konfigurointia. Aliverkon peitteen avulla ilmaistaan missä kohtaa IP-osoitteen binaarisessa muodossa olevan IP-osoitteen verkko-osa loppuu ja mistä alkavat sitten laitteen osoitteet. Aliverkon peite on IPv4-osoitteen tavalla 32-bittinen, eli siinäkin on neljä kahdeksan bitin osaa, eli oktettia. Tästä syystä aliverkon peitteen numeraalisten arvojen laskeminen tehdään samalla tavalla kuin IPv4-osoitteessakin. Se, miten aliverkon peite ja IP-osoite eroavat toisistaan, on siinä, että kun aliverkon peitteen bitin arvo on yksi, merkitsee se, että kyseessä on verkko-osa. Kun se on nolla, on kyseessä laiteosa. Aliverkon peite voidaan ilmaista joko numeraalisena arvona, esimerkiksi 255.255.192.0 tai sitten käytettyjen ykkösbittien määrällä, ja sitä edeltävällä merkinnällä. Esimerkkinä vaikkapa IP-osoite 192.168.0.1/24. Tämä /24 – merkintä merkitsee, että aliverkon peitteeseen on käytetty 24 ykkösbittiä mahdollisesta 32:sta. Numeraalisena arvona /24 olisi 255.255.255.0. [7.] Otetaanpa esimerkki, niin näemme, miten tämä toimii:

Taulukko 2. Verkko-osan ja laiteosan määrittäminen [8.]

	Binaarinen esitystapa	Numeraaliset arvot	
IP-osoite	**10101100.00010000.0000**1111.00110010	172.16.15.50	
Aliverkon peite	**11111111.11111111.1111**0000.00000000	255.255.240.0	
Verkko-osa	**10101100.00010000.0000**0000.00000000	172.16.0.0	
Laiteosa	**00000000.00000000.0000**1111.00110010	0.0.15.50	

Vahvistetulla tekstillä oleva näyttää verkko-osan ja vahvistamaton teksti laiteosan. Havainnointisyistä vahvistin myös IP-osoitteen ja aliverkon peitteen verkko-osaa vastaavasta kohdasta. Kuten nähdään, aliverkon pituus määrittää, missä kohdassa verkko-

osa päättyy ja laiteosa alkaa. Aliverkon peite on aina ykkösbiteistä koostuva, ei koskaan nollabitistä. Verkko-osa ja laiteosa eivät voi myöskään olla koskaan ”päällekkäin”, eli esimerkiksi kolmannen oktetin viides bitti ei voi olla sekä aliverkon peitteessä ykkönen että laiteosassa ykkönen, vaan se on oltava nolla jommassakummassa tai molemmissa. Edellä oleva sääntö voidaan todeta seuraavalla tavalla Wikipedian mukaan:

> Verkko-osan laskeminen tapahtuu binäärisenä JA-operaationa IP-osoitteesta ja aliverkon peitteestä. Laiteosan laskeminen puolestaan tapahtuu binäärisen XOR-operaation avulla verkko-osasta ja IP-osoitteesta. [8.]

Lainaus tarkoittaa sitä, että jos sekä IP-osoitteen eräs bitti ja aliverkon peitteen vastaava bitti ovat molemmat yksi, on se verkko-osa. Jos taas molempien, sekä laite- että verkko-osan vastaavat bitit ovat yksi tai nolla, on kyseessä laiteosa. Näin ollen voidaan todeta, että jos verkko-osasta lähtee yksi bitti, se lisätään laiteosaan ja toisin päin. Edellä mainittujen syiden takia aliverkon peite ei koskaan voi olla esimerkiksi 255.192.252.0, vaan se menee niin, että aina otetaan aliverkon peitteen viimeinen ykkösbitti nollaksi, tai ensimmäinen numero nolla viimeisen ykkösen jälkeen ykköseksi. Tämä riippuen siitä mihin suuntaan halutaan verkko-osan ja laiteosan ”rajaa” siirtää, ja sitä myöten verkon tai aliverkon kokoa muuttaa pienemmäksi tai isommaksi.

2.2.3 IPv6-osoite

IPv6-osoite on nimensä mukaisesti Internetin käyttämän IP-protokollan kuudes versio. Tämä versio suunniteltiin kohtaamaan ne ongelmat, joihin IPv4:n käytössä oli törmätty. Pahimpana niistä ongelmista on osoitteiden loppuminen kesken. Koska IPv4-osoitteisto on 32-bittinen, mahdollisia osoitteita on ”vain” päälle neljä miljardia. Koska IPv6 on 128-bittinen, on sillä osoitteita 2^{128} kappaletta, eli $3{,}4*10^{38}$ osoitetta. Tämä varmistaa sen, että osoitteet eivät tule loppumaan kesken meidän elinaikanamme, jos koskaan. Ja koska IPv6 on 128-bittinen, tarkoittaa se sitä, että IP-osoitteen pituus tällä osoitteistolla on 128 merkkiä ykköstä ja/tai nollaa. Mutta, koska IPv6-osoite on niinkin pitkä, ei ole mitään järkeä käyttää kymmenjärjestelmän tapaa muuntaa bittijonot lyhyemmäksi, vaan käytetään heksadesimaaleja. Heksadesimaalit jaotellaan kahdeksaan neljän mer-

kin ryhmään, ja erottimen toimii kaksoispiste. [9.] Eli IPv6-osoite voisi olla vaikkapa 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Mutta koska IPv6-osoitteen saa myös lyhentää tietyin säännöin, voidaan edellä oleva osoite lyhentää muotoon 2001:0db8:85a3:0:0:8a2e:0370:7334. Vielä lyhyempi muoto on mahdollista saavuttaa sillä, että nuo keskellä olevat nollat korvataan tuplakaksoispisteellä (::), jonka jälkeen osoite näyttää tältä: 2001:0db8:85a3::8a2e:0370:7334. Wikipedian [10.] mukaan nollien lyhentämiseen pätevät seuraavat säännöt:

- Yksi tai useampi jatkuva ryhmä voidaan esittää tuplakaksoispisteellä (::).
- Osoitteessa oleva esim. ”0001” voidaan esittää pelkästään muodossa ”1”. Esimerkiksi 2001::8a2e:0001 muuttuu muotoon 2001::8a2e:1.
- Tuplakaksoispisteellä tulisi lyhentää pisin perättäisten nollien jono, mutta ei kuitenkaan yhtä kenttää. Esimerkkinä toimikoon osoite 2001:db8:0000:0000:0000:0000:0002:0001. Tämä osoite voidaan edellä luetelltujen sääntöjen perusteella lyhentää muotoon 2001:db8::2:1. Toisaalta taas osoite 2001:db8:0000:0001:0001:0001:0001:0001 suositellaan lyhennettäväksi muotoon 2001:db8:0:1:1:1:1:1.
- Jos osoitteessa on monta yhtä pitkää toisistaan erillään olevaa nollien sarjaa, pitäisi vasemmanpuoleisin lyhentää. Tästä esimerkkinä osoite 2001:db8:0000:0000:0001:0000:0000:0001 pitäisi muuttaa muotoon 2001:db8**::**1:0:0:1 mieluummin kuin muotoon 2001:db8:0:0:1::1.

Verrattuna IPv4-osoitteisiin tuo IPv6 muitakin muutoksia. Yksi niistä muutoksista on, että verkossa ei enää ole broadcast-osoitteita, vaan sama toiminnallisuus saadaan lähettämällä datapaketti ”link-local *all nodes* multicast” -ryhmälle. [11.] Mitä omista opinnoista jäi mieleen IPv6:n osalta, on se, että osoitteiston uusien ominaisuuksien ymmärtäminen on haastavaa, ja näin jälkikäteen ajateltuna pitäisi koulu(i)ssa panostaa enemmän IPv6:n opettamiseen Se kuitenkin tulee olemaan tulevaisuudessa IPv4:n korvaaja ja yksi Internetin (ja muidenkin verkkojen) tärkeimmistä perustekniikoista.

2.2.4 Aliverkon peite IPv6-verkossa

Aliverkon peitteen tehtävä IPv6-verkoissa on sama kuin IPv4-verkoissa. IPv6-verkoissa aliverkon peitteen pituudeksi kotikäyttäjille IETF suosittelee 64 bittiä. Tämä tarkoittaisi sitä, että bittijonoa katsottaessa, asiakasverkko olisi pituudeltaan puolet IP-osoitteen pituudesta. Se ei suinkaan tarkoita sitä, että kotikäyttäjälle olisi annettu puolet koko IPv6-osoiteavaruudesta. Kun käytetään näinkin pitkää aliverkon peitettä, kotikäyttäjille annettavien osoitteiden määräksi tulisi huimat 2^{64} kappaletta. [12.] Tulevatko operaattorit todellisuudessa jakamaan näin paljon osoitteita vai vähemmän? Mutta joka tapauksessa operaattorit tulevat jakamaan tarpeeksi osoitteita loppukäyttäjien käyttöön.

2.3 NAT

NAT, eli Network Address Translation (osoitteenmuunnos), on tapa jolla IP-osoitteita voidaan piilottaa maailmalta niin, että yrityksen verkko näkyy ulkomaailmaan yhtenä tai muutamana, esimerkiksi alle kymmenenä IP-osoitteena, mutta sisäverkossa voi olla sitten hyvinkin paljon osoitteita, jopa tuhansia. Tälle tekniikalle on monia eri nimiä sekä toteutustapoja, ja monet verkkolaitteita valmistavat yritykset ovatkin luoneet omia versioitaan tästä tekniikasta. Mutta yleisimmät tavat osoitteenmuutokselle ovat seuraavat:

- Porttimuunnos Port Address Translation (PAT), tekniikka jolla yhden julkisen IP-osoitteen takana voi olla tuhansia koneita johtuen siitä, että yhdellä IP-osoitteella on yli 65 000 porttia.
- Staattinen NAT Static NAT, tässä tavassa nettiyhteydellä annetaan vaikkapa 10 julkista IP-osoitetta, jotka sitten reititetään vastaamaan 10 sisäverkon IP-osoitetta. Sisäverkossa on siis vähintään yhtä monta konetta kuin on julkisia IP-osoitteita.
- Dynaaminen Nat Dynamic NAT, dynaamisen NAT:n ero staattiseen on se, että verkossa voi olla enemmänkin kuin se määrä IP-osoitteita, mitä reitittimelle on konfiguroitu. Julkiset osoitteet jaetaan tarpeen mukaan sisäverkon koneille.

- Käänteinen NAT Reverse NAT, tekniikka, joka muistuttaa hyvin paljon porttimuunnosta, mutta yksi julkinen IP-osoite käyttää samaa porttia koko ajan eikä vaihtele sitä yhteyden mukaan. Tätä käytetään esimerkiksi palvelinten kuormanjaossa.

Tämä tekniikka kehitettiin auttamaan IPv4-osoitteiston hupenemisen kanssa. Vääjäämättä kuitenkin koko ajan enemmän ja enemmän Internet-liikenne reitittyy kulkemaan IPv6-verkon kautta. [13.]

2.4 DHCP

DHCP eli Dynamic Host Configuration Protocol on nimitys verkoprotokollalle, jolla verkossa olevalle laitteelle annetaan IP-osoite. Tätä protokollaa voidaan käyttää joko fyysisellä palvelimella tai sitten se voidaan konfiguroida myös suoraan kytkimille tai reitittimelle, mikäli verkossa ei ole olemassa olevaa palvelinta tätä toimenpidettä hoitamaan. DHCP-palvelin ylläpitää listaa jaettavista IP-osoitteista sekä koneista, joille niitä on jaettu. DHCP-palvelimelle konfiguroidaan myös IP-osoitteen laina-aika eli aika, kauanko yksi asiakaslaite voi kerrallaan varata yhtä osoitetta. IP-osoitteen ja laina-ajan lisäksi palvelimelle määritetään oletusyhdyskäytävän (default gateway) osoite, aliverkon peite (subnet mask) sekä nimipalvelimen/-palvelinten osoite/osoitteet. Nämä tiedot auttavat asiakaskonetta pääsemään käyttämään verkon resursseja. DHCP-palvelimella on kolme erilaista jakotapaa IP-osoitteille:

- Dynaaminen jako: Palvelimelle määritetään IP-osoiteavaruus ja sen vaatimat lisäparametrit. Kun puolet laina-ajasta on kulunut umpeen, asiakaslaite ilmoittaa DHCP-palvelimelle, että kyseistä IP-osoitetta halutaan käyttää vielä saman laitteen toimesta. Mikäli vastausta ei kuulu, asiakaslaite odottaa jonkin aikaa ja yrittää ottaa uudelleen yhteyttä palvelimelle, kunnes onnistuu tässä. Tämän jälkeen laina-aikalaskuri käynnistetään alusta. Mikäli asiakaslaite on pois päältä kun laina-aika kuluu umpeen, osoite palautuu takaisin kiertoon ja vapaaksi käytettäväksi seuraavalle asiakkaalle.

- Automaattinen jako: Tämä on muuten sama kuin dynaaminen jako, mutta erona on se, että sama asiakaslaite saa aina saman IP-osoitteen. Tämä hoidetaan si-

ten, että palvelin ylläpitää listaa, jossa ovat tiedot siitä, että mille asiakaslaitteelle on annettu mikäkin osoite.

- Staattinen jako: Tämä tapa toimii siten, että palvelimella on lista asiakaslaitteiden MAC-osoitteista jotka ovat liitettyjä tiettyihin IP-osoitteisiin. Sitten kun kyseinen asiakaslaite liittyy verkkoon, antaa palvelin etukäteen määritetyn IP-osoitteen laitteelle. Vain tässä listauksessa olevat laitteet voivat saada IP-osoitteen palvelimelta. [14.]

2.5 LAN

LAN eli Local Area Network, suomeksi lähiverkko, on termi, jolla tarkoitetaan fyysisillä kaapeleilla yhteen liitettyjä tietokoneita. Tietokoneet voivat olla joko suoraan toisissa koneissa yhteydessä tai sitten kytkimen tai reitittimen välityksellä. Erilaisia LAN-tekniikoita on ollut monia käytössä, mutta ne ovat sittemmin korvautuneet yhdellä tekniikalla. Nykyinen käytössä oleva LAN-tekniikka perustuu Xeroxin vuosina 1973 – 1975 kehittämään Ethernet-tekniikkaan. [15.] Ennen Ethernetiä oli olemassa esimerkiksi Token Ring -tekniikka, ja koska Ethernet oli suhteellisen halpa valmistaa sekä erittäin taipuisa markkinoiden vaatimuksiin, se saavuttikin nopeasti suosiota sekä lopulta vei voiton Token Ringistä sekä muista kilpailijoista. Ensimmäinen Ethernet-tekniikka oli nimeltään StarLAN, ja se oli nopeudeltaan 1 megabitti sekunnissa. [16.] Nykyinen kupariseen kaapelointiin perustuva yleisin Ethernetin nopeus on gigabitti sekunnissa, mutta vuonna 2006 kehitettiin standardi, joka tukee jopa 10 gigabitin sekuntinopeutta. [17.] Ethernet-verkon luomiseksi voidaan myös käyttää optista kaapelointia, eli kupariin lähetettävien sähkösignaalien sijaan lähetetään valosignaaleja silikaatista tai muovista tehtyihin hiukan ihmishiusta paksumpaan kuitujohtimeen. [18.]

Ethernet-käyttöön tarkoitetussa kuparikaapelissa, 10 ja 100 megabitin sekuntinopeudessa, on käytössä kaksi paria toisiinsa kiedottuja eristettyjä kuparijohtimia. Gigabitin verkoissa suositellaan käytettäväksi kaapelia, jossa on neljä kierrettyä paria. [19.] Eristetyt johtimet on siis kiedottu ensin pareittain, ja sen jälkeen parit on kiedottu vielä toisiinsa. Tämän tarkoituksena on vähentää elektromagneettisia häiriöitä, joita kaapelit jo itsessään luovat. Ja kun nämä kiedotaan toisiinsa, niiden aiheuttamat häiriöt kumoavat

toisensa ja kaapeli toimii luotettavammin. [20.] LAN-tekniikka kuuluu IEEE:n 802.3-standardin alaisuuteen. [21.]

2.6 WLAN

Wireless LAN, langaton LAN, on verkkotekniikka, jolla saadaan lähiverkkoa laajennettua toimimaan myös langattomana. Langattoman lähiverkon kantavana ideana on se, että käyttäjä voi olla koko ajan kodin tai yrityksen verkossa kiinni ilman katkoksia tietoliikenteeseen sallien näin liikkuvamman työtavan tai kotona Internetin selaamisen. Tämä on erittäin hyödyllistä etenkin toimistoissa, joissa ei ole omia paikkoja, tai kun työntekijän pitää liikkua eri kokousten välillä. Ensimmäinen langaton lähiverkko kehitettiin Havaijin yliopistossa ja sille tulikin nimeksi ALOHANet. Tämä prototyyppiverkko aloitti toimintansa jo kesäkuussa 1971. [22.] Eli langaton lähiverkko ei ole kovinkaan uusi keksintö, vaikka se on vasta viimeisen kymmenen vuoden aikana vasta levinnyt kunnolla käyttöön. Nykyään langattomia lähiverkkoja käyttäviä laitteita on todella paljon; kannettavat tietokoneet, pelikonsolit, TV:t, matkapuhelimet, erilaiset taulutietokoneet jne.

Koska WLAN käyttää avoimempaa tiedon välitystapaa (siis ilmatietä) kuin LAN, on siinä kulkevat tietopaketit helpompi kaapata tai tietovirtaa vakoilla. Tästä johtuen WLAN:n käyttöön on kehitetty erilaisia salauksia, kuten WEP (Wired Equivalent Privacy) tai WPA (Wi-Fi Protected Accecss). [23.] Salauksien käyttäminen on suositeltavaa etenkin kotioloissa, jos ei halua omaan kotiverkkoonsa ylimääräisiä kävijöitä. Nykyään suositeltava salaus on WPA2 yhdistettynä PSK:hon. Yritysten osalta toimiston langattoman tietoliikenteen salaaminen on itsestäänselvyys. Uusin langattoman standardi on IEEE:n määrittelemä 802.11n, jonka tiedonsiirtonopeus nousee 802.11g-standardin 54 Mbps:n nopeudesta jopa 600 Mbps:n nopeuteen. [24.]

2.7 Virtual Local Area Network

Virtual Local Area Network, eli lyhyesti VLAN, on tekniikka, jolla voidaan olemassa oleva IP-osoiteavaruus pilkkoa pienempiin segmentteihin, jotka voidaan sitten jakaa esimerkiksi käytettävien laitteiden mukaan. Tämä jaottelu erottelee jokaisen VLAN:in omaksi jakelualueekseen, ja tietoliikenne näiden virtuaalisten lähiverkkojen välillä ei kulje ilman, että liikennettä reitittää vähintään yksi kytkin tai reititin. Tällainen verkon suunnittelu helpottaa huomattavasti loogisen verkkotopologian suunnittelua. Hyvänä esimerkkinä voidaan ottaa vaikkapa myyntimiesten koneet ja heidän palvelimensa. Ne voivat kaikki sijaita eri paikoilla toimistossa, jopa eri kerroksissa ja eri kytkimiin yhdistettyinä, mutta silti kaikilla myyntimiehillä on pääsy omalle palvelimelleen, koska se on samassa VLAN:ssa. Eli VLAN ei sido konetta tai käyttäjää mihinkään yksittäiseen kytkimeen tai porttiin, sillä kytkimien portit ovat vapaasti liitettävissä eri VLAN:iin tarpeen mukaan.

Virtual LANien konfiguroimiseksi koko verkkoon automaattisesti voidaan käyttää Ciscon protokollaa nimeltä VTP, VLAN Trunking Protocol. Koska kyseessä on Ciscon protokolla, toimii se vain Ciscon laitteissa. VTP toimii siten, että yksi laite toimii VTP serverinä, eli kaikki siihen laitteeseen tehdyt muutokset VLANeihin välitetään kaikille niille laitteille, jotka ovat client-moodissa. Client-moodissa oleva kytkin tai reititin ottaa vastaan VLAN:ien tiedot ja sisällyttää ne omaan konfiguraatioonsa sekä jakaa konfiguraation eteenpäin. Kolmas VLAN-moodi on ”transparent”-moodi. Tässä moodissa oleva laite välittää VLAN-päivitykset eteenpäin, mutta ei itse lisää niitä omiin asetuksiinsa. [25.]

2.8 FlexStack, StackWise ja StackWise+

StackWise ja FlexStack ovat Ciscon kytkimissä ja reitittimissä olevia teknologia, joilla saadaan useampi kytkin tai reititin yhdistettyä yhdeksi isoksi vastaavaksi laitteeksi. Tällä tavalla saadaan porttien sekä laitteiden hallinta yhden IP-osoitteen ja konsolin taakse. FlexStackia käytetään Catalyst 2960-S -sarjan laitteissa, ja sen käyttöön tarvitaan erillinen moduuli sekä kaapeli. FlexStack –kaapelin nopeus on 10 Gbps yhteen

suuntaan, ja koska yhdessä kytkimessä voi olla kaksi FlexStack-kaapelia kiinni, nopeus nousee näin ollen 20 Gbps:n nopeuteen per kytkin. FlexStack rajoittaa nippuun liitettävien kytkimien määrän 4 kappaleeseen. [26.]

Stackwisea käytetään Catalyst 3750 -sarjan nipuissa silloin, kun yksi tai useampi jäsen on Catalyst 3750. Mikäli kaikki jäsenet ovat 3750-E tai 3750-X, voidaan käyttää StackWise+:aa. StackWisen nopeus on yhdellä kaapelilla 16 Gbps per kytkin, ja kun toisen kaapelin kiinnittää, nopeus nousee 32 Gbps:iin per kytkin. StackWise sekä StackWise+ rajoittavat nippuun liitettävien kytkinten määrän 9 kappaleeseen. [27.]

Erot StackWisen ja StackWise+:n välillä ovat pienet, mutta hyvinkin hyödylliset ja tärkeät. Jos tietopaketti on tarkoitettu yhden kytkimen portista toiseen, StackWise+ osaa tehdä sen niin, ettei tietopaketti lähde kytkimestä kiertämään koko nippua. Eli tietopaketti ei pääse StackWise-moduuliin eikä -kaapeleihin asti. Toinen ominaisuus on ns. ”destination stripping”, eli kun datapaketti lähtee kulkemaan nipussa, se menee suoraan oikeaan osoitteeseen eikä jää kiertämään koko nippua läpi. StackWise taasen käyttää ”source strippingiä” eli tietopaketti kiertää koko nipun kerran, ennen kuin se tiputetaan pois kierrosta ja oikeaan kytkimeen. Nämä kaksi StackWise+:n ominaisuutta lisäävät moduulien ja kaapelien tehokkuutta ja kaistansäästöä. Nipun pääkytkimen valinta kaikissa kolmessa nipputekniikassa tapahtuu seuraavan viiden ehdon mukaisessa järjestyksessä: [26; 27.]

1. Kytkin, joka on tämänhetkinen pääkytkin.

2. Kytkin, jolla on suurin prioriteetti (laitteisto- ja/tai ohjelmistoversio).

3. Kytkin, jossa konfiguraatiotiedosto sijaitsee.

4. Kytkin, jolla on korkein päälläoloaika.

5. Kytkin, jolla on pienin MAC-osoite.

Kuvio 1. StackWise-kaapeleiden kytkentäkaavio.

Kuvio 1 näyttää, miten FlexStack, StackWise sekä StackWise+ kytketään neljällä moduulilla toisiinsa tehden nipusta näin vikasietoisen. Mikäli yksi kaapeli katkeaa, moduuli menee rikki tai kytkin hajoaa, nippu toimii edelleen vaikkakaan ei yhtä nopeasti kuin toimivassa järjestelmässä. [26; 27.]

2.9 EtherChannel

EtherChannel on Ciscon omistama arkkitehtuuri, jolla kuvataan, miten monta eri fyysistä linkkiä (kaapelia) voidaan yhdistää yhdeksi virtuaaliseksi kaapeliksi. Tällä tavalla voidaan kasvattaa tiedonsiirtokapasiteettia verkkolaitteiden tietoliikenneporttien määrän kustannuksella, eli toisin sanoen mitä nopeampi EtherChannel-kaapeli, sitä vähemmän on verkkolaitteissa portteja saatavilla. Fyysisiä portteja voi yhteen EtherChanneliin käyttää kahdesta kahdeksaan. Sen lisäksi voidaan luoda niin sanotut ”failover”-portit siltä varalta, että joku EtherChannelissa olevista porteista hajoaa tai verkkojohto katkeaa. Näin luodaan vikasietoisuutta. EtherChannel voidaan luoda 100 Mbps:n, 1 Gbps:n ja 10 Gbps:n porteista, eli teoriassa sen nopeus voi olla 200 Mbbps:sta aina 80 Gbps:iin asti. Jokaisen yhdessä EtherChannelissa olevan portin pitää olla yhtä nopeita, eli ei ole mahdollista sekoittaa esimerkiksi 100 Mbps:n ja1 Gbps:n portteja samaan EtherChanneliin. Perinteisessä EtherChannelissa porttien pitää olla samassa kytkimessä, tai mikäli käytössä on joku nipputekniikka, voivat portit olla myös saman nipun eri kytkimissä. Ciscon kehittämä Multi Chassis EtherChannel antaa mahdollisuuden käyttää myös erillisiä ei-niputettuja kytkimiä yhdessä EtherChannelissa käyttäen Virtual Switching System -tekniikkaa. [28.]

2.10 PAgP

PAgP, Port Aggregation Protocol, on Ciscon kehittämä ja tästä syystä yksityisomisteinen protokolla, jota käytetään EtherChannelin pohjana verkkoliitäntöjen yhdistämiseksi yhdeksi loogiseksi linkiksi. PAgP on kolme eri toimintamoodia:

- Auto: Vaikka tämän tilan nimi on ”auto”, on portti silti passiivisessa tilassa, eli se odottaa asetuksia linkin toisesta päästä. Tästä syystä EtherChannel ei toimi, jos tässä tilassa olevan portin toisessa päässä on joko ”auto”- tai ”on”-tilassa. Tämä tila toimii portin kanssa, joka on ”desirable”-tilassa.

- Desirable Portti on aktiivisessa tilassa, eli lähettää ja vastaanottaa asetuksia toiseen päähän tai toisesta päästä. Toimii sellaisessa tilassa olevan portin kanssa, joka on joko ”auto”- tai ”desirable”-tilassa.

- On Portti on tilassa, jossa se olettaa, että toisella osapuolella on oikeat asetukset eikä mitään protokollaa käytetä. Tästä johtuen ”on”-tilassa oleva portti voi muodostaan EtherChannelin ainoastaan toisen ”on”-tilassa olevan portin kanssa. [29.]

3 Nykyinen verkko

3.1 Tarve

Philipsillä töissä ollessani sain tietää esimieheltäni, että yhdessä toimipisteessä on vanhentuneita verkkolaitteita, jotka olisi pitänyt vaihtaa ja samalla sitten järkeistää IP-osoitteiden jakelua DHCP-palvelimelta, parantaa verkkolaitteiden konfiguraatioita, luoda ja muokata IP-osoitteiden muodostamia segmenttejä ja mahdollisesti laajentaa verkon IP-osoiteavaruutta. Tästä sitten syntyi idea tehdä opinnäytetyö yritykselle.

Jostain syystä myös välikatossa olevien lähiverkko- sekä sähköpistorasioiden paikat näyttävä kartta oli kadonnut, joten näiden kartoittaminen pohjapiirustukseen oli myös tarpeellinen. Tähän osaan meni paljon aikaa, sillä samalla, kun piti kartoittaa nämä paikat, piti myös vaihtaa tukiasema, kun vanha laite tuli vastaan. Ennen laitteen vaihtoa piti ensin ajaa vanhan tukiaseman konfiguraatio uuteen tukiasemaan ja muuttaa hieman joitain asetuksia. Tämän jälkeen piti vaihtaa laite fyysisesti, jonka jälkeen sitten merkitsin listaan, mikä tukiasema vaihdettiin. Tukiasemista vaihdettuina oli jo noin puolet, ja minun piti sitten vaihtaa loput. En saanut tätä vaihetta tässä vaiheessa kokonaan valmiiksi siitä syystä, että yksi uusi tukiasema oli rikki. Tukiasema ei käynnistynyt ollenkaan, oli se sitten kytkettynä virtalähteeseen, PoE-liittimellä varustettuun kytkimeen tai sitten power injectoriin. Alettiin selvittää, miten sen vaihto onnistuu. Tukiaseman vaihto ei koskaan ehtinyt tapahtua tämän työn aikana.

3.2 Olemassa olevat laitteet

Olemassa olevat laitteet ovat pääasiassa vanhoja laitteita. Niitä oli sekä Ciscolta, Hewlett-Packardilta, 3Com:lta että Delliltä. Tämä aiheuttaa ongelmia siinä, että kaikkia Ciscon laitteissa käytettäviä verkkotekniikoita ei voi ottaa käyttöön, koska ne ovat ns. ”proprietary”-tekniikoita, eli ne ovat Ciscon patentoimia sekä Ciscon yksityisomistuksessa. Laitteina oli sekä kytkimiä, reitittimiä ja WLAN-tukiasemia. Tietysti toinen vaihtoehto oli vaihtaa koko verkon laitteet jonkin toisen valmistajan laitteisiin, jotka tukisivat

avoimia standardeja. Mutta päädyin käyttämään Ciscon laitteita siitä syystä, että näiden konfigurointiin koulussa on olemassa kurssit. Toki muidenkin valmistajien laitteille on koulussa kursseja, mutta Ciscon kurssit ovat laajimmat, joten harjoitusta on myös enemmän. Philipsin verkoissa on myös mahdollista käyttää muiden valmistajien laitteita, mutta Cisco on se pääasiallisin valmistaja, jonka laitteita Philipsin verkoissa käytetään. Joissain toimipisteissä on myös käytössä IP-puhelimia, ja ne ovat järjestäen Ciscon puhelimia, joten se asettaa myös verkolle omat vaatimuksensa.

Kuvio 2. Cisco Aironet 1121G

Kuviossa 2 oleva Ciscon Aironet 1121G oli yksi vanhoista langattoman verkon tukiasemista jotka piti vaihtaa. Yksi syy laitteiden vaihtoon oli se, että ne eivät tue uutta ja nopeampaa 802.11n-standardia. Ne tukevat 802.11-standardia 802.11g-standardiin asti, jonka tiedonsiirtonopeus on enintään 54 Mt/s 2,4 GHz:n (gigahertzin) taajuudella. Tällä laitteella on käytössä myös käytössä kolme ei-päällekkäistä kanavaa (non-overlapping channels). Ethernet-portin nopeus on korkeintaan 100 Mbps. Laite tukee tavallisen virtalähteen lisäksi virransyöttöä PoE-kytkimeltä (Power over Ethernet), eli virran saa laitteeseen suoraan kytkimen tietoliikenneportista, jossa tukiasema on kiinni. [30.] Tätä ominaisuutta ei Philipsillä ollut käytössä ollenkaan.

Kaikki Philipsillä olevat Aironet 1121G-malliset tukiasemat ovat ns. ”standalone”-tukiasemia, eli ne eivät tarvitse erillistä keskusohjainta, jotta niitä voidaan konfiguroida, vaan jokainen konfiguroidaan erikseen. Tilanteesta ja verkosta riippuen tämä voi olla

etu tai haitta. Laitteen konfigurointi tapahtuu Ethernet-portin kautta PC:n selaimen avulla, tai sitten terminaaliohjelman kautta käyttäen komentoriviä.

Kuvio 3. 3Com Baseline Switch 2250

Ensimmäiset 2250-mallin kytkimet on julkistettu jo 2004. Eli kytkin on jo aika vanha ja vaihtamisen tarpeessa. Kytkimessä on 48 kappaletta perusporttia, jotka ovat nopeudeltaan korkeintaan 100 Mbps. Lisänä on vielä 2 kappaletta portteja, joihin voi kiinnittää lisäosalla joko 1 Gbps:n kuparikaapelin tai sitten kuitukaapelin. Pelkästään nämä nopeuserot vaikuttavat verkon nopeuteen hidastavasti. Toisaalta, koska nämä portit ovat hitaampia, hiljentää se liikennettä tämän kytkimen ja muun verkon välillä, vähentäen mahdollisuutta verkon tukkeutumiseen. Kytkin tukee sekä VLAN:ja, linkkien yhdistämistä, tietoliikenteen priorisointia sekä automaattista MDI/MDIX-operaatiota. Kytkimen konfiguraation voi hoitaa ainoastaan Internet-selaimen kautta. 3Com onkin kehittänyt sitä varten oman ohjelmansa, Discoveryn, joka etsii laitteen verkosta ja jonka kautta konfigurointi tapahtuu. [31.]

Kuvio 4. HP ProCurve 2510G

Tämä Hewlett-Packardin kytkin toimii nykyisessä verkossa verkon liityntäpisteenä. Tarkoittaa siis sitä, että siitä jaetaan verkkoyhteydet siihen liitetyille tietokoneille. Tämä laite on myös lainattu erään työntekijän testipenkistä sen takia, että sopivia kytkimiä ei IT-osastolta ollut löytynyt, kun tarve tuli. Tästä kytkimestä halutaan eroon, joten se ei siis tule olemaan osa uutta suunniteltua verkkoa. En löytänyt tarkkaa vuotta, milloin kyseinen laite on julkistettu, mutta ohjelmistopäivityksen päiväys ulottuu vuoteen 2008. Eli laite voi hyvinkin olla 5 vuotta vanha.

Kytkimessä on yhteensä 24 RJ-45-porttia, joista neljä on ns. ”dual-personality”-portteja. Tämä tarkoittaa sitä, että kun loppuihin neljään lisäporttiin kytketään valokuitukaapelille tarkoitettu muunto-osa, RJ-45-portit 21 – 24 menevät pois päältä eivätkä näin ollen ole käytettävissä. Sama toisinpäin, mikäli neljä viimeistä porttia otetaan käyttöön, eivät nämä neljä lisäporttia kuituliittimille ole käytössä. Kytkimessä on Auto-MDIX-ominaisuus ja jokaisen portin kohdalla voidaan yltää 1 Gbps:n nopeuteen. Kytkintä voidaan hallita joko suoran konsoliyhteyden kautta, graafisesti web-selaimen kautta tai sitten erillisen HP Manager-ohjelman kautta. [32.]

Kuvio 5. Cisco Catalyst 3750G -kytkimet

Tällä hetkellä keskusnipussa on käytössä kaksi kappaletta Ciscon Catalyst 3750G -mallin kytkimiä. Toinen on 24-porttinen, jossa on 4 lisäporttia esimerkiksi vaihdettaville kuituliittimille ja toinen on 12-porttinen kytkin, joissa kaikki portit on toteutettu vaihdetta-

villa liittimillä. Näiden kaikkien porttien nopeudet ovat korkeintaan 1 Gbps, joten valokuitukaapeleilla ei saa merkittävää nopeuseroa jos ollenkaan. Ja koska kaikki portit ovat vaihdettavia, voidaan kaikki 12 porttia käyttää joko RJ-45-liittimillä tai kuituliittimillä. 3750G-mallin kytkimet olivat suunnitelmaa aloittaessa jo saavuttaneet elinkaarensa pään, joten niiden sisällyttäminen uuden suunnitelman käyttöön ei ollut mitenkään järkevää. Edellisen lisäksi, nämä kytkimet eivät tue älykkäämpää StackWise+ -teknologiaa, vaan ainoastaan tavallista StackWise-tekniikkaa. [33.]

Kuvio 6. Catalyst 2950G

Ciscon Catalyst 2950G on malli, jonka elinkaari päättyi jo joulukuussa 2006, joten tässäkin on kyse hyvin vanhasta mallista. Tästäkin syystä tätä ei haluttu ottaa mukaan suunniteltuun verkkoon niin Philipsin puolelta kuin omalta osaltanikaan. Kyseisessä kytkimessä on 24 RJ-45-porttia sekä kaksi lisäporttia. Lisäportit toimivat jopa 1 Gbps:n nopeudella, ja ne ovat ainoastaan kuituliittimiä varten. Perusportit taasen ovat tarkoitettu RJ-45-liittimille ja toimivat korkeintaan 100 Mbps:n nopeudella. [34.]

3.3 IP-osoiteavaruus

Nykyinen IP-osoiteavaruus on kyseissä toimipisteessä äärimmilleen käytetty. Muutenkaan kyseinen osoiteavaruus ei ole mitenkään järkevästi jaettu, vaan verkossa oleville laitteille on joko jaettu osoitteet DHCP:n kautta tai sitten käsin määritetty. Philipsillä käytössä olevia erilaisia verkkolaitteistotyyppejä ovat esimerkiksi verkkotulostimet sekä tietokoneiden langattomat ja langalliset verkkosovittimet. Osoiteavaruuden pituudeksi oli varattu 2 kpl 256 IP-osoitteen verkkoa, joille varataan yksi IP-osoite verkko-

osoitteeksi ja yksi nk. ”broadcast”-osoitteeksi, eli osoitteeksi, johon tiedon laittaminen levittää tiedon koko verkkosegmenttiin.

Tekniikka, jolla verkko jaoteltaisiin pienempiin erikokoisiin segmentteihin (nk. broadcast domaineihin) laitteiden tai tarkoituksen perusteella kytkimissä tai reitittimissä, on nimeltään VLAN. Nykyisessä verkkototeutuksessa tätä jaottelua ei ole käytössä ollenkaan, vaan koko verkkoa voisi kuvata yhdeksi kokonaiseksi VLAN:ksi. Taulukosta 3 näkee, miten IP-osoitteet on jaettu toimipisteessä. Kyseessä ei tietenkään ole alkuperäiset verkon IP-osoitteet, vaan muutin ne toisiksi sitä varten, että saan käyttää näitä verkon tietoja opinnäytetyössäni.

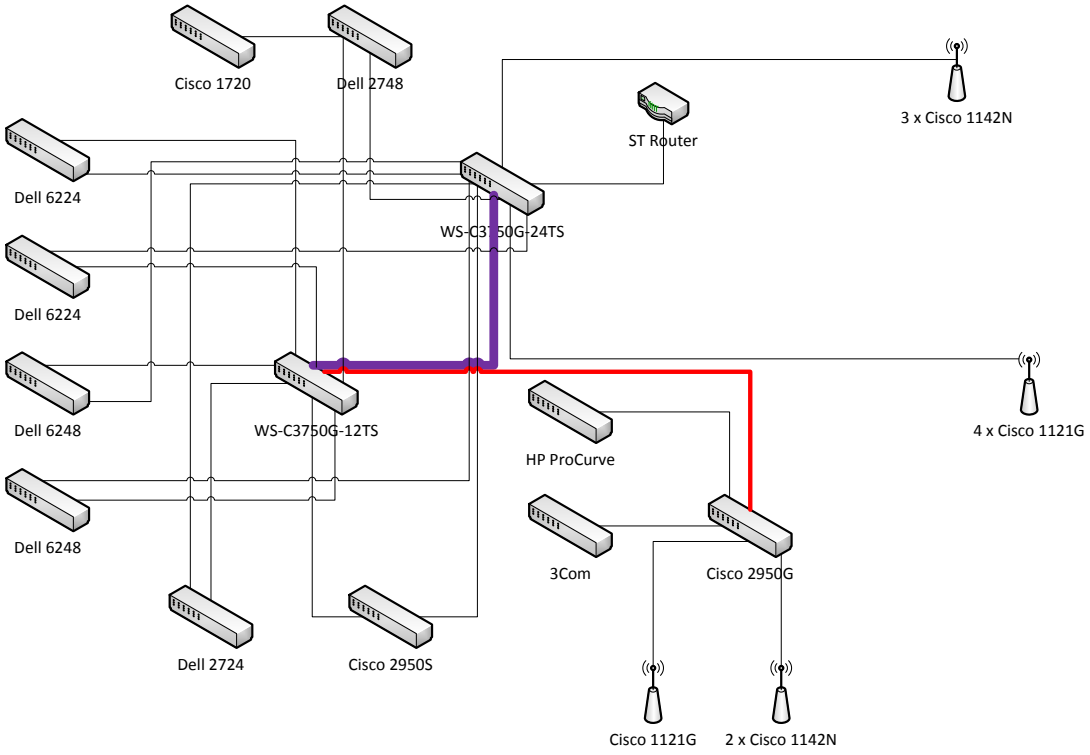
Taulukko 3. Philipsin toimipisteen käyttämä IP-osoitteiden olemassa ollut jakotapa

Tarkoitus	IP-osoitteet (192.168.0.xxx / 192.168.1.xxx)
Verkkolaitteet ja palvelimet	1 – 30
Tulostimet	31 – 50
DHCP-palvelimen kautta automaattisesti jaettavat osoitteet	51 – 150
Staattiset osoitteet	151 – 191
	192 – 223
Verkkolaitteet ja palvelimet	224 – 254

Taulukossa 1 on lueteltu toimipisteessä käytetyt IP-osoiteavaruudet ja se, miten ne on jaettu. Kun taulukkoa katsotaan, nähdään, että molemmista 256 osoitteen verkosta on sama osa jaettu samalle tarkoitukselle, eli samojen laitteiden käyttöön. Esimerkiksi alue 192.168.0.1 – 30 ja 192.168.1.1 – 30 on varattu sekä verkkolaitteille että palvelimille. Seuraavat osoitteet eli 31 – 50 molemmista verkoista on varattu tulostimille. Eli vaikka jaottelua onkin tehty, ei kyseessä ole kuitenkaan varsinainen VLAN-tekniikka. Osoitteet välissä 192.168.0.192 – 223 on jaettu erillisesti, eivätkä ne millään tavalla ole jaettuna DHCP-palvelimen kautta. Aliverkon peitteenä verkossa toimii 255.255.240.0 molemmilla alueilla.

3.4 Topologia

Olemassa oleva verkon topologia toimi, mutta koska verkossa oli eri valmistajien laitteita, se ei lopulta ollut kovinkaan optimaalinen. Tämä aiheuttaa myös sen, että joitain valmistajakohtaisia tekniikoita ei voi käyttää muiden valmistajien laitteista puuttuvan tuen vuoksi. Yksi sellainen tekniikka, mitä olisi voinut käyttää, on nimeltään EtherChannel.



Kuvio 7. Verkon vanha topologia.

Kuviossa 7 on toimipisteen vanha topologia. Laitteita tässä topologiassa on yhteensä 24. Näistä 24 laitteesta 10 langattoman lähiverkon tukiasemia, 13 kytkimiä sekä yksi reititin Internet-yhteyttä varten. Kaksi kytkintä toimii niin sanottuina ”Core-kytkiminä”, eli keskuskytkiminä, jotka hoitavat liikenteen reitityksen verkon muiden kytkinten välillä. Nämä kytkimet ovat liitettyinä toisiinsa niin sanotulla ”stack-kaapelilla”, ja ne käyttävät Ciscon omaa StackWise+ -teknologiaa, jolla saadaan jopa 32 gigabitin tiedonsiirtono-

peuksia kytkinten välillä. Nämä kaksi muodostavat näin ollen keskusnipun. Nykyisestä verkon laitteista on taulukko liitesivuilla (liite 1).

3.5 Verkon konfiguraatiot

Ciscon verkkolaitteiden peruskonfigurointi on todella helppoa. Tähän vaikuttaa todennäköisesti se, että koulussa niitä on käyty melkeinpä kyllästymiseen asti läpi. Toisaalta se, miten niitä konfiguroidaan, miten verkko rakentuu ja miten eri operaattorien verkot liitetään toisiinsa, on erittäin kiinnostava aihe. Valitettavasti ihan kunnolla ei operaattorien väliseen liikenteeseen ehditty perehtymään kummemmin omasta mielestäni, mutta toisaalta koulun Ciscon kurssit antoivat todella hyvät perusteet verkkojen suunnittelulle ja toteutukselle. Loppu on sitten itsestä kiinni, miten näitä opittuja asioita pystyy ja haluaa hyödyntää.

3.5.1 Langattoman tukiaseman konfiguraatio

Kuten aiemmin mainitsin, langattoman lähiverkon tukiasemien vaihtoon kuului vanhan laitteen löytäminen, konfiguraation lataaminen uuteen laitteeseen sekä laitteiden fyysinen vaihto ja merkintä, mikä laite vaihdettiin. Tässä käyn hieman läpi yhden langattoman tukiaseman konfiguraatiotiedostoa, joka löytyy liitesivuilta (liite 2). Kaikkien tukiasemien konfiguraatiotiedostot ovat lähes täysin identtiset. Ainoat poikkeavat erot ovat käytännössä tukiaseman laitenimen ja IP-osoitteen osalta sekä SNMP-palvelimen nimen kohdalla. Nämä kun ovat laitekohtaisia.

Aloitetaan konfiguraatiosta, joka liittyy RADIUS-autentikointiin. RADIUS on siis nimitys verkossa toimivalle protokollalle, jolla käyttäjä voi autentikoida itsensä. Sitä käytetään yleensä verkoissa autentikoimaan esimerkiksi verkkosertifikaatti, jolla käyttäjä voi sitten liittyä yrityksen langattomaan verkkoon.

```
aaa group server radius rad_eap
 server ip_osoite1 auth-port <port> acct-port <port>
```

```
server ip_osoite2 auth-port <port> acct-port <port>
server ip_osoite3 auth-port <port> acct-port <port>
```

Ensimmäisellä rivillä luodaan ryhmä nimeltä ”rad_eap” RADIUS-palvelinten ryhmälle. Kolmella viimeisellä rivillä kerrotaan, mitkä ovat RADIUS-palvelinten IP-osoitteet sekä niiden käyttämät autentikointi- ja käyttäjätiliportit. Näitä ryhmiä voi luoda monia eri käyttöä varten. Liitteenä olevassa konfiguraatiossa näitä RADIUS-ryhmiä on luotu kolme kappaletta.

```
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login tunnus_tähän group nimi_tähän
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
```

Ensimmäisellä rivillä määritetään, että tukiasemaan kirjautuminen tapahtuu oletuksena paikallisella tunnuksella. Toisella rivillä määritetään, että kirjautuminen LEAP-metodilla sallitaan rad_eap-ryhmältä. Kolmannella rivillä määritetään käytettäväksi MAC-osoitteita paikallisesta tunnuslistasta. Seuraavalla rivillä sitten määritetään yksi paikallinen käyttäjätunnus aiemmin luodusta ryhmästä, jolla laitteeseen pääsee kirjautumaan. Viides rivi määrittää, että paikallisesta laitteen tietokannasta löytyvät käyttäjätunnukset saavat oikeuden käyttää komentoriviä laitteen konfigurointiin. Viimeinen rivi kertoo, että laitteeseen on määritetty laskurit rad_acct-ryhmän verkon käytön, esimerkiksi siirretyn tietomäärän seuraamiseksi.

```
dot11 ssid nimi_tähän
vlan yyy
authentication open eap eap_methods
authentication network-eap eap_methods
```

```
mbssid guest-mode
```

Tässä osassa määritellään ensimmäisellä rivillä, mille SSID:lle nämä yllä olevat komennot tapahtuvat. Toisella rivillä määritellään, mikä on kyseisen SSID:n käyttämä VLAN, kolmannella ja neljännellä rivillä määritetään, että autentikointi voi olla joko avaimella, tai sitten verkon kautta, eli RADIUS-palvelimen avulla. Viides rivi puolestaan kertoo, että VLAN:n SSID:tä jaetaan laitteiden näkyville.

```
dot11 ssid nimi_tähän
  vlan xxx
  authentication open
  authentication key-management wpa
  mbssid guest-mode
  wpa-psk ascii 7 salsana_tähän
```

Tämä osio on samanlainen kuin edellinenkin, mutta rivi 4 on erilainen ja lisäksi tässä on myös kuudes rivi olemassa. Ne näkyvät vahvennettuina riveinä. Tämä erilainen neljäs rivi kertoo, että käytetään WPA-avainta. Kuudes rivi taasen määrittää salasanan ja sen, millä WPA-metodilla salasana on jaettu asiakaslaitteelle. Tässä tapauksessa WPA-metodi on, että salasana on esijaettuna (PSK, Pre-Shared Key).

```
username käyttäjätunnus1_tähän privilege 15 password 7 salasana_tähän
username käyttäjätunnus3_tähän password 7 salasana_tähän
```

Näillä kahdella rivillä määritellään käyttäjätunnukset, salasanat sekä pääsytasot, jotka määrittävät, mitä komentoja kukin saa käyttää. Taso 15 on korkein, eli sillä tasolla on kaikki mahdolliset komennot käytettävissä. Kolmannella käyttäjätunnuksella ei ole tasoa mainittu, joten oletuksena sillä pääsee kyllä kirjautumaan, mutta ei sen enempää.

```
interface Dot11Radio0
 encryption vlan yyy mode ciphers tkip
 encryption vlan xxx mode wep mandatory
 broadcast-key change 300
 station-role root fallback shutdown
```

Tässä osassa olen poistanut osan riveistä, mutta ne löytyvät edelleen liitteestä 2. Loput rivit ovat mielenkiintoisempia, ja siksi käyn ne läpi tässä. Ensimmäinen rivi jälleen määrittää, mille sovittimelle sitä seuraavia komentoja kohdistetaan. Toinen ja kolmas rivi kertovat sen, millä tavalla tietyn VLAN:n lähettämä signaali salataan. Neljäs rivi määrittää, kuinka monen sekunnin välein jakeluavain vaihtuu. Tämä jakeluavain on kaikille yhteinen osa salausavainta. Viides rivi määrittää tukiaseman roolin sekä sen, mitä tapahtuu, jos ethernet-portti ei ole toiminnassa. Tukiaseman rooli on tässä tapauksessa ”root”, eli se toimii siltana langalliseen verkkoon. Tämä tarkoittaa myös sitä, että siihen tukiasemaan voivat muut alemman roolin tukiasemat liittyä, eli jatkaa langatonta verkkoa. Tässä tapauksessa komento ”fall back shutdown” sammuttaa laitteen lähetyksen.

```
interface Dot11Radio0.yyy
 encapsulation dot1Q yyy
 bridge-group yyy
 bridge-group yyy subscriber-loop-control
 bridge-group yyy block-unknown-source
 no bridge-group yyy source-learning
 no bridge-group yyy unicast-flooding
 bridge-group yyy spanning-disabled
```

Poistin taas pari ylimääräistä riviä käydäkseni läpi ne mielenkiintoisimmat konfiguraatiokomennot. Ensimmäinen rivi ilmoittaa taas, mille sovittimelle komennot pätevät. Huomionarvoista tässä komennossa on se, että sovitin on tunnukseltaan ”0.yyy”. Tämä tarkoittaa sitä, että käytetään sovitinta 0, mutta luodaankin siihen alisovitin, johon asetukset pätevät alkuperäisen sovittimen sijaan. Toinen rivi määrittää sen, mitä tekniikkaa

käytetään liikenteen kapselointiin. Dot1Q-kapselointi on protokolla, joka mahdollistaa VLAN:ien tietopakettien kuljettamisen ja erottelun yhden fyysisen linkin kautta. Kolmannella rivillä oleva ”bridge-group yyy” -komento luo siltaavan ryhmän nimeltä ”yyy”. Tällä siltauksella voidaan lisätä yksi tai useampi laitteen sovitin samaan lähetysalueeseen (broadcast domain). Seuraava komento lisää siltaukseen kierronhallinnan, eli data ei lähde pyörimään verkossa holtittomasti päättymätöntä ympyrää, vaan pääsee onnistuneesti perille. Siltaukseen liittyvä block-unknown-source-komento tekee sen, että tuntemattomista MAC-osoitteista estetään liikenne tietyssä sovittimessa. Seuraavan komennon alussa oleva ”no” merkitsee sitä, että perässä tuleva komento otetaan pois käytöstä. Eli tässä tapauksessa se tarkoittaa sitä, että ”bridge-group yyy source-learning” -komento ei lue lähettäjän tietoja datapaketista. Seuraava rivi onkin sitten sellainen, että se kannattaa olla päällä. Kun ”bridge-group yyy unicast-flooding” –komennon eteen laitetaan ”no”, ei tukiasema lähettele unicast-paketteja jokaiseen mahdolliseen VLANiin tukkien koko verkkoliikennettä. Syynä tähän verkon tukkeutumiseen on asymmetrinen reititys. Viimein rivi ottaa spanning tree -protokollan pois käytöstä kyseisellä verkkosovittimella.

```
ip http server
ip http authentication aaa
no ip http secure-server
ip radius source-interface BVI1
logging trap warnings
snmp-server community salasana1_tähän RW
snmp-server community salasana2_tähän RO
snmp-server location tekstijono1_tähän
snmp-server contact tekstijono2_tähän
snmp-server chassis-id tekstijono3_tähän
snmp-server enable traps tty
snmp-server enable traps rogue-ap
radius-server attribute 32 include-in-access-req format %h
radius-server host ip-osoite_tähän auth-port <portti> acct-port <portti> key 7 salasana_tähän
```

```
radius-server deadtime 15
radius-server vsa send accounting
bridge 1 route ip
```

Ensimmäinen komento luo laitteelle HTTP-palvelimen, jota voidaan käyttää toiminnan testaamiseksi. Toinen komento luo kyseiselle palvelimelle paikallisen autentikoinnin. Kolmas komento määrittää, että palvelin ei ole suojattu palvelin. Tämä komento voi olla verkolle vaarallinen jos tätä käytetään Internetiin kytketyssä reitittimessä. Mutta koska kyseessä on sisäverkossa olevat tukiasema, ei ulkopuolelta siihen pääse käsiksi.

Seuraava komento tekee sen, että tukiaseman BVI lähetetään eteenpäin laskureita varten. Komento ”logging trap warnings” tarkoittaa sitä, että laite kirjoittaa lokitiedostoon kaikki varoitukset ja sitä pahemmat virhetilanteet. Kaksi seuraavaa riviä määrittävät salasanat SNMP-palvelimelle muokkaus- (RW) ja ”vain luku”-oikeuksille (RO). Seuraava rivi on kuvaus sille, missä SNMP-palvelin sijaitsee. Sitten on kontaktihenkilön tai -ryhmän nimi, sitten tulee sen laitteen nimi, jossa tämä SNMP-palvelin toimii. Komento ”snmp-server enable traps” pistää päälle ilmoitukset erilaisista tapahtumista. Näitä mahdollisia tapahtumia on monia, joten käyn tässä läpi vain pari kohtaa, vaikka konfiguraatiossa niitä on enemmänkin. Ensimmäinen näistä kahdesta kertoo, kun telnet-istunto laitteeseen katkeaa. Normaalisti tämä on erittäin turhaa tietoa, mutta yritysverkossa siitä voinee olla hyötyä esimerkiksi telnet-yhteyksien katkosten selvittämiseksi. Toinen kohta ilmoittaa, jos verkossa havaitaan ns. ”rosvotukiasema”, eli tukiasema, jolla ei esimerkiksi ole verkon ylläpitäjän hyväksyntää tai sitten, että se on verkkorikollisen asentama laite jolla rikollinen yrittää suorittaa ”man-in-the-middle”-hyökkäyksen.

Seuraava komento lähettää verkkolaitteen tunnuksen (nk. NAS-tunnuksen) RADIUS-palvelimelle pääsyoikeuspyynnön tai laskuripyynnön aikana. Sitten tulee yhden RADIUS-palvelimen IP-osoite sekä tarvittavat portit. Erona konfiguraation alussa oleviin riveihin on tässä salasana sekä taso, jolla se on nähtävissä konfiguraatiossa. Taso 7 näyttää salasanan ainoastaan salattuna. Seuraava komento määrittää, kuinka monta minuuttia odotetaan ennen kuin RADIUS-palvelin merkataan ”kuolleeksi”, eli vaihdetaan seuraavaan palvelimeen. Toiseksi viimeinen rivi määrittää, että tukiasema tunnistaa ja käyttää valmistajakohtaisia attribuutteja vain laskureihin. Viimeinen komento sitten ohjaa sovitinta siten, että jos siinä on IP-osoite, niin kaikki tietoliikenne siihen ja siitä kulkee vain tämän sovittimen kautta.

3.5.2 Catalyst 2960S:n konfiguraatio

Seuraavaksi onkin vuorossa kytkimen konfiguraatiota. Tämä kyseinen kytkin on uusin lisäys verkkoon, ja se on Ciscon peruskytkin mallilta an 2960S. Tässä verkossa nämä kytkimet on tarkoitettu verkon liityntäpisteiksi. Konfiguraatiosta jonkin verran on samaa kuin tukiasemassa, joten niitä en suotta käy uudestaan läpi. Käyn taas mielenkiintoisimmat kohdat konfiguraatiosta. Tämän kytkimen konfiguraatio löytyy myös liitesivulta (liite 3).

```
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree uplinkfast
spanning-tree vlan 1-100 priority 8192
```

Nämä kaikki rivit koskevat STP:n (Spanning Tree Protocol) käyttöönottoa sekä sen ominaisuuksia. STP:n tarkoituksena on portteja sulkemalla estää verkossa tapahtuvia reitititysvirheitä, joissa tietopaketit jäävät kiertämään verkkoon loputtomasti aiheuttaen verkon hidastumisen tai jopa kaatumisen. Ensimmäisellä rivillä määritetään, mikä on STP:n käyttämä moodi. Tässä tapauksessa se on PVST, eli Per-VLAN Spanning Tree. Sen tarkoituksena on mahdollistaa jokaiselle VLAN:lle omat STP:t, jotta eri VLAN:ien tietoliikenne voi kulkea eri kaapeleissa. Seuraava komento tekee sen, että tuettujen VLAN:ien määrä nousee 1005:sta 4096:een sekä VLAN ID lisätään kytkimen bridge ID:hen. Kolmas komento parantaa yhteyden palautumisnopeutta tilanteessa, jossa alkuperäinen linkki katkeaa. Viimeinen komento muokkaa VLAN:ien 1 – 100 prioriteettia. Mitä pienempi numero, sitä todennäköisemmin kytkin valitaan pääkytkimeksi.

```
interface Port-channel3
 description Port-channel3 to Core stack
 switchport mode trunk
 storm-control broadcast level 0.50
```

Nämä komennot koskevat EtherChannelin luontia kytkimelle. Ensimmäisessä komennossa luodaan EtherChannel numero 3. EtherChannelin numerotunnuksen ei tarvitse olla sama molemmissa päissä, vaan se voi olla ihan vapaasti valittu molemmissa yhdistetyissä kytkimissä. Toinen komento lisää kuvauksen, joka näkyy kun konfiguraatiotiedostoa luetaan. Seuraava komento määrittää, että luotu linkki yhdistää tähän EtherChanneliin liitetyt linkit yhdeksi näennäiseksi linkiksi. Viimeinen komento määrittää, että verkkoa suojellaan ylimääräisiltä tietopaketeilta. Kun broadcast-liikennettä on puoli prosenttia tietovirrasta, kaikki broadcast-liikenne tiputetaan automaattisesti kytkimessä pois, eikä enempää broadcast-tietopaketteja päästetä porteista ulos. Prosenttirajan voi vapaasti määrittää, mutta mitä pienempi se on, sitä tiukempi on raja broadcast-liikenteelle. Toisaalta, mahdollisen broadcast-myrskyn sattuessa liikenne estetään nopeammin. Puolen prosentin raja on pieni, ja se on yleensä esimerkeissä ollut rajana. Raja voidaan alustavasti määrittää oman mielen mukaan ja nostaa tai laskea sitten tarpeen tullen.

```
interface GigabitEthernet1/0/51
 switchport mode trunk
 storm-control broadcast level 0.50
 channel-group 1 mode on
```

Tässä osassa määritellään portti, joka kuuluu EtherChanneliin. Ensimmäisellä komennolla valitaan kytkimen portti, joka halutaan liittää EtherChanneliin. Toinen ja kolmas komento ovat sama kuin EtherChannelin luonnissa, ja ne tulevatkin portin konfiguraatioon automaattisesti, kun portti neljännellä komennolla liitetään EtherChanneliin. Eli toista ja kolmatta komentoa ei tarvitse itse tehdä.

3.5.3 Keskusnipun konfiguraatio

Tässä käyn läpi keskusnipun konfiguraation mielenkiintoisimmat kohdat. Keskusnipussa olevat kytkimet jakavat konfiguraation, eli se on lähes identtinen jokaisessa kytkimessä. Kun nippuun kirjaudutaan käyttäen joko SSH:ta tai telnetiä, näkyy konsolissa vain yhden kytkimen konfiguraatio. Kuitenkin kaikki muutokset, jotka siinä konsolissa

tehdään, tulevat kaikkien kytkinten konfiguraatioon samanlaisina. Konfiguraatio löytyy neljäntenä liitteenä liitesivuilta (liite 4).

```
switch 1 provision kytkin1
```

Tämä komento näyttää, että ykköskytkimenä toimii nipun tietty kytkin. Kohtaan ”kytkin1” tulee ensimmäisen kytkimen tyyppi. Eli esimerkiksi ”ws-c3750x-24”.

```
ip cef load-sharing algorithm universal DE676A1B
```

Tämä komento käynnistää reitittimessä tai kytkimessä kuormanjaon. Komento myös määrittää sen universaaliksi, joka käyttää sekä lähettäjän että vastaanottajan osoitetta sekä ID hashia, joka tässä esimerkissä on DE676A1B. Universaali tarkoittaa sitä, että kun se on käytössä, voidaan kuormaa jakaa esimerkiksi molemmille WAN-linkeille.

```
ip multicast-routing distributed
```

Tämä komento aktivoi multicast-reitityksen sekä sen, että multicast-reititystaulu otetaan käyttöön ja täytetään reititystiedolla.

```
ip route ip_osoite aliverkon_peite ip_osoite
```

Tämä komento sisällyttää oletusreitin kytkimen reititystauluun. Syntaksin mukaan ensimmäinen osa määrittää, että kyseessä on staattinen reitti, eli reitti joka ei muutu verkon muuttuessa. Toinen osa ja kolmas osa ovat kohteen IP-osoite sekä aliverkon peite. Neljäs osa on sitten se IP-osoite, jonka kautta reitin pitää kulkea. Yleensä käytetään esimerkiksi yrityksen verkon omaa Internet-reititintä.

```
ip access-list extended ryhmän_nimi
 deny ip any host ip_osoite
 remark *** Block all access to specific hosts ***
 deny tcp any host ip_osoite eq 3389
 permit ip any any
```

Ensimmäisellä komennolla luodaan pääsylista. Kyseessä on ns. ”extended”-pääsylista, eli se osaa katsoa tietopaketista lähettäjän IP-osoitteen lisäksi myös esimerkiksi vastaanottajan IP-osoitteen sekä lähtö- ja kohdeportin. Seuraava komento estää kaikista IP-osoitteista tulevan liikenteen tiettyyn IP-osoitteeseen. Tässä komennossa ei ole järkeä sisäverkossa, mutta kun ensimmäisessä komennossa määritetty ryhmä lisätään vaikkapa Internet-reitittimeen kytkeytyvän portin pääsylistoihin, estää tämä toinen komento Internetin suunnasta tulevan tai suuntaan menevän liikenteen. Kolmas komento eli ”remark” on sama kuin kuvaus-komento (”description”), eli sillä voidaan kuvailla, mikä on edeltävän tai seuraavan komennon tarkoitus. Neljäs komento estää kaikki tcp-protokollaa käyttävät yhteydet tietyn IP-osoitteen tiettyyn porttiin. Viides komento sallii kaiken muun liikenteen. Sillä, missä järjestyksessä nämä estot ja sallimiset ovat, on väliä. Ylempänä oleva esto- tai sallintakomento on vahvempi kuin alempana oleva komento. Eli jos salliva komento on ylempänä, ei alempana oleva ristiriitainen estokomento ole voimassa. Tätä pääsylistaa ja siihen liitettyjä IP-osoitteita käytettiin Philipsillä estämään tietyn osoitealueen IP-osoitteita pääsemästä Internetiin sekä Internetistä niihin osoitteisiin. Tämän tarkoitus oli toimia IP-pohjaisena ”VLAN:ina”, koska virtuaalisia lähiverkkoja ei ollut toimipisteessä konfiguroituna.

4 Suunniteltu verkko

Tässä kappaleessa käyn läpi, mitä kaikkea uuteen verkkoon suunnittelin annettujen tarpeiden pohjalta. Siihen liittyy vanhan IP-osoiteavaruuden jakaminen VLAN:eihin, jotta saadaan verkon jaottelua paremmaksi, ja siltä osin myös sitten DHCP-palvelimen osalta järkevöitettyä IP-osoitteiden jakelua sekä myös uuden verkkotopologian suunnitelma. Suunnitelman tarkoitus on olla toteutuskelpoinen muutoksin mahdollisesti myös muille yrityksille, vaikka se onkin tähän yhteen Philipsin toimipisteeseen suunniteltu.

4.1 Uuden IP-osoiteavaruuden suunnittelu

IP-osoiteavaruuden laajentaminen ja sen jakaminen olivat yksi keskeisiä kohtia tässä työssä, sillä osoitteet olivat loppumassa kesken käyttäjämäärien sekä lähiverkkoa että langatonta verkkoa käyttävien laitteiden lisääntymisen vuoksi. Tein viisi erilaista suunnitelmaa, miten nykyisen kokoista verkkoa voidaan hyödyntää VLAN-tekniikalla. Käyn tässä osiossa läpi kolme suunnitelmaa ja niiden eroja. Kaksi muuta suunnitelmaa jätän käymättä, koska ne ovat hyvin samanlaisia kuin nämä muut, mutta hyvin pienin eroin. Näissä kolmessa läpikäytävässä erot ovat kaikkein suurimmat, joten siksi ne ovat valittuina.

Liitteessä 5 olevassa taulukossa on huomattavaa, että siinä pyrin pitämään verkon suurin piirtein samanlaisena, kuin se nyt on. Käytännössä tämä ei ole kovinkaan hyvä tapa, sillä se tekee verkosta alttiimman IP-osoitteiden hukkaamiselle. Tämä johtuu siitä syystä, että mitä enemmän näitä broadcast domaineja on, sitä enemmän on myös broadcast- ja network-osoitteita. Jokainen oma VLAN-segmentti tarvitsee omat broadcast- ja network-osoitteensa. Tämä on myös paljon vähemmän joustava tapa luoda VLANeja, koska aina kun luodaan joku tietyn kokoinen VLAN vaikkapa 192.168.1.192 – 255 välille, pitää varata saman verran IP-osoitteita myös toisesta verkosta. Tämä sen takia kun halutaan, että molemmista verkoista on samat ”kohdat” samalle tarkoitukselle varattuna (liite 5).

Ehdotuksessa näkyy myös sitten nämä käyttämättömät alueet. Ne ovat toisin sanoen alueita, joita ei ole vielä allokoitu mihinkään tarkoitukseen, vaan ovat vapaata riistaa. VLANien osalta pyrin pitämään numerointikäytännön sellaisena, että rinnakkaiset segmentit alkaisivat samalla numerolla. Tästä syystä esimerkiksi on olemassa VLANit 3 ja 33. Eli ovat samalle tarkoitukselle allokoituja, mutta rinnakkaisissa verkoissa. Käytin tässä erilaisia nimityksiä eri VLANeille niiden tarkoitukset mukaan. Näitähän ovat siis:

- **Transit** Tarkoitettu Internetiin kytkettäviä reitittimiä varten. Ne sallivat Internet-liikenteen sisään ja ulos toimipisteen verkosta. Laitteita voi olla useampia, mikäli useampia yhteyksiä taloon tulee ja ne on tarve yhdistää vikasietoisuuden parantamiseksi.

- **Verkkolaitteet** Tarkoitettu sisäverkon laitteille pois lukien Internetiin yhdistävä laitteet. Sisältää sekä langattomat tukiasemat, kytkimet ja muut reitittimet.

- **Tulostimet** Nimensä mukaisesti VLAN on tarkoitettu verkkoon kytketyille tulostimille ja niiden IP-osoitteille.

- **Palvelimet** Myös tämä on tarkoituksensa mukaisesti nimetty, eli palvelimille, joille on tarkoitus käyttäjien päästä joko käyttämään jotain palvelua, kuten tietokantoja tai sitten tallentamaan tiedostoa.

- **DHCP** Tämä sisältää ne IP-osoitteet, jotka jaetaan verkon asiakaslaitteille DHCP-palvelimen kautta automaattisesti. Ei sisällä niitä, jotka määritetään käsin tai MAC-osoitteen kautta.

- **Ei Internet-yhteyttä** Tämä VLAN on tarkoitettu sellaisille laitteille, joiden pitää päästä sisäiseen verkkoon ja joihin pitää päästä sisäisestä verkosta, mutta Internet-liikenne laitteeseen ja laitteesta halutaan estää.

- **Staattiset osoitteet** Niille laitteille tarkoitettu VLAN, joille halutaan määrittää pysyvät osoitteet. Internet-liikenne on mahdollista tähän VLANiin, mutta tärkeintä näille laitteille on, että niillä on koko ajan samat osoitteet. Tämä hoidetaan niin, että laitteelle määritellään osoite ja se pistetään ylös tietokantaan. Voidaan myös mahdollisesti hoitaa MAC-osoitteeseen perustuvalla jakelulla DHCP-palvelimelta.

- **Käyttämätön** Tämä on nimensä mukaisesti käyttämätön ”VLAN”. Varsinaisesti vain IP-osoitealue, jota ei ole allokoitu mihinkään käyttöön. Siihen voidaan mahdollisuuksien mukaisesti luoda yksi tai useampia alueita joko uusiin käyttötarkoituksiin tai sitten jonkin, jo olemassa olevan, alueen lisäalueeksi.

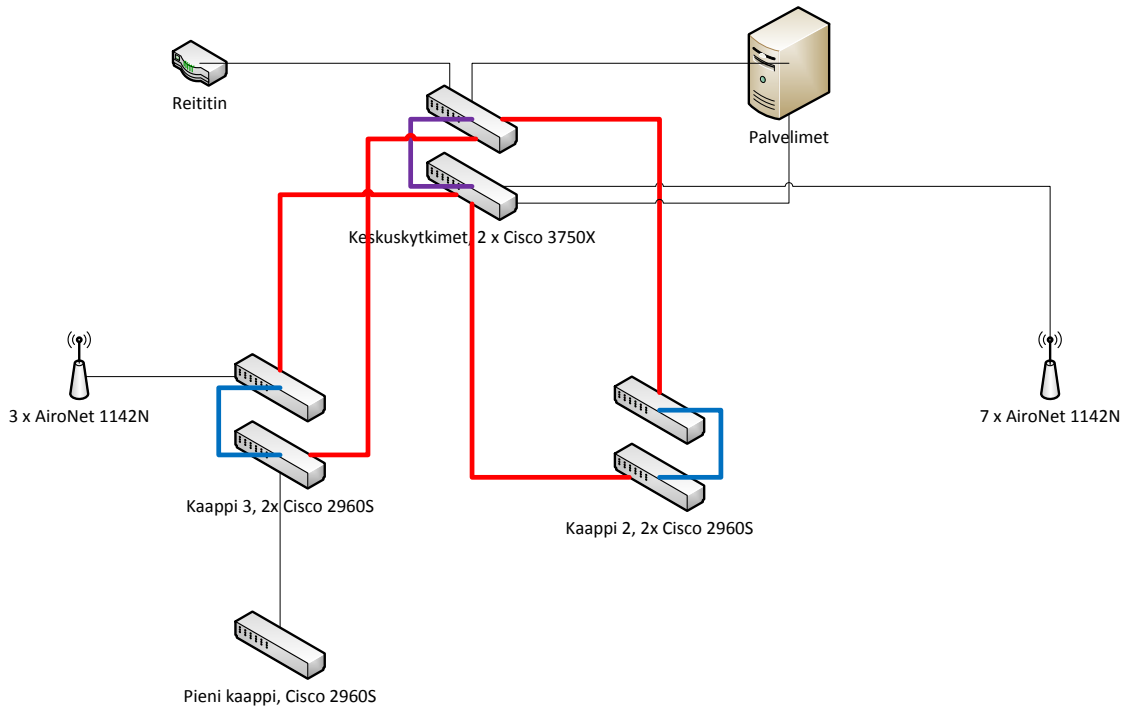
Liitteessä 6 olevan osoiteavaruuden suunnitelman erot edeltävään ovat ne, että nyt on järjestyksessä allokoitu segmentit alusta lähtien. Myös langattomien sekä langallisten laitteiden käyttäjät on erotettu omiin VLAN-segmentteihinsä, joihin DHCP-palvelimelle on luotu omat IP-osoitealueet, joista se jakaa osoitteita. Se, onko tämä tarpeellista tai

järkevää, on lähinnä suunnittelukysymys. Toisaalta, kun nämä on erotettu toisistaan, menetetään kaksi IP-osoitetta yhden lisä-VLANin verkko- ja lähetysosoitteisiin (liite 6).

Liitteessä 7 oleva suunnitelma onkin sitten hieman mutkikkaampi mahdolliseksi IP-osoitteiden jakotavaksi. Palvelimet ja tulostimet on yhdistetty yhteen VLAN:iin, mutta sitten yksi IP-osoite on varattu aliverkolla ja sitä myöten niille laitteille, joiden ei ole tarkoitus päästä Internetiin. Käytännössä tarkoittaa sitä, että jostain kytkimestä on varattu yksi kokonainen portti pelkässä sisäverkossa toimiville laitteille. Langattoman verkon laitteet ovat tässä ehdotuksessa omassa VLAN:issaan, mutta sitten staattiset osoitteet on sisällytetty samaan VLAN:iin kuin langallisen verkon laitteet. Käytännön toteutuksen osalta tämä menisi niin, että DHCP-palvelimelta varataan sitten sopiva määrä osoitteita, joita jaetaan. Tämähän voidaan toteuttaa joko niin, että puolet annetaan automaattisesti jaettaviksi ja puolet sitten joko määritetään manuaalisesti käsin laitteille tai jaetaan MAC-osoitteiden perusteella. Toinen vaihtoehto on. että koko VLAN:n osoiteavaruus jaetaan DHCP-palvelimen kautta, mutta sitten erikseen määritetään mitkä osoitteet jätetään jakamatta. Näin ollen sitten ne jaettavat osoitteet voidaan käsin määrittää laitteelle (liite 7).

4.2 Suunniteltu topologia

Uusitun verkon topologia ei hirveästi muutu alkuperäisen, vanhan verkon topologiasta. Muutokset koskevat lähinnä sitä, miten uudessa verkossa vanhat Dellin kytkimet tulevat kytketyiksi verkkoon. Suoraan keskuskytkimiin ne eivät tule kiinni, vaan niitä voidaan käyttää esimerkiksi peruskytkiminä ns. pääsytasolla. En niitä kuitenkaan ole sisällyttänyt varsinaiseen suunnitelmaani, koska niitä voidaan siirrellä uudessa topologiassa tarpeen mukaan.



Kuvio 8. Uusi, suunniteltu verkko.

Kuten mainitsin, tämä uusittu verkko ei suoranaisesti paljoa eroa vanhasta verkosta, samat tietoliikennekaapit ovat käytössä, mutta tällä kertaa on kaikissa kaapeissa käytetty Ciscon laitteita ja nipuissa Ciscon StackWise- sekä FlexStack-tekniikkaa. StackWisea käytetään keskuskytkimissä ja FlexStackia 2960-sarjan kytkimissä. Molemmat niput on kytketty molemmista kytkimistä keskuskytkimiin (yksi kumpaankin) ja ne on yhdistetty kuituyhteydellä, jonka nopeus on 10 Gbps.

4.3 Uudet laitteet

Uuden verkon suunnittelussa uusien laitteiden on tarkoitus koostua ainoastaan Ciscon laitteista. Näin taataan mahdollisimman hyvä yhteensopivuus verkon laitteiden kesken. Toki vanhasta verkosta säästetään Dellin kytkimet, mutta ne toimivat tässä tapauksessa ainoastaan pääsytasolla, eli verkon asiakaslaitteiden liityntäpisteenä yrityksen verkkoon, mikäli ne otetaan käyttöön. Langattomat tukiasemat tulevat suoraan kiinni keskuskytkimiin.

Kuvio 9. Cisco Aironet 1142N

Kuten aiemmin mainitsin, uudemmat AiroNet-tukiasemat valittiin niiden tukeman 802.11n-standardin sekä sen tuoman nopeuslisän takia. Uusi, nopeampi N-standardi tukee jopa 600 Mt/s, ja tukee tietoliikennettä sekä 2,4 GHz:n että 5 GHz:n taajuusalueilla. Ei-päällekkäisten kanavien määrä vaihtelee seuraavasti: 2,4 GHz:n taajuusalueella ja 20 MHz:n kanavakoolla b-, g-, ja n-standardin verkoissa on 3 kappaletta. 5 GHz:n taajuusalueella ja 20 MHz:n kanavakoolla a- ja n-standardin verkoissa on 21 kappaletta sekä 40 MHz:n kanavakoolla n-standardin verkolla on 9 kappaletta.

Laitteessa on kaksi RJ-45-liitäntää, toinen konsolille ja toinen lähiverkolle. Verkolle menevän portin nopeus on korkeintaan 1 Gbps. Laitteelle voidaan antaa virtaa niin tavallisen virtalähteen, PoE-kytkimeltä kuin myös power injectorin kautta. Power injector tulee tukiaseman ja kytkimen väliin, ja se voidaan sijoittaa vaikkapa kytkinkaappiin. Näin ollen tukiaseman lähellä ei tarvitse olla erillistä pistorasiaa, vaan pelkkä tietoliikenneportti riittää. Power injector kuljettaa siis myös tietoliikenteen muuntimen sisällä. [35.] Kuten 1121G-mallisten tukiasemien tapauksessa, myös nämä uudemmat tukiasemat ovat ”standalone”-tyyppisiä.

Kuvio 10. Cisco Catalyst 3750X -mallin kytkin sekä moduuleja

Catalyst 3750X on uudempi versio 3750-mallista. Suunnitelluissa laitteissa on 24 kappaletta 1 Gbps:n maksiminopeudella toimivaa porttia sekä paikka moduulille, jolla saa esimerkiksi 2 kappaletta 10 Gbps:n nopeudella toimivaa RJ-45-liitintä. [36.] Tarkoituksena oli ottaa käyttöön nimenomaan tuo edellä mainittu moduuli, mutta käyttää kuituliittimiä RJ-45-liittimien sijasta. Moduulin porttien nopeuden takia 3750X valikoitui käytettäväksi kytkimeksi. Muuten olisi sopinut jo olemassa olevat 3750-sarjan peruskytkimet keskusnippuun. Molempiin keskusnipun laitteisiin halusin tilata tämän moduulin, ja sitä kautta sitten käyttää kuituyhteyttä molempiin erillisten kaappien nippuihin. Myös langattomat tukiasemat sekä palvelimet tulisivat suoraan kiinni näihin kytkimiin. Laitteiden ohjelmistona olin suunnitellut olevant Ciscon IP Base, joka siis sisältää myös LAN Basen toiminnot, koska IP Services -paketti olisi ollut turhan laaja sisäverkon käyttöön.

Kuvio 11. Cisco Catalyst 2960S.

Vaikka tämä kytkin olikin jo käytössä olemassa olevassa verkossa, laitan laitteen esittelyn tähän osioon siitä syystä, että se kuitenkin on olennainen osa uutta suunniteltua verkkoa. Tämä kytkin, tarkemmin 2960S-24TS-L, valittiin etäkaappien nippuihin käyttöön, sillä jokainen laite tarjoaa 24 kappaletta 1 Gbps:n nopeudella toimivia RJ-45-portteja sekä 4 kappaletta lisäpaikkoja joihin voidaan kytkeä valokuitu SFP-sovittimien avulla. Valokuidun nopeus on valitettavasti vain 1 Gbps, mutta se riittänee kuitenkin toistaiseksi verkon nopeaan toimintaan. Nämä kytkimet myös tukevat FlexStack-moduuleita, joten niputuskin onnistuu näiden laitteiden osalta. PoE-ominaisuutta ei kyseisiin kytkimiin nähty tarpeelliseksi, joten siitäkin syystä tämä kyseinen malli oli sopiva Philipsin tarpeisiin. [37.]

4.4 Budjetti/laitelistaus

Alun perin kun aloitin tämän työn tekemistä, ei budjetista ollut puhetta. Ensin oli tarkoitus tehdä suunnitelma, miten verkkoa voidaan parantaa, millä laitteilla ja miltä osin. Kun sitten sain suunnitelmat valmiiksi, jäi jäljelle vain päättää, mitä lähdetään hakemaan. Se, mikä näistä laitetilauksista tekee mielenkiintoisen, on se että osa laitteista oli jo tilattu aiemmin. Niitä ei siis suoranaisesti tarvinnut sitten lisätä tilauslistaan ja näin ollen kasvattaa budjettia.

Taulukko 4. Tilattavat laitteet, osa 1

Kuvaus	Osanumero	Kappalehinta ($)	Määrä	Yhteensä ($)
Keskuskytkimet	WS-C3750X-24T-S	6500	2	13000
4 x 1Gig SFP moduuli	C3K-X-NM-1G	500	2	1000
1000BaseT GBIC	GLC-SX-MM	500	10	5000
StackWise-kaapeli	CAB-STACK-3M	300	1	300
Kaappi2 + pieni kaappi	WS-C2960S-24TS-L	2995	3	8985
2960 FlexStack moduuli	FlexStack Moduuli	1500	2	3000
Listahinta yhteensä				31285 $

Listahinnat jouduin etsimään useista eri lähteistä, mutta jokaisen laitteen/lisäosan hinta oli sama riippumatta siitä, mikä kauppa oli kyseessä. Samalla kun jokaisessa kaupassa oli sama listahinta, myös jokainen kauppa myi tuotteita 54 %:n ”alennuksella”, eli todennäköisesti hinnoissa on ilmaa hyvin paljon, jos jokainen kauppa voi myydä noin paljon halvemmalla. Koska listahinnasta voi pudottaa 54 % pois, jää tuon laitelistauksen lopulliseksi hinnaksi noin €12000.

Taulukko 5. Tilattavat laitteet, osa 2

Kuvaus	Osanumero	Kappalehinta ($)	Määrä	Yhteensä ($)
Keskuskytkimet	WS-C3750X-24T-S	6500	2	13000
2 x 10Gig SFP-moduuli	C3K-X-NM-10G	2500	2	5000
10G SFP+ GBIC	SFP-10G-SR	1795	10	17950
StackWise-kaapeli	CAB-STACK-3M	300	1	300
Kaappi2 + pieni kaappi	WS-C2960S-24TS-L	3908	3	11724
2960 FlexStack-moduuli	FlexStack Module	1500	2	3000
Listahinta yhteensä ($)				50974 $

Verrattuna edelliseen listaukseen tämä laitelistaus sisältää 10 gigabitin ethernet-portit. Nämä portit tulisivat asennetuiksi keskuskytkimiin ja ne toimisivat sekä kuituyhteyksille että kytkinten välisille kuparikaapeleille. 10 gigabitin portit maksavat huomattavasti enemmän kuin gigabitin portit, mutta niiden avulla pystyttäisiin kasvattamaan verkon kapasiteettia sekä parantamaan laajennettavuutta. Päätös kuitenkin kallistui Philipsin puolelta halvempaan vaihtoehtoon. Laitteiden tilaukselle piti hakea erikseen sisäisesti hyväksyntä, mutta siihen ei koskaan saatu vastausta, onko tilaus hyväksytty vai ei. Tästä johtuen tämän opinnäytetyön käytännön osuus, eli laitteiden asennus ja konfigurointi, jäi lähes kokonaan toteutumatta.

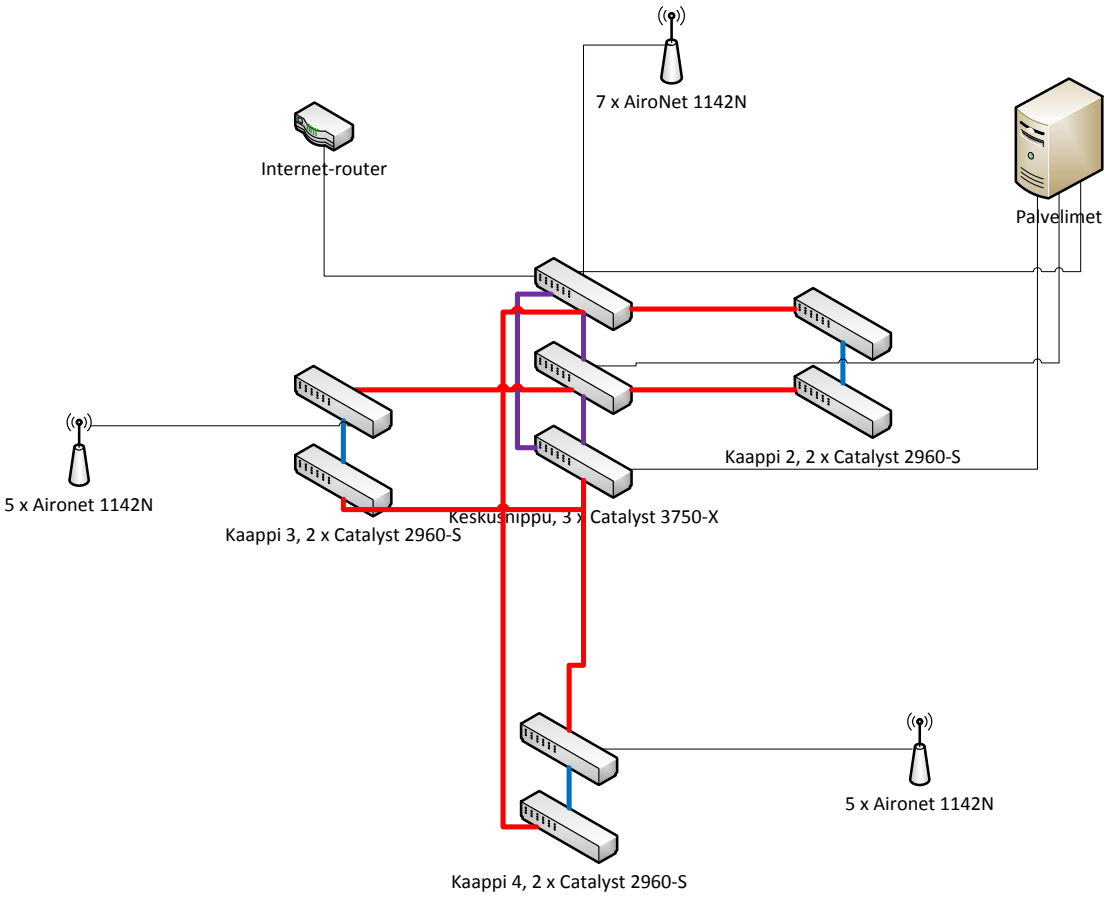
5 Tuleva verkon päivitys

Nykyinen verkko on auttamatta vanhentunut niin laitteiden, IP-osoitteiden määrän sekä konfiguraation muodossa. Uusi suunniteltu verkkotopologia ja IP-osoiteavaruus auttavat ongelmaan todella paljon, mutta siinä ei oteta huomioon sitä, mitä tapahtuu, jos tilat

kasvavat. Sitä varten pitää varautua ja suunnitella mahdollinen tuleva verkkotopologia, jonka avulla sitten laajentaminen on mahdollista.

5.1 Mahdollinen tuleva topologia

Koska ennustaminen on käytännössä mahdotonta, ei voida varmuudella sanoa, miten toimipisteessä tulee olemaan ihmisiä töissä tai miten sitä laajennetaan. Sitä myöten pitää myös tarkastella nykyistä verkkoa ja selventää, miten kyseistä verkkoa voidaan laajentaa mahdollisimman helposti.



Kuvio 12. Mahdollinen laajennettu topologia

Nykytilanteeseen verrattuna keskuskytkimiä on kolme kappaletta, ja jokainen sellaista mallia, että ne voidaan kytkeä toisiinsa StackWise-kaapeleilla, ja koska kytkimet ovat kaikki Catalyst 3750X-mallia, ne tukevat StackWise+-protokollaa. StackWise+-

protokolla ja -kaapelit ovat kuvassa merkitty violetin värisillä viivoilla. Edellä mainittujen protokollan ja kaapelien avulla keskuskytkinten välinen liikenne toimii 32 Gbps:n nopeudella.

Keskuskytkimistä lähtevät kuituyhteydet jokaiseen kolmeen nippuun niin, että jokaiseen nippuun menee kaksi kuitukaapelia. Näin saavutetaan nippujen välille vikasietoisuutta. Samalla saavutetaan 10 Gbps:n tiedonsiirtonopeus. Kuitukaapelit ovat kuvassa merkitty punaisilla viivoilla. Kaappien peruskytkimet, eli Catalyst 2960S:t, ovat nipussa kytkettyinä toisiinsa FlexStack-kaapeleilla, joiden nopeus voi olla jopa 20 Gbps. Reititin Internetin suuntaan on sitten kytkettynä ensimmäiseen keskusnipun kytkimeen. Samaan kytkimeen on myös kytkettyinä tukiasemia. Palvelimet kytketään keskusnipun toiseen ja kolmanteen kytkimeen siten, että jokainen palvelin saa kaksi kaapelia. Näin varmistetaan vikasietoisuus. Kahdessa peruskytkimen nipussa on myös sitten langattomat tukiasemat yhdistettyinä.

5.2 IP-osoiteavaruuden laajentaminen

Uusi suunniteltu IP-osoiteavaruus käsittää 512 IP-osoitetta eri verkkosegmenteissä. Tästä nousee pakostakin kysymys, onko tarpeen nostaa IP-osoiteavaruuden kokoa. Jos on, niin miten tästä sitten jatketaan? Yhdistetäänkö kahden eri toimipisteen IP-osoiteavaruudet ja samalla sitten verkot toisiinsa, jotta saadaan mahdollisimman paljon osoitteita käyttöön, vai mikä on se ratkaisu, jolla tämä tultaisiin tekemään? Tein verkkosuunnitelman, jossa jaetaan 1024 IP-osoitetta eri VLANeille. Koska jokaiseen toimipisteeseen on jaettu tietyn verran osoitteita, ja yksi toimipiste ollaan sulkemassa, vapautuvasta osoiteavaruudesta saataisiin toinen 512 osoitteen alue käyttöön ja yhdistettyä nykyiseen 512 osoitteen alueeseen.

Liitteessä 8 olevassa taulukossa on jaoteltu 1024 IP-osoitetta yhdeksään eri VLANiin. Sekä langallinen että langaton verkko, joiden IP-osoitteet jaetaan DHCP-palvelimen kautta, ovat molemmat saaneet 256 IP-osoitteen kokoisen verkon. Eli ne veisivät puolet koko verkon kapasiteetista. Tämä olisi enemmän kuin tarpeeksi kattamaan käyttö, sillä työntekijöitä on tällä hetkellä alle 200. Osalla on kuitenkin kannettavien tietokonei-

den lisäksi vielä pöytäkone(ita), joten useampi osoite saattaa mennä yhden henkilön käyttöön. Mutta sitten kun otetaan huomioon, miten ison virtuaalisen LANin esimerkiksi staattiset sekä sisäiset osoitteet muodostavat, ja osalla työntekijöistä on jompaankumpaan tai jopa molempiin VLAN:ihin kuuluvia koneita, vie se käyttöä pois DHCP:n jakamilta osoitteilta. Eli suoraan ei pysty toteamaan, miten paljon osoitteita menee mistäkin verkosta. Staattiset ja sisäiset osoitteet vievät molemmat tämän hetken suunnitelmassa 64 osoitetta, mutta niissä on optio, jolla ne voidaan laajentaa käyttämään 128 osoitetta kumpainenkin. Ne vievät näin yhden 256 osoitteen verkon. Edelleen jäisi 256 osoitetta verkkolaitteiden, palvelinten sekä tulostinten käyttöön. Tämä verkko on iso ja sen pitäisi kestää hyvinkin ison käyttäjämäärän nousun (liite 8).

6 Yhteenveto

Tässä työssä oli monta eri kohdetta verkon parantamiseksi. Yksi päämääristä oli päivittää verkon laitteisto. Vaihdon kohteina olivat niin langattomat tukiasemat kuin kytkimetkin. Samalla piti myös kartoittaa, mihin kaikkialle langattomia tukiasemia oli asennettu. Kartta, joka näytti, mihin pistorasiat ja lähiverkkorasiat oli asennettu, oli hukkunut, joten siitä piti tehdä uusi versio. Tähän uuteen karttaan sitten lisäsin myös langattomien tukiasemien paikat. Toinen päämäärä oli luoda verkkoon erilliset virtuaaliset lähiverkot, jotta verkkoon saataisiin vikasietoisuutta mahdollisia tietomyrskyjä varten. Tätä varten, tai tästä johtuen myös IP-osoiteavaruudet piti suunnitella uusiksi. Kolmas päämäärä oli suunnitella verkolle uusi topologia, joka toimisi mahdollisimman hyvin yhteen jo olemassa olleen verkon sekä kaapeloinnin kanssa.

Suunnittelin yhteensä kuusi erilaista mahdollista tapaa jakaa IP-osoiteavaruus, joista tulevaisuutta ajatellen yksi oli 1024 osoitteen verkko, mikäli laajentamiselle olisi tarvetta. Viisi muuta suunnitelmaa oli tarkoitettu nykyisen verkon päivitysvaihtoehdoiksi. Käsittelin näistä viidestä kolme, sillä kahden muun vaihtoehdon eroavaisuudet olivat hyvin pieniä. Tässä työssä käsittelin myös sitä, miten paljon ja missä järjestyksessä virtuaalisiin lähiverkkoihin IP-osoitteet olisi jaettu. Tämän lisäksi suunnittelin myös kaksi erilaista topologiaa, joista toinen oli tarkoitettu olemassa olevan verkon korvaajaksi ja toinen tulevaisuutta varten. Kävin läpi myös erilaisia verkkolaitteissa olevia mielenkiintoisimpia komentoja, sekä verkkotekniikoita, joita tarvitaan nykyaikaisen verkon pystyttämiseksi ja ylläpitämiseksi. Nämä verkkotekniikat kävin läpi joiltain osin yksityiskohtaisemmin (kuten esimerkiksi IPv4) ja joiltain osin vain raapaisin pintaa (esimerkkinä MAC-osoite). Käytännön osuudessa ehdin vaihtaa ja konfiguroida kolme tukiasemaa, sekä liittää ja konfiguroida yhden kytkimen verkkoon. Loput laitteet liitetään toivottavasti verkkoon vielä samoilla konfiguraatioilla.

Vaikka käytännön osuutta en saanutkaan suoritettua loppuun asti syystä, että en saanut tarvittavia verkkolaitteita hyväksynnän puutteen takia, enkä näe, että työ itsessään olisi epäonnistunut tai ollut turhaa. Tätä opinnäytetyötä tehdessä tulin kerranneeksi jo opiskeltuja asioita niin verkkotekniikoista kuin verkkolaitteiden komennoistakin. Myös

uusia asioita tuli opittua Ciscon laitteiden komennoista. Sain tästä työstä myös hyvää kokemusta topologian suunnittelusta, sillä huonosti suunniteltu topologia voi pahimmassa tapauksessa ruuhkauttaa koko verkon ja aiheuttaa näin isoja katkoksia tietoliikenteeseen. Uskon, että näistä kerratuista asioista Philipsin toimipiste voi kuitenkin käyttää suunnitelmiani tulevaisuudessa joko suoraan, tai sitten pohjana omalle versiolleen. Ei myöskään ole pois suljettuna vaihtoehto, että käytän suunnitelmiani jonkin toisen yrityksen verkon kehittämisprojektissa muokattuna heidän verkkoonsa sopivaksi.

Lähteet

1 Historia. Verkkodokumentti. Philips. <http://www.philips.fi/about /company/history/ourheritage/index.page> Luettu 3.1.2013.

2 Tuotteet. Verkkosivu. Philips. <http://www.philips.fi/c/> Luettu 10.1.2013.

3 MAC-osoite. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /MAC_address> Luettu 16.4.2013.

4 OUI. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Organizationally_unique_identifier> Luettu 10.1.2013.

5 IPv4. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IPv4> Luettu 3.2.2013.

6 Reserved IPv4 addresses. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Reserved_IP_addresses#Reserved_IPv4_addresses> Luettu 3.2.2013.

7 Subnetwork. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Subnetwork#> Luettu 3.2.2013.

8 IPv4 Subnetting. Verkkodokumetti. Wikipedia. <http://en.wikipedia.org /wiki/Subnetwork#IPv4_subnetting> Luettu 3.2.2013.

9 IPv6. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IPv6> Luettu 10.2.2013.

10 IPv6 address presentation. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IPv6_address#Presentation> Luettu 10.2.2013.

11 IPv6 address classes. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IPv6_address#IPv6_address_classes> Luettu 10.2.2013.

12 IPv6 subnetting. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org /wiki/Subnetwork#IPv6_subnetting> Luettu 10.2.2013.

13 Osoitteenmuunnos. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org /wiki/Osoitteenmuunnos> 19.2.2013.

14 DHCP. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Dynamic_Host_Configuration_Protocol> Luettu 15.2.2013.

15 LAN. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Local_area_network> Luettu 20.3.2013.

16 StarLAN. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /StarLAN> Luettu 20.3.2013.

17 10 Gbps Ethernet. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org /wiki/10-gigabit_Ethernet> Luettu 21.3.2013.

18 Optical fiber. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org /wiki/Optical_fiber> Luettu 21.3.2013.

19 Ethernet over twisted pair variants. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/Ethernet_over_twisted_pair#Variants > Luettu 21.3.2013.

20 Twisted pair. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Twisted_pair> Luettu 21.3.2013.

21 IEEE 802.3. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /IEEE_802.3> Luettu 21.3.2013.

22 Wireless LAN. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org /wiki/Wireless_LAN> Luettu 23.3.2013.

23 Wireless LAN types. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Wireless_LAN#Types_of_wireless_LANs> Luettu 23.3.2013.

24 IEEE 802.11n. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org /wiki/IEEE_802.11n-2009> Luettu 23.3.2013.

25 Virtual LAN. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Virtual_LAN> Luettu 30.3.2013.

26 Cisco Catalyst 2960-S FlexStack. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406 /white_paper_c11-578928.html> Luettu 17.3.2013.

27 Cisco StackWise & StackWise+ Technology. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023 /prod_white_paper09186a00801b096a.html> Luettu 19.2.2013.

28 EtherChannel. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org /wiki/Etherchannel> Luettu 15.2.2013.

29 PAgP. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki /Port_Aggregation_Protocol> Luettu 15.2.2013.

30 Aironet 1121G Data Sheet. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps4570/ps4 612/product_data_sheet09186a00800f9ea7_ps4570_Products_Data_Sh eet.html> Luettu 9.4.2013.

31 Baseline Switch 2250 Plus User Guide. Verkkodokumentti. HP. <http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02581 571/c02581571.pdf> Luettu 7.4.2013.

32 HP ProVurve 2510G-24. Verkkodokumentti. HP. <http://h10010.www1.hp.com/wwpc/il/en/sm/WF06b/12883-12883-3445275-427605-427605-3356807-3757516.html?dnr=1> Luettu 9.4.2013.

33 Cisco Catalyst 3750 Data Sheet. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.html> Luettu 9.4.2013.

34 Cisco Catalyst 2950 Series Switches with Enhanced Image SW. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps628/product_data_sheet09186a00801cfb64.html> Luettu 8.4.2013.

35 Cisco Aironet 1140 Series Access Point Data Sheet. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/datasheet_c78-502793.html> Luettu 9.4.2013.

36 Cisco Catalyst 3750-X and 3560-X Series Switches Data Sheet. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/data_sheet_c78-584733.html> Luettu 10.4.2013.

37 Cisco Catalyst 2960-S Series Switches Data Sheet. Verkkodokumentti. Cisco. <www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12200/data_sheet_c78-726680.html> Luettu 10.4.2013.

Luettelo olemassa olevan verkon laitteista

Tehtävä	Merkki	Malli	Tyyppi	IP-osoite
Reititys Internetin ja toimiston verkon välillä	Cisco	2811	Reititin	192.168.0.1
Keskuskytkin	Cisco	3750G, 12-porttinen	Kytkin	192.168.0.250
Keskuskytkin	Cisco	3750G, 24-porttinen	Kytkin	192.168.0.250
Verkon liityntäpiste	Cisco	2960S	Kytkin	192.168.0.246
Verkon liityntäpiste	Cisco	2950G	Kytkin	192.168.0.247
	Cisco	1720	Kytkin	
Verkon liityntäpiste	Cisco	1142N	WLAN-tukiasema1	192.168.1.240
Verkon liityntäpiste	Cisco	1142N	WLAN-tukiasema2	192.168.1.241
Verkon liityntäpiste	Cisco	1142N	WLAN-tukiasema3	192.168.1.242
Verkon liityntäpiste	Cisco	1121G	WLAN-tukiasema4	192.168.1.243
Verkon liityntäpiste	Cisco	1121G	WLAN-tukiasema5	192.168.1.231
Verkon liityntäpiste	Cisco	1121G	WLAN-tukiasema6	192.168.1.232
Verkon liityntäpiste	Cisco	1121G	WLAN-tukiasema7	192.168.1.233
Verkon liityntäpiste	Cisco	1142N	WLAN-tukiasema8	192.168.1.252
Verkon liityntäpiste	Cisco	1142N	WLAN-tukiasema9	192.168.1.244

Verkon liityntä-piste	Cisco	1142N	WLAN-tukiasema10	192.168.1.245
Verkon liityntä-piste	Dell	2748	Kytkin	-
Verkon liityntä-piste	Dell	6224	Kytkin	-
Verkon liityntä-piste	Dell	6224	Kytkin	-
Verkon liityntä-piste	Dell	6248	Kytkin	-
Verkon liityntä-piste	Dell	6248	Kytkin	-
Verkon liityntä-piste	Dell	2724	Kytkin	-
Verkon liityntä-piste	HP	ProCurve 2510g-24	Kytkin	-
Verkon liityntä-piste	3Com	Baseline switch 2250	Kytkin	-

Langattoman tukiaseman konfiguraatio

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname langaton_tukiasema_1
!
logging rate-limit console 9
enable secret 5 salasana_tähän
!
aaa new-model
!
aaa group server radius rad_eap
 server ip_osoite1 auth-port <port> acct-port <port>
 server ip_osoite2 auth-port <port> acct-port <port>
 server ip_osoite3 auth-port <port> acct-port <port>
!
aaa group server radius rad_acct
 server ip_osoite1 auth-port <port> acct-port <port>
```

```
 server ip_osoite2 auth-port <port> acct-port <port>
 server ip_osoite3 auth-port <port> acct-port <port>
!
aaa group server radius nimi_tähän
 server ip_osoite1 auth-port <port> acct-port <port>
 server ip_osoite2 auth-port <port> acct-port <port>
 server ip_osoite3 auth-port <port> acct-port <port>
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login tunnus_tähän group nimi_tähän
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
clock timezone +0200 2
ip domain name domain_nimi_tähän
ip name-server ip_osoite1_tähän
ip name-server ip_osoite2_tähän
ip name-server ip_osoite3_tähän
!
```

```
dot11 mbssid
dot11 syslog
dot11 vlan-name vlanin1_nimi_tähän
dot11 vlan-name vlanin2_nimi_tähän
!
dot11 ssid nimi_tähän
   vlan yyy
   authentication open eap eap_methods
   authentication network-eap eap_methods
   mbssid guest-mode
!
dot11 ssid nimi_tähän
   vlan xxx
   authentication open
   authentication key-management wpa
   mbssid guest-mode
   wpa-psk ascii 7 salsana_tähän
!
username käyttäjätunnus1_tähän privilege 15 password 7 salasana_tähän
username käyttäjätunnus2_tähän privilege 15 password 7 salasana_tähän
username käyttäjätunnus3_tähän password 7 salasana_tähän
username käyttäjätunnus4_tähän privilege 15 password 7 salasana_tähän
```

```
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan yyy mode ciphers tkip
 !
 encryption vlan xxx mode wep mandatory
 !
 broadcast-key change 300
 !
 ssid nimi_tähän
 !
 ssid nimi2_tähän
 !
 antenna gain 0
 speed  basic-1.0 basic-2.0 basic-5.5 basic-11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root fallback shutdown
 rts threshold 2312
 no dot11 extension aironet
```

```
 no cdp enable
!
interface Dot11Radio0.xxx
 encapsulation dot1Q xxx native
 no ip route-cache
 no cdp enable
 bridge-group xxx
 bridge-group xxx subscriber-loop-control
 bridge-group xxx block-unknown-source
 no bridge-group xxx source-learning
 no bridge-group xxx unicast-flooding
 bridge-group xxx spanning-disabled
!
interface Dot11Radio0.yyy
 encapsulation dot1Q yyy
 no ip route-cache
 no cdp enable
 bridge-group yyy
 bridge-group yyy subscriber-loop-control
 bridge-group yyy block-unknown-source
 no bridge-group yyy source-learning
 no bridge-group yyy unicast-flooding
```

```
 bridge-group yyy spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 no dfs band block
 channel dfs
 station-role root
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 no keepalive
!
interface GigabitEthernet0.xxx
 encapsulation dot1Q xxx native
 no ip route-cache
 bridge-group xxx
```

```
 no bridge-group xxx source-learning
 bridge-group xxx spanning-disabled
!
interface GigabitEthernet0.yyy
 encapsulation dot1Q yyy
 no ip route-cache
 no cdp enable
 bridge-group yyy
 no bridge-group yyy source-learning
 bridge-group yyy spanning-disabled
!
interface BVI1
 ip address ip_osoite aliverkon_peite
 no ip route-cache
!
ip default-gateway ip_osoite
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
logging trap warnings
```

snmp-server community tekstijono1_tähän

snmp-server community tekstijono2_tähän

snmp-server location tekstijono3_tähän

snmp-server contact tekstijono4_tähän

snmp-server chassis-id tekstijono5_tähän

snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

snmp-server enable traps tty

snmp-server enable traps entity

snmp-server enable traps disassociate

snmp-server enable traps deauthenticate

snmp-server enable traps authenticate-fail

snmp-server enable traps dot11-qos

snmp-server enable traps switch-over

snmp-server enable traps rogue-ap

snmp-server enable traps wlan-wep

snmp-server enable traps config

snmp-server enable traps syslog

snmp-server enable traps aaa_server

radius-server attribute 32 include-in-access-req format %h

radius-server host ip_osoite auth-port <portti> acct-port <portti> key 7 salasana_tähän

radius-server host ip_osoite auth-port <portti> acct-port <portti> key 7 salasana_tähän

radius-server host ip-osoite_tähän auth-port <portti> acct-port <portti> key 7 salasana_tähän

```
radius-server deadtime 15

radius-server vsa send accounting

bridge 1 route ip

!

line con 0

 exec-timeout 120 0

line vty 0 4

 access-class 20 in

!

sntp server ip_osoite_tähän
```

Catalyst 2960S:n konfiguraatio

Current configuration : xxxx bytes

!

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname kytkimen_nimi

!

boot-start-marker

boot-end-marker

!

enable secret 5 salasana_tähän

!

username käyttäjätunnus_tähän privilege 15 password 0 salasana_tähän

username käyttäjätunnus2_tähän privilege 15 password 7 salasana2_tähän

!

aaa new-model

!

```
aaa session-id common
clock timezone UTC 2
clock summer-time UTC recurring last Sun Mar 3:00 last Sun Oct 4:00
!
vtp domain nimi_tähän
vtp mode transparent
!
crypto pki trustpoint PKI-nimi_tähän
 enrollment selfsigned
 subject-name cn=sertifikaatin_nimi_tähän
 revocation-check none
 rsakeypair PKI-nimi_tähän
!
crypto pki certificate chain PKI-nimi_tähän
 certificate self-signed 01
RSA-avain_tähän
  quit
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree uplinkfast
spanning-tree vlan x-xxx priority 8192
```

```
!
vlan internal allocation policy ascending
!
vlan yyy
 name nimi_tähän
!
interface Port-channelXX
 description Port-channelXX to Core stack
 switchport mode trunk
 storm-control broadcast level 0.50
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/2
 switchport mode access
 storm-control broadcast level 0.50
!
```

```
interface GigabitEthernet1/0/3
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/4
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/5
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/6
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/7
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/8
 switchport mode access
```

```
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/9
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/10
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/11
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/12
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/13
 switchport mode access
 storm-control broadcast level 0.50
!
```

```
interface GigabitEthernet1/0/14
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/15
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/16
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/17
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/18
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/19
 switchport mode access
```

```
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/20
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/21
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/22
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/23
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/24
 switchport mode access
 storm-control broadcast level 0.50
!
```

```
interface GigabitEthernet1/0/25
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/26
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/27
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/28
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/29
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/30
 switchport mode access
```

```
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/31
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/32
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/33
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/34
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/35
 switchport mode access
 storm-control broadcast level 0.50
!
```

```
interface GigabitEthernet1/0/36
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/37
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/38
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/39
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/40
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/41
 switchport mode access
```

```
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/42
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/43
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/44
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/45
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/46
 switchport mode access
 storm-control broadcast level 0.50
!
```

```
interface GigabitEthernet1/0/47
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/48
 switchport mode access
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
 switchport mode trunk
 storm-control broadcast level 0.50
 channel-group XX mode on
!
interface GigabitEthernet1/0/52
 switchport mode trunk
 storm-control broadcast level 0.50
 channel-group XX mode on
!
```

```
interface VlanXXX
 ip address ip_osoite_tähän aliverkon_peite_tähän
!
ip default-gateway gateway_tähän
ip http server
ip http secure-server
ip sla enable reaction-alerts
logging trap debugging
logging palvelimen_IP-osoite_tähän
snmp-server community tieto_tähän
snmp-server contact tieto_tähän
snmp-server enable traps snmp authentication warmstart
snmp-server enable traps tty
snmp-server enable traps license
snmp-server enable traps config
banner motd ^C
**********************************************************************
**                                                                  **
**              Access to this  IT System is for authorised users only              **
**                                                                  **
**    Unauthorised access contravenes the Computer Misuse Act 1990 and may    **
**                  incur criminal or civil penalties including damages             **
```

```
**                                                                  **
**          Please log out immediately if you are not an authorised user          **
**                                                                  **
**********************************************************************
^C
!
line con 0
line vty 5 15
logging synchronous
!
ntp clock-period 22518657
ntp server palvelimen_IP-osoite_tähän
end
```

Keskusnipun konfiguraatio

Current configuration : xxxx bytes

!

! No configuration change since last restart

! NVRAM config last updated at 01:57:53 UTC Wed Mar 27 2013 by user

!

version 12.2

no service pad

service timestamps debug datetime localtime show-timezone

service timestamps log datetime localtime show-timezone

service password-encryption

!

hostname laitteen_nimi

!

boot-start-marker

boot-end-marker

!

logging buffered 16384

enable secret 5 salasana_tähän

!

username käyttäjätunnus privilege 15 password 7 salasana

username käyttäjätunnus2 privilege 15 password 7 salasana

!

no aaa new-model

clock timezone UTC 2

clock summer-time UTC recurring last Sun Mar 3:00 last Sun Oct 4:00

switch 1 provision kytkin1

switch 2 provision kytkin2

system mtu routing 1500

vtp domain domainin_nimi_tähän

vtp mode transparent

ip routing

ip cef load-sharing algorithm universal tunnus_tähän

no ip domain-lookup

ip domain-name domain_nimi

ip name-server nimipalvelimen_osoite

!

ip multicast-routing distributed

!

mls qos map cos-dscp 0 10 18 26 34 46 48 56

mls qos

!

errdisable recovery cause udld

```
archive
 log config
  logging enable
  logging size 250
  hidekeys
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-1000 priority 4096
!
vlan internal allocation policy ascending
!
vlan yyy
 name nimi_tähän
!
ip ssh version 2
!
interface Port-channel1
 description kuvaus_tähän
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 logging event bundle-status
 storm-control broadcast level 0.50
!
interface Port-channel2
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/2
 description kuvaus_tähän
```

```
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/3
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/4
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/5
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/6
 description testi_yhteys
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 storm-control broadcast level 0.50
 channel-protocol lacp
 channel-group 1 mode active
 spanning-tree bpduguard disable
!
interface GigabitEthernet1/0/7
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/8
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/9
 switchport access vlan yyy
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/10
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 channel-group 3 mode on
!
interface GigabitEthernet1/0/11
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport mode trunk
 storm-control broadcast level 0.50
!
interface GigabitEthernet1/0/12
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode on
!
interface GigabitEthernet2/0/1
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet2/0/2
 description kuvaus_tähän
```

```
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
 spanning-tree bpduguard disable
!
interface GigabitEthernet2/0/3
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet2/0/4
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
 spanning-tree bpduguard disable
!
interface GigabitEthernet2/0/5
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet2/0/6
 description kuvaus_tähän
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 storm-control broadcast level 0.50
 channel-protocol lacp
 channel-group 1 mode active
 spanning-tree portfast trunk
 spanning-tree bpduguard disable
!
interface GigabitEthernet2/0/7
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet2/0/8
 description kuvaus_tähän
 switchport mode dynamic desirable
 storm-control broadcast level 0.50
!
interface GigabitEthernet2/0/9
 description kuvaus_tähän
 switchport access vlan yyy
 switchport mode access
```

```
 storm-control broadcast level 0.50
 spanning-tree bpduguard disable
!
interface GigabitEthernet2/0/10
 description kuvaus_tähän
 switchport mode access
 ip access-group nimi_tähän in
 storm-control broadcast level 0.50
 spanning-tree bpduguard disable
!
interface GigabitEthernet2/0/11
 switchport access vlan yyy
 switchport mode access
 storm-control broadcast level 0.50
 spanning-tree portfast
!
interface GigabitEthernet2/0/12
 switchport mode access
 storm-control broadcast level 0.50
 spanning-tree portfast
!
interface GigabitEthernet2/0/13
```

```
 switchport mode access
 storm-control broadcast level 0.50
 spanning-tree portfast
!
interface GigabitEthernet2/0/14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/15
 description kuvaus_tähän
 switchport mode access
 speed 100
 duplex full
 storm-control broadcast level 0.50
 spanning-tree portfast
 spanning-tree bpduguard disable
!
interface GigabitEthernet2/0/16
 switchport mode access
```

```
 storm-control broadcast level 0.50
 spanning-tree portfast
!
interface GigabitEthernet2/0/17
 switchport mode access
 storm-control broadcast level 0.50
 spanning-tree portfast
!
interface GigabitEthernet2/0/18
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/19
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
```

```
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/20
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/21
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/22
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
```

```
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/23
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/24
 description kuvaus_tähän
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan xxx,yyy
 switchport mode trunk
 storm-control broadcast level 0.50
 spanning-tree portfast
!
interface GigabitEthernet2/0/25
!
```

```
interface GigabitEthernet2/0/26
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode on
!
interface GigabitEthernet2/0/27
 switchport trunk encapsulation dot1q
 switchport mode trunk
 shutdown
!
interface GigabitEthernet2/0/28
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode on
!
interface Vlanxxx
 ip address ip_osoite aliverkon_peite
 ip helper-address ip_osoite
 ip helper-address ip_osoite
!
interface Vlanyyy
 no ip address
```

```
 shutdown
!
ip default-gateway ip_osoite
ip classless
ip route ip_osoite aliverkon_peite ip_osoite
no ip http server
no ip http secure-server
!
ip access-list extended ryhmän_nimi
 deny ip any host ip_osoite
 remark *** Block all access to specific hosts ***
 deny tcp any host ip_osoite eq 3389
 permit ip any any
!
ip sla enable reaction-alerts
logging ip_osoite
snmp-server community tekstijono_tähän RO
snmp-server location tekstijono_tähän
snmp-server contact tekstijono_tähän
!
banner motd ^C
**********WARNING**********
```

```
This system is NOT FOR PUBLIC USE.

Unauthorized access or use is subject to

DISCIPLINE, CRIMINAL, and/or CIVIL SANCTIONS.

All users consent to MONITORING.

******************WARNING******************^C

privilege exec level 2 enable

privilege exec level 14 sho run

privilege exec level 14 sho conf

!

line con 0

 exec-timeout 15 0

 password 7 salasana_tähän

line vty 0 4

 exec-timeout 15 0

 password 7 salasana_tähän

 login local

 transport input ssh

line vty 5 15

 login local

 transport input ssh

!

ntp clock-period 36029772
```

```
ntp server ip_osoite

end
```

Ensimmäinen ehdotus verkon IP-osoiteavaruudesta

Tarkoitus	VLAN-tunnus	IP-osoitteet	VLAN:n yhdyskäytävän osoite	Aliverkon peite	Verkon koko
Transit (Internet)	2	192.168.0.0 – 3	192.168.1.2	255.255.255.252	Yhteensä 8 IP-osoitetta.
	-	192.168.1.0 – 3	-	-	
Käyttämätön	-	192.168.0.4 – 15	-	-	Yhteensä 24 IP-osoitetta.
	-	192.168.1.4 – 15	-	-	
Verkkolaitteet	3	192.168.0.16 – 31	192.168.0.30	255.255.255.240	Yhteensä 32 IP-osoitetta.
	33	192.168.1.16 – 31	192.168.1.30	255.255.255.240	
Tulostimet	4	192.168.0.32 – 47	192.168.0.46	255.255.255.240	Yhteensä 32 IP-osoitetta.
	44	192.168.1.32 – 47	192.168.1.46	255.255.255.240	
Palvelimet	5	192.168.0.48 – 63	192.168.0.62	255.255.255.240	Yhteensä 32 IP-osoitetta.
	55	192.168.1.48 – 63	192.168.1.62	255.255.255.240	
DHCP	6	192.168.0.64 – 127	192.168.0.126	255.255.255.192	Yhteensä 128 IP-osoitetta.
	66	192.168.1.64 – 127	192.168.1.126	255.255.255.192	
Ei Internet-yhteyttä	7	192.168.0.128 – 159	192.168.0.158	255.255.255.224	Yhteensä 64 IP-osoitetta.
	77	192.168.1.128 – 159	192.168.1.158	255.255.255.224	
Staattiset osoitteet	8	192.168.0.160 – 191	192.168.0.190	255.255.255.224	Yhteensä 64 IP-osoitetta.
	88	192.168.1.160 – 191	192.168.0.190	255.255.255.224	
Käyttämätön	-	192.168.0.192 – 255	-	-	Yhteensä 128 IP-osoitetta.
	-	192.168.1.192 – 255	-	-	

Toinen ehdotus verkon IP-osoiteavaruudesta.

Tarkoitus	VLAN-tunnus	IP-osoitteet	WLAN:in yhdyskäytävän osoite	Aliverkon peite	Verkon koko
Transit	2	192.168.0.0 – 7	192.168.0.6	255.255.255.252	Yhteensä 8 IP-osoitetta.
Käyttämätön	-	192.168.0.8 – 31	-	-	Yhteensä 24 IP-osoitetta.
Verkkolaitteet	3	192.168.0.32 – 63	192.168.0.62	255.255.255.224	Yhteensä 32 IP-osoitetta.
Tulostimet	4	192.168.0.64 – 95	192.168.0.94	255.255.255.224	Yhteensä 32 IP-osoitetta.
Palvelimet	5	192.168.0.96 – 127	192.168.0.126	255.255.255.224	Yhteensä 32 IP-osoitetta.
Staattiset osoitteet	6	192.168.0.128 – 191	192.168.0.190	255.255.255.192	Yhteensä 64 IP-osoitetta.
Ei Internet-yhteyttä	7	192.168.0.192 – 255	192.168.0.254	255.255.255.192	Yhteensä 64 IP-osoitetta.
LANia käyttävät, DHCP	8	192.168.1.0 – 127	192.168.1.126	255.255.255.128	Yhteensä 128 IP-osoitetta.
WLANia käyttävät, DHCP	9	192.168.1.128 – 255	192.168.1.254	255.255.255.128	Yhteensä 128 IP-osoitetta.

Kolmas ehdotus verkon IP-osoiteavaruudesta.

Tarkoitus	VLAN-tunnus	IP-osoitteet	VLANin yhdyskäytävän osoite	Aliverkon peite	Verkon koko
Transit	2	192.168.0.0 – 7	192.168.0.6	255.255.255.252	Yhteensä 8 IP-osoitetta
Käyttämätön	-	192.168.0.8 – 31	-	-	Yhteensä 24 IP-osoitetta.
Verkkolaitteet	3	192.168.0.32 – 63	192.168.0.62	255.255.255.224	Yhteensä 32 IP-osoitetta.
Palvelimet, tulostimet ja ei pääsyä Internetiin	4	192.168.0.64 – 127	192.168.0.126	255.255.255.192	Yhteensä 64 IP-osoitetta.
WLAN-käyttäjät	5	192.168.0.128 – 255	192.168.0.254	255.255.255.128	Yhteensä 128 IP-osoitetta.
LAN-käyttäjät sekä staattiset osoitteet	6	192.168.1.0 – 255	192.168.1.254	255.255.255.0	Yhteensä 256 IP-osoitetta.

Ehdotus laajennetun osoiteavaruuden jakamiseksi

Tarkoitus	VLAN	IP-osoitteet	VLANin yhdyskäytävän osoite	Aliverkon peite	VLANin koko (osoitetta)
Transit	2	192.168.0.0 – 7	192.168.0.6	255.255.255.248	8
Käyttämätön	-	192.168.0.8 – 31	-	-	24
Verkkolaitteet	3	192.168.0.32 – 63	192.168.0.62	255.255.255.224	32
Käyttämätön	-	192.168.0.64 – 95	-	-	32
Tulostimet	4	192.168.0.96 – 127	192.168.0.126	255.255.255.224	32
Palvelimet	5	192.168.0.128 – 191	192.168.0.190	255.255.255.192	64
Käyttämätön	-	192.168.0.192 – 255	-	-	64
Staattiset osoitteet	6	192.168.1.0 – 63	192.168.0.62	255.255.255.192	64
Käyttämätön	-	192.168.1.64 – 127	-	-	64
Sisäinen käyttö	7	192.168.1.128 – 191	192.168.1.190	255.255.255.192	64
Käyttämätön	-	192.168.1.192 – 255	-	-	64
Langattoman verkon käyttäjät / DHCP	8	192.168.2.0 – 255	192.168.2.254	255.255.255.0	256
Langallisen verkon käyttäjät / DHCP	9	192.168.3.0 – 255	192.168.3.254	255.255.255.0	256