OULUN AMMATTIKORKEAKOULU

Ari-Pekka Visuri

ORGANISAATION LANGATTOMAN VERKON SUUNNITTELU JA TOTEUTUS

ORGANISAATION LANGATTOMAN VERKON SUUNNITTELU JA TOTEUTUS

Ari-Pekka Visuri
Opinnäytetyö
Syksy 2016
Tietotekniikan koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Tekijä: Ari-Pekka Visuri
Opinnäytetyön nimi: Organisaation langattoman verkon suunnittelu ja toteutus
Työn ohjaaja: Teemu Korpela
Työn valmistumislukukausi ja -vuosi: Syksy 2016 Sivumäärä: 35 + 2 liitettä

Opinnäytetyön aiheena oli suunnitella ja toteuttaa langaton lähiverkko Pyhäjärven terveyskeskukseen. työn tilaajana toimi Pyhäjärven kaupunki sekä PyhäNet Oy. Työn tavoitteena oli toteuttaa laadukas, turvallinen ja helposti hallittava langaton lähiverkko terveyskeskuksen sisäiseen käyttöön.

Työ aloitettiin tutustumalla kohteen pohjapiirustuksiin sekä tietoliikennekaapelointi suunnitelmiin ja tekemällä alustavia suunnitelmia tukiasemien sijoittelusta. Ensimmäinen kohdekäynti toteutettiin maaliskuussa ja kuuluvuusmittaukset tehtiin toukokuussa. Laitevalintojen ja kilpailutuksen jälkeen laitteet tilattiin, asennettiin paikalleen ja tehtiin tarvittava konfiguraatio. Testauksen jälkeen verkko luovutettiin tuotantoon.

Työ saatiin valmiiksi määräpäivään mennessä ja verkko tuotantoon. Työ loi pohjan tulevaisuudessa tapahtuville tietoliikennemuutoksille yrityksessä sekä parantaa dokumentointi käytäntöjä. Verkon valvonta, ylläpito ja kehitys jatkuu. Tarvittavia muutoksia tehdään asiakkaan toiveiden perusteella.

Asiasanat: tietoliikenne, langaton lähiverkko, WLAN

ABSTRACT

Oulu University of Applied Sciences
Degree programme in Information Technology

Author: Ari-Pekka Visuri
Title of thesis: Enterprise wireless network desing and implementation
Supervisor: Teemu Korpela
Term and year when the thesis was submitted: Autumn 2016 Pages: 35 + 2 appendices

---

The subject of this thesis was to desing and implement a wireless local area network for Pyhäjärvi health center. The work was assigned by the City of Pyhäjärvi and PyhäNet Ltd. Main goal was to implement enterprise level wireless network which is secure and easy to maintain.

At February first thing in this project was to research floor and cable plans. We had to add some extra cabling for the wireless access points. First visit to the site was in March when construction was still far from complete. Cabling was done by electricians in June and then we had time to do coverage measurements. According to those results active device selections were made. Devices were installed and configured a couple of weeks before the deadline.

The assignment was completed just before the due date and the network is in production. This thesis laid foundation to do similar projects in the future. Network maintenance, monitoring and further development will continue. One big thing to look in the future is security and how to improve especially network security but also physical security.

Keywords: network, wireless, LAN, telecommunications

SISÄLLYS

SANASTO

AES	Advanced Encryption Standard, lohkosalausmenetelmä.
AP	Access Point, laite, jonka kautta liitytään verkkoon.
ARP	Address Resolution Protocol, protokolla, jolla selvitetään IP-osoitetta vastaava MAC-osoite.
CCMP	Counter mode CBC-MAC Protocol, langattoman verkon salausprotokolla
DHCP	Dynamic Host Control Protocol, automatisoitu verkkoasetusten jako.
DMZ	Demilitarized Zone, verkkoalue, johon sijoitetaan laitteet, jotka palvelevat myös ulkoverkosta tulevia käyttäjiä.
EAPOL	Extensible Authentication Protocol over LAN, paketointitekniikka, jolla kuljetetaan 802.1X-protokollan viestit.
GW	Gateway, yhdyskäytävä.
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö, joka muun muassa määrittelee alan keskeisiä standardeja.
LACP	Link Aggregation Control Protocol, linkkiaggrekaation ohjausprotokolla.
LAG	Link Aggregation Group, linkkiaggrekaatioryhmä.
LAN	Local Area Network, tietoliikenneverkko, joka toimii rajoitetulla alueella.
MAC	Media Access Control, laitteen fyysinen yksilöllinen osoite.
MIC	Message Integrity Check, pakettien eheyden valvonta.

MIMO	Multiple-input and Multiple-output, tekniikka, jolla sekä lähettämiseen että vastaanottamiseen käytetään useampaa antennia.
MPLS	Multiprotocol Label Switching, menetelmä, jolla kuljetetaan IP-paketteja runkoverkossa ilman, että solmujen täytyy tehdä reititystä.
NDP	Neighbor Discovery Protocol, protokolla verkossa olevien laitteiden tunnistukseen.
PoE	Power over Ethernet, tekniikka käyttöjännitteen siirtoon samassa verkkokaapelissa datan kanssa.
PVLAN	Private VLAN, samalla yleislähetysalueella olevien porttien eristäminen.
SFP	Small Form-factor Pluggable, valokuidun kanssa käytettävä lähetin-vastaanotinmoduuli.
SNMP	Simple Network Management Procotol, verkon ylläpitoon ja valvontaan käytettävä protokolla.
TKIP	Temporal Key Integrity Protocol, langattoman verkon salausprotokolla.
UTP	Unshielded Twisted Pair, suojaamaton parikaapeli.
VLAN	Virtual Local Area Network, looginen yhteys, joita voi olla useita yhden fyysisen yhteyden läpi.
VRRP	Virtual Router Redundancy Protocol, reitittimien virtuaalisen kahdentamisen protokolla.
WAN	Wide Area Network, tietoliikenneverkko, joka kattaa LAN-verkon ulkopuoliset osat
WEP	Wired Equivalent Privacy, 802.11-standardissa määritelty salausmenetelmä

WLC	Wireless Lan Controller, langattoman verkon tukiasemien keskitetty hallintalaitteisto, kontrolleri.
WLAN	Wireless LAN, langaton lähiverkko.
WIFI	Wireless Fidelity, langaton lähiverkko.
WPA(2)	Wi-Fi Protected Access (II), langattoman verkon salausmenetelmä.

1 JOHDANTO

Tekniikka ja tietoliikenneyhteydet ovat nykyään tarpeellisia jokaisen päivittäisessä elämässä ja varsinkin tietoliikenneyhteyksiä hyödyntävien teknisten sovellusten tarve kasvaa jatkuvasti, mikä taas luo tarpeen tietoliikenneyhteyksien vakaudelle ja kaistan riittävyydelle.

Tietoliikenneyhteydet ovat tärkeitä myös nykyaikaisessa terveydenhoidossa. Potilaiden tiedot ovat E-arkistossa ja lääkkeiden reseptit menevät nykyään verkon kautta apteekkiin. Myös mittalaitteet, kuten EKG, vaativat häiriöttömiä tietoliikenneyhteyksiä voidakseen keskustella keskusjärjestelmien kanssa.

Tähän opinnäytetyöhön idea syntyi lopulta nopeasti, mutta takana oli pitkä, vuosien mittainen prosessi. Alun perin tarkoitusena oli tehdä vastaava työ edelliselle työnantajalleni jo vuonna 2012, mutta yrityskauppojen se lopulta peruuntui. Nykyinen työnantajani sai toimeksiannon suunnitella ja toteuttaa langaton lähiverkko rakenteilla olevaan uuteen terveyskeskukseen, ja koska itselläni oli jo aiempaa kokemusta vastaavista ratkaisuista, sain työn tehtäväksi ja päätin, että tulen tekemään myös opinnäytetyöni samalla. Kohteen luonteen vuoksi varsinainen suunnittelu, testaus ja dokumentointi tullaan tekemään erillisellä dokumentilla ja se ei ole julkinen. Tässä dokumentissa esitetyt tiedot, kuvat ja muu dokumentaatio on toteutettu testiolosuhteissa.

Työn varsinainen suunnitteluosuus aloitettiin helmikuussa 2016 muiden töiden ohella ja ensimmäinen kohdekäynti tehtiin maaliskuussa. Langattoman verkon tukiasemien sijoittelua varten tehtiin mittaus toukokuun lopussa. Sen perusteella tilattiin tarvittava määrä tukiasemia sekä lisäksi muutamia varalaitteita. Samalla tilattiin myös verkon muut aktiivilaitteet.

Työn tilaajana toimi PyhäNet Oy ja Pyhäjärven kaupunki ja työ tehtiin kevään ja kesän 2016 aikana. PyhäNet Oy on Pyhäjärven kaupungin, Haapajärven kaupungin ja Kärsämäen kunnan omistama yhtiö, joka rakentaa ja hallinnoi nykyaikaisia kiinteitä valokuituverkkoja ja tuottaa niihin palveluita omistajilleen ja asiakkailleen. PyhäNet on kuiduttanut vuoden 2015 loppuun mennessä valmiiksi lähes kaikki taajamien ulkopuoliset alueet Pyhäjärvellä ja Kärsämäellä sekä osittain myös kuntien taajamia. Valokuitukaapelointi jatkuu vuonna 2016 Pyhäjärven keskustan alueella. Uutena alueena aloitetaan Haapajärven

kaupungin alueella valokuituverkon rakennus. Verkkojen rakennus on osa ”Laajakaista kaikille 2015” -hanketta ja on ELY-keskuksen ja Viestintäviraston tukemaa.

2 TIETOLIIKENNEYHTEYDET LÄHIVERKOSSA

Lähiverkolla (LAN, Local Area Network) tarkoitetaan maantieteellisesti rajatun alueen sisäistä tietoliikennettä välittävää suuren siirtokapasiteetin omaavaa verkkoa, jota tyypillisesti hallitsee yksi organisaatio. Lähiverkko koostuu reitittimistä, kytkimistä, palvelimista, työasemista sekä fyysisistä kaapeloinneista. Lähiverkko voi myös olla langaton. Nykypäivän lähiverkossa yhdistellään sekä Ethernet- että WLAN-tekniikalla toteutettuja verkkoja.

Lähiverkko on lähes aina yhteydessä MAN (Metropolitan Area Network)- tai WAN (Wide Area Network) -verkkoon. MAN-verkko voi olla esimerkiksi kaupungin tai kunnan sisäinen verkko, joka yhdistää useita LAN-verkkoja ja WAN-verkko taas on kunta- tai maanrajojen ulkopuolelle asti yltävä verkko, käytännössä siis koko maapallon kattava.

2.1 Kiinteä lähiverkko

2.1.1 Lähiverkkojen historiaa

Lähiverkkoteknologioiden ensimmäiset askeleet otettiin 1970-luvun alkupuolella Xerox Palo Alto Research Centerissä Robert Metcalfin toimesta. Metcalfista tuli myöhemmin 3COM-yhtiön perustaja. Xerox, DEC ja Intel myöhemmin yhdessä esittivät Ethernet-tekniikkaa LAN-verkkojen standardiksi. (1.)

Ensimmäisiä versioita oli ns. paksu Ethernet, eli paksua koaksiaalikaapelia, joka täytti IEEE-standardin 10Base5. Sen suurin tiedonsiirtonopeus on 10 Mbit/s ja maksimikantama 500 metriä. Koska paksu koaksiaalikaapeli oli hankalaa käsitellä, tuli seuraavana versiona IEEE standardi 10Base2 ja tekniikkaa kutsuttiin ”ohueksi ethernetiksi” johtuen RG-58-kaapelista, joka on huomattavasti ohuempaa. Kaapelien liitäntöinä käytettiin BNC-liittimiä. Uutena asiana tuli myös se, että kaapeli voitiin viedä suoraan verkkokortille ja erillistä liitinyksikköä ei tarvittu. Kaapelin sähköisten ominaisuuksien takia segmentin maksimipituus oli enää vain 185 metriä. (1.)

Nämä ensimmäiset kaksi versiota olivat väyläratkaisuja. Laitteet oli kytketty samaan kaapeliin. Vuonna 1990 Ethernet LAN- ja StarLAN-ratkaisujen parhaita puolia yhdisteltiin ja syntyi uusi Ethernet LAN -tekniikka, joka käytti hyväksi

UTP-kaapelia. Uuden tekniikan nimi on 10BaseT, jossa laitteet kytkeytyvät UTP-kaapelilla tähtimäisesti joko toistimeen tai hubiin. Tekniikan maksiminopeus on edelleen 10 Mbit/s, mutta maksimikaapelimatka tippui jo 100 metriin. (1.)

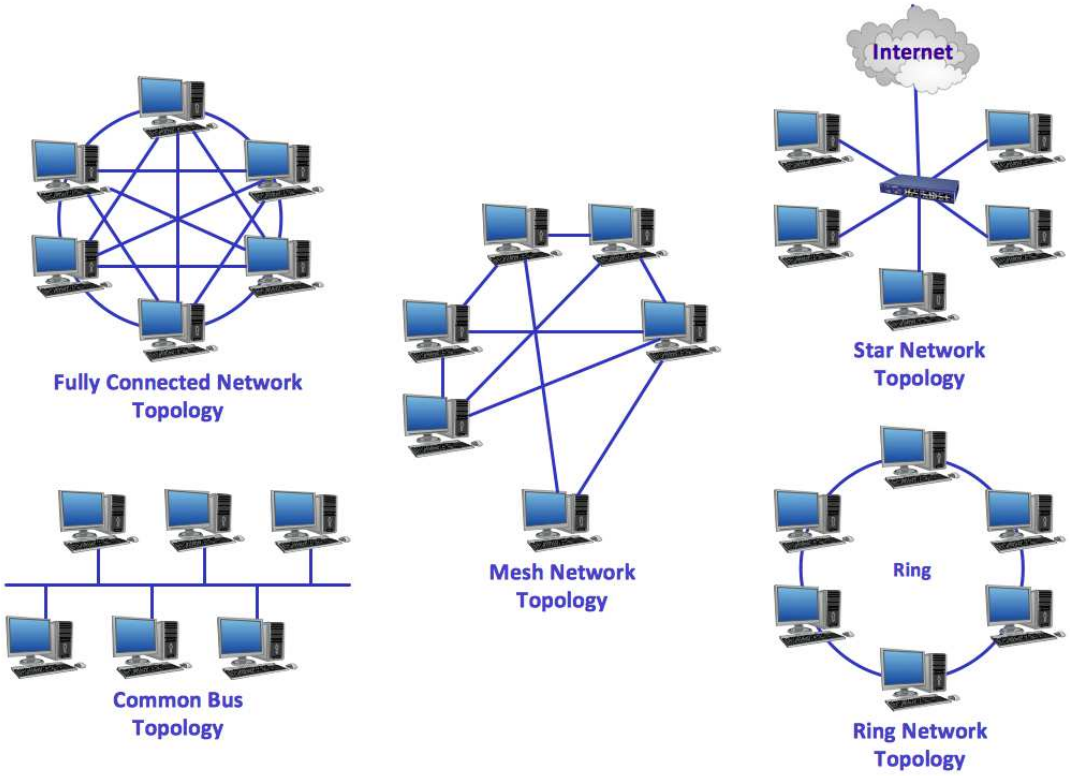
Seuraavaksi lanseerattiin vuonna 1995 Fast Ethernet, 100BaseT, jolla maksiminopeus kasvatettiin 100 Mbit/s:iin samoissa UTP-kaapeleissa. 100BaseT:n mukana yleistyi myös aikaisemmin harvinainen ”kytketty Ethernet”. (1.)

2.1.2 Lähiverkot nyt

2010-luvulla on tiedonsiirron tarve moninkertaistunut, jos verrataan 2000-luvun alkupuoleen. Kotitalouksillekin tarjottavat tietoliikenneyhteydet ovat nopeudeltaan tyypillisesti jo useita kymmeniä megabittejä sekunnissa. Lähiverkkojen työasemien osalta yleisin nopeus on nykyään 1 Gbit/s, joka vaatii 1000BaseT-standardin mukaiset laitteet ja kaapeloinnin. Selvästi yleisin käytössä oleva tekniikka on Ethernet.

Paljon kapasiteettia vaativissa kohteissa, kuten palvelimet, kytkinten runkoyhteydet tai verkkolevyt, käytetään jo yleisesti 10 Gbit/s:n nopeuksia eli 10GBaseX-tekniikoita. Tiedonsiirtomediana käytetään pidemmillä matkoilla valokuitua ja lyhyemmillä kuparikaapelointia.

Lähiverkkojen topologioita on useita erilaisia: tähti, rengas, väylä, silmukka (mesh) ja täysin kytketty (kuva 1). Yleisin näistä on tähtiverkko. Siinä yksi keskipistelaite jakaa yhteydet muille laitteille.



KUVA 1. Lähiverkon topologiat (2).

2.1.3 Lähiverkkojen tietoturvauhat ja suojaaminen

Suurin tietoturvauhka lähiverkoille on käyttäjä, joka tietämättömyydellään päästää haittaohjelman tai tunkeutujan koneelleen ja tätä kautta organisaation sisäverkkoon. Tähän voidaan vaikuttaa käyttäjätasolla pitämällä laitteistojen tietoturvapäivitykset ajantasalla sekä kouluttamalla käyttäjiä toimimaan julkisessa internetissä oikein.

Yksi uhkatekijä on myös mahdollisen tunkeutujan pääsy kiinteään verkkoon esimerkiksi kytkemällä koneensa kytkimeen tai siihen kytkettyyn lähiverkkorasiaan. Tällöin käytännössä hän pystyy esimerkiksi kaappaamaan kaiken liikenteen, mitä VLANissa liikkuu. Tämä voidaan estää käyttämällä privaatti VLAN (PVLAN) -tekniikkaa. PVLAN eristää samalla yleislähetysalueella olevat portit siten, että ne voivat liikennöidä vain UPLINK-liitännän suuntaan. PVLANin ja VLANin ero on käytännössä siinä, että PVLANissa host-laitteet kuuluvat samaan IP-aliverkkoon, vaikka eivät voi liikennöidä suoraan keskenään. (3.)

Luvattomat asiakaslaitteet lähiverkossa voidaan myös estää käyttämällä IEEE 802.1x -standardiin perustuvaa porttikohtaista todentamista. Käyttäjät voivat myös tuoda organisaation verkkoon omia laitteitaan, esimerkiksi WLAN-tukiasemia tai reitittimiä. Nämä aiheuttavat tietoturvauhkia sekä vaarantavat verkon toiminnan. Esimerkiksi väärin konfiguroitu WLAN-reititin voi toimia verkossa DHCP-palvelimena, jolloin se jakaa omia osoitteitaan (yhdyskäytävä ja nimipalvelimet) ja täten rikkoo verkon toiminnan.

2.2 Langaton lähiverkko

Tässä dokumentissa käsitellään langattomina lähiverkkoina IEEE 802.11 -työryhmän standardoimia verkkoja, jotka käyttävät joko 2,4 tai 5 gigahertsin lupavapaita taajuusalueita.

2.2.1 Historia

Ensimmäinen kokoontuminen IEEE:n Wireless LAN -työryhmällä oli vuonna 1991. Vuonna 1998 tuli ensimmäinen standardi 802.11-1997, mutta se ei vielä saavuttanut suurta suosiota. Ensimmäinen julkisesti suosiota saavuttanut standardi on vuonna 1999 julkaistu 802.11b. Sen maksimitiedonsiirtonopeus on 11 Mbit/s ja taajuusalueena on käytössä 2,4 GHz. (4, s. 2.)

Vuonna 2003 julkaistu 802.11g on verkko, joka viimeistään toi langattoman lähiverkon kuluttajien saataville. Tiedonsiirtonopeus on maksimissaan 54 Mbit/s ja käytettävä taajuusalue 2,4 GHz. (4, s. 2.)

2.2.2 Nykyaika

Nykyisin käytössä on yleisimmin vuonna 2009 julkaistu 802.11n -standardin mukaiset WLAN-ratkaisut. Käytettävissä on sekä 2,4 että 5 gigahertsin taajuuskaistat. Yleisimmin kuitenkin käytetään 2,4 GHz:n aluetta. Kovaa vauhtia yleistyvä tekniikka on 802.11ac, joka on standardoitu tammikuussa 2014. Tämä standardi käyttää vain 5 GHz:n aluetta ja on täten parempi häiriönsiedoltaan. (4.)

2,4 GHz:n taajuuden osalta ongelmaksi muodostuvat häiriölähteet ja 20 MHz:n kanavien vähäinen määrä. Johtuen lupavapaudesta 2,4 GHz:n alueella on hyvin paljon myös muuta liikennettä: langattomia puhelimia, itkuhälyttimiä, Bluetooth-laitteet, autohälyttimiä, mikroaaltouuneja ja langattomia mikrofoneja.

Nämä kaikki aiheuttavat ongelmia WLAN-verkon käytölle. Tiheästi asutuilla alueilla, kuten kerrostaloissa ja rivitaloissa, ongelmaksi muodostuvat myös kanavien vähäinen määrä. 802.11n-standardin mukaisesti 2,4 GHz:n alueella on maailmanlaajuisesti määriteltynä 14 kanavaa, mutta riippuen maasta määrä vaihtelee (5). Suomessa Viestintäviraston ”määräys 15 luvasta vapaiden radiolähettimien yhteystaajuuksista ja käytöstä” määrittelee pykälässä 13 taajuusalueeksi 2400–2483,5 megahertsiä. Tämä vastaa 20 MHz:n kanavia 1–13 IEEE 802.11n -standardissa (6, s. 9). Näistä kanavista 1, 6 ja 11, ovat ainoat jotka eivät mene toistensa kanssa päällekkäin. Yhden kanavan maksimitiedonsiirtonopeus on kahdella lähettävällä ja kolmella vastaanottavalla antennilla 144,44 Mbit/s. Yhdistämällä kaksi 20 Mhz:n taajuusaluetta ja käyttämällä sekä kolmea lähettävää että vastaanottavaa antennia voidaan tiedonsiirtonopeudeksi saada jopa 450 Mbit/s. (7.) Toki on muistettava, että tämä on siirtotien maksiminopeus. Todellinen käyttäjän kokema tehollinen nopeus jää usein noin puoleen ilmoitetusta.

802.11ac poistaa 2,4 GHz:n verkkojen ongelmat ja tuo huomattavan parannuksen myös tiedonsiirtonopeuteen. Nopeus on jopa 1300 Mbit/s käytettäessä 3 x 3 antennikonfiguraatiota ja 80 MHz:n taajuuskaistaa. 802.11ac-standardissa on myös tuotu uutena asiana Beamforming-tekniikka, jolla voidaan suunnata signaalia kohti asiakaslaitetta sen sijaan, että signaali levitettäisiin joka suuntaan. (8.)

2.2.3 WLAN-verkon tietoturvauhat ja salausmenetelmät

Koska WLAN-tekniikka perustuu vapaasti eteneviin radioaaltoihin, on se kaikkien alueella olevien asemien kuultavissa (9). Tästä syystä käyttäjän täytyy pystyä varmistumaan, että liikennöi oikean tunnetun tukiaseman kautta eivätkä muut laitteet pysty tulkitsemaan liikennettä. Mahdollisia hyökkäystapoja on esimerkiksi välimieshyökkäys. Välimieshyökkäyksessä radiotielle tulee laite, joka esittää olevansa oikea tunnettu tukiasema, ja käyttäjä liittyy kyseiseen verkkoon luullen käyttävänsä oikeaa laillista verkkoa. Tällöin vihamielinen hyökkääjä pääsee käsiksi verkossa liikkuvaan dataan. (10.)
Langattoman verkon data voidaan myös kaapata kauempaa suunta-antenneilla tai verkkoon voidaan kytkeä myös luvattomia tukiasemia. Nämä ovat tukiasemia jotka on liitetty organisaation sisäverkkoon yleensä esimerkiksi tietämättömän henkilökunnan toimien takia.

WLAN-verkkojen salausmenetelmät salaavat vain radiotien, näitä salausmenetelmiä on useita vaihtoehtoisia. Vanhin ja haavoittuvaisin niistä on WEP (Wireless Equivalent Privacy), WEP-salaus on helposti murrettavissa eikä sitä suositella käytettäväksi. Ongelmaksi muodostuvat jotkin vanhemmat laitteet, jotka eivät tue uudempia WPA/WPA2-salausmenetelmiä.

Suositeltavin ratkaisu verkoissa on käyttää WPA2 (Wi-Fi Protected Access II)-salausta, joka on ollut vuodesta 2006 lähtien tuettu laitteissa jotka Wi-Fi Alliance on hyväksynyt. WPA2-salausta käytettäessä tulee käyttää AES-CCMP salaustekniikkaa koska TKIP on haavoittuvainen MIC-hyökkäyksiä vastaan. Organisaatioille suositellaan käytettäväksi WPA2 Enterprise -suojausta, joka käyttää hyväkseen 802.1x -todentamista. (11.)

3 SUUNNITTELUOSUUS

Suunnittelua lähdetään viemään eteenpäin asiakkaan vaatimusten ja tarpeiden perusteella. Kohdeympäristö on kaksikerroksinen, betonirakenteinen rakennus. Käyttäjämäärät langattoman verkon osalta ovat arviolta muutamia kymmeniä, kiinteässä verkossa laitteita tulee olemaan huomattavasti enemmän. Alkuperäinen tarkoitus oli toteuttaa vain kiinteistön WLAN-verkon suunnittelu, mutta matkan aikana todettiin, että tarvitaan myös sekä kiinteän verkon laitteita että verkon valvontaan ja ylläpitoon soveltuvia järjestelmiä. Työ aloitettiin helmikuussa palaverilla, jossa käytiin läpi asiakkaan tarpeet sekä kaapelointisuunnitelmat. Kaapelointisuunnitelmiin tehtiin muutamia lisäyksiä tukiasemia ja muuta käyttöä varten.

3.1 Organisaatioiden sisäverkkojen suunnittelu

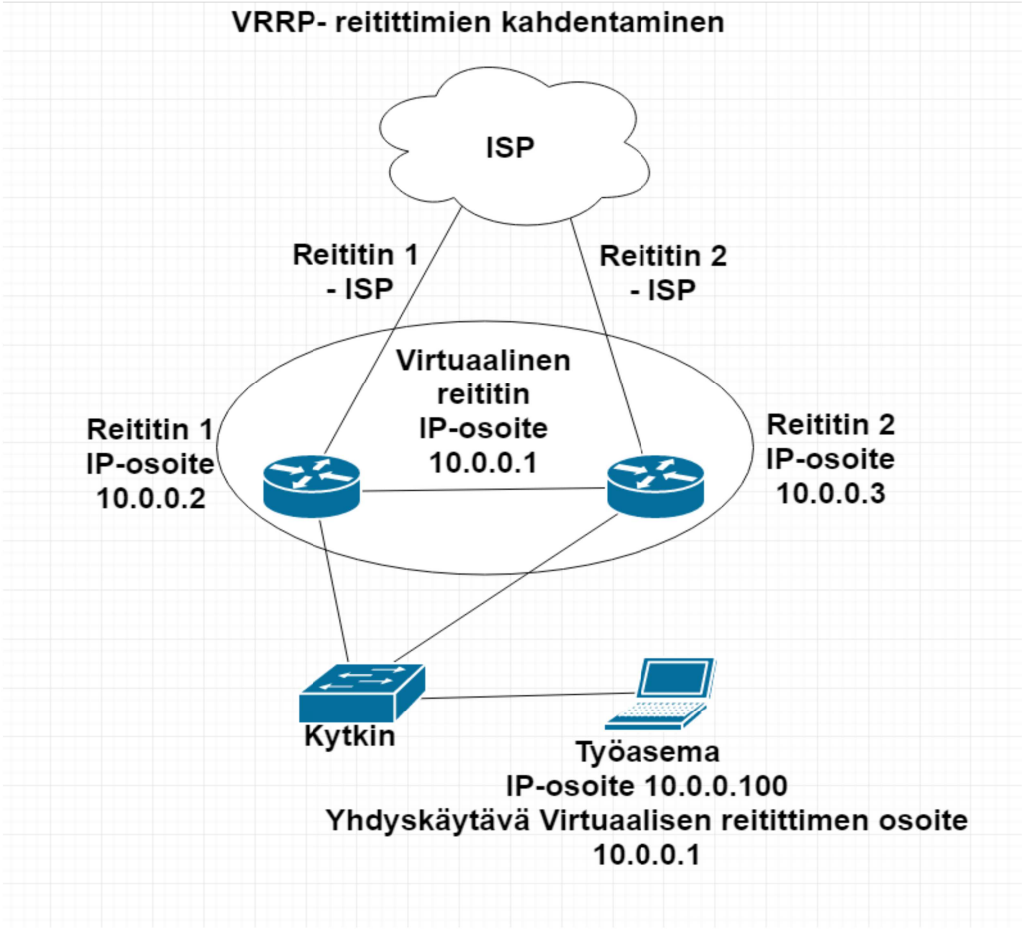
Tyypillisesti organisaatioiden sisäverkko koostuu sekä langattomista että langallisista verkoista. Kiinteät työpisteet on varustettu lähiverkkokaapeloinnilla ja mobiililaitteet hyödyntävät langatonta verkkoa. LAN-verkot pyritään myös jakamaan käytön ja käyttäjien mukaan omiin VLAN-verkkoihin. Esimerkiksi kouluissa voi olla opettajilla ja hallinnolla oma verkkonsa, oppilaskoneille toinen ja kolmas vierailijoille.

Yksittäinen VLAN on myös L2-tasolla yleislähetysalue. Tämä tuo sekä etuja että haittoja. Eduiksi voidaan laskea helppo verkon konfigurointi ja käyttöönotto, mutta toisaalta yleislähetysliikenne voi aiheuttaa verkossa ongelmia, jos verkon koko kasvaa.

Johtuen edellä mainituista L2-tason ongelmista on suositeltavaa, että jokainen yksittäinen toimipiste on oma verkkonsa. Tällöin helpoin ratkaisu on toteuttaa MPLS-verkko, jolla yksittäinen toimipiste saadaan organisaation verkkoon ja jokaiseen toimipisteeseen oma reititin.

Kriittisissä kohteissa pyritään poistamaan kahdennuksella yhden pisteen vaurioitumisen mahdollisuus ja tätä kautta myös koko verkon kaatuminen. Parhaimmassa tapauksessa käytetään ulkoverkkoon päin kahta erillistä kuituyhteyttä, jotka tulevat fyysisesti eri reittejä rakennukseen ja myös eri operaattoreilta.

Aktiivilaitteista kahdennetaan reitittimet ja käytetään hyväksi VRRP-protokollaa. Tällöin reitittimet muodostavat yhden virtuaalisen reitittimen, ja jos toinen laite jostain syystä putoaa pois, jää toinen laite käyttöön. VRRP:n etu on se, että ryhmä virtuaalisia reitittimiä näkyy työasemille yhtenä reitittimenä ja yhden yhdyskäytävä osoitteen takaa. (Kuva 2.) Reitittimien takana on yleensä kahdennettu palomuuriratkaisu, jossa toinen laite on valmiustilassa, jos ensisijainen laite rikkoutuu. Palomuuri jakaa verkon yleensä kolmeen loogiseen osaan: julkinen verkko, DMZ ja organisaation sisäverkko. DMZ-alueella on yleensä palvelimia, joita käytetään myös liikennöintiin ulkoverkon suunnasta.



KUVA 2. VRRP-Virtuaalinen reititin.

Sisäverkko on isommissa organisaatioissa yleensä jaettu runkokytkimiin ja työasemakytkimiin. Runkokytkimet muodostavat nimensä mukaisesti verkon rungon ja yhdistävät työasemakytkimet toisiinsa, sekä muihin verkon aktiivilaitteisiin. Kytkimien vikasietoisuutta voidaan parantaa pinoamisella, jolla fyysisiä kytkimiä voidaan pinota yhdeksi loogiseksi kokonaisuudeksi. Pinoon voidaan liittää uusia tai poistaa vanhoja kytkimiä ilman toiminnan häiriintymistä.

Periaatekuva sisäverkon vikasietoisesta toteutuksesta on liitteessä 1.

3.2 Kaapelointi

Verkkoja suunnitellessa tulee ottaa huomioon tietoturva, laitteiden vikasietoisuus, käyttäjämäärät ja käyttäjien sijainti.

Kohteen yleiskaapeloinnin on suunnitellut sähkösuunnittelija sähköurakoinnin yhteydessä. Kaapelointi on toteutettu siten, että jokaiseen huoneeseen tulee vähintään kaksi kappaletta lähiverkkorasioita. Jokaiseen rasiaan tulee kaksi CAT6-kategorian kaapelia. ATK-kaappeja kiinteistöön tulee useita. Yksi toimii keskipisteenä. Keskipisteestä lähtee jokaiseen ATK-kaappiin valokuitu sekä kuparikaapelointi. Valokuitu on toteutettu hybridikaapelilla, jossa on sekä monimuoto- että yksimuotokuituja.

3.3 Laitevalinnat

Tämän kohteen liityntärajapinnasta ja reitityksestä vastaa operaattorin reitittimet, joten erilliset reitittimet eivät kuulu suunnitelman piiriin. Keskipistepinoksi valittiin reitittävät kytkimet jos myöhemmin tarvitaan L3-ominaisuuksia.

Laitteiden valinnoissa ratkaisevia tekijöitä on nykyisten järjestelmien kanssa yhteensopivuus, hinta, luotettavuus sekä hallittavuus. Kytkinten tulee tukea LACP-protokollaa. Keskipistekytkimeltä jokaiseen atk-kaappiin viedään kaksi fyysistä liitäntää, jolla saadaan tuplattua kapasiteetti ja lisättyä vikasietoisuutta.

Langattoman verkon hallinnassa tullaan käyttämään kontrolleripohjaista ratkaisua. Kyseisessä ratkaisumallissa yksi keskitetty laite, WLAN-kontrolleri, huolehtii tukiasemien toiminnasta. Tällöin jokaista tukiasemaa ei tarvitse erikseen konfiguroida verkkoon, vaan ne saavat automaattisesti asetukset kontrollerilta. Kontrollerilaitteisto tullaan kahdentamaan.

WLAN-tukiasemien tulee tukea vanhempaa 802.11n- ja uudempaa 802.11ac-tekniikkaa. Tukiasemien käyttöjännite syötetään PoE-tekniikalla lähiverkko-kaapeloinnin kautta. Riippuen tukiasemien määrästä yhden keskitinkaapin alueella käytetään joko PoE-kytkimiä tai erillisiä PoE-injektoreita.

WLAN-tukiasemien paikat suunnitellaan alustavan tutustumiskäynnin jälkeen pohjapiirrustukseen. Tämän jälkeen suoritetaan toinen käynti jossa suunnitelmien mukaisesti mitataan WLAN-verkon kuuluvuus. Kuuluvuuden mittauksessa käytetään hyväksi kannettavaa tietokonetta sekä kiinteistön pohjapiirrustusta. Mittaus tehdään Ekahau HeatMapper -ohjelmistolla (http://www.ekahau.com/wifidesign/ekahau-heatmapper).

Tarkemmat laitevalinnat ja dokumentaatio ovat erillisellä dokumentilla.

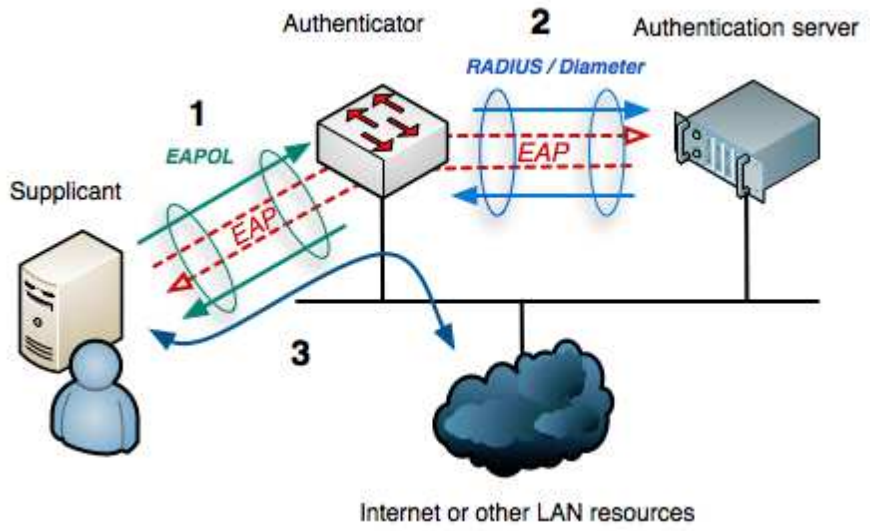
3.4 Tietoturvaratkaisut

Käyttäjät tullaan erottamaan omiin virtuaalilähiverkkoihin. Vierailijaverkossa tullaan estämään käyttäjien liikennöinti keskenään. Lisäksi myös vieralijaverkko tullaan salaamaan, salausavain on saatavilla käyttäjille infotiskiltä. Tuotantoverkon suositeltu todennustapa on käyttää 802.1x-tunnistusta, jolla voidaan suojata sekä fyysisisiä liitäntöjä että myös WLAN-verkkoja. Tärkeänä tekijänä on myös käyttäjien perehdyttäminen tietoturvaan.

3.4.1 802.1x

Porttikohtaisessa 802.1x-todennuksessa on kolme eri fyysistä komponenttia: työasema (supplicant), todentaja (authenticator) sekä todennuspalvelin (authentication server). 802.1x:n avulla voidaan antaa käyttäjälle hänen tarvitsemansa verkkoresurssit käyttöön, kirjautui hän sitten langattoman tai kiinteän verkon kautta missä tahansa yrityksen toimipisteissä. (12, s. 3.) (Kuva 3.)

Kiinteän LAN-verkon osalta todentajana toimii kytkin. Työaseman liittyessä verkkoon kytkin päästää läpi vain EAPOL-liikennettä jos porttikohtainen tunnistus on päällä. Kun käyttäjä on tunnistettu, liitetään portti oikeaan VLANiin ja käyttäjä voi liikennöidä normaalisti verkossa. Jos laitetta ei tunnisteta, voidaan portti liittää vierailija-VLANiin tai estää liikenne kokonaan. Tällä tavalla voidaan myös estää langattoman verkon luvattomien tukiasemien asennus yrityksen kiinteään verkkoon. Langattomassa lähiverkossa todentajana toimii WLAN-tukiasema tai kontrolleri. (12.)

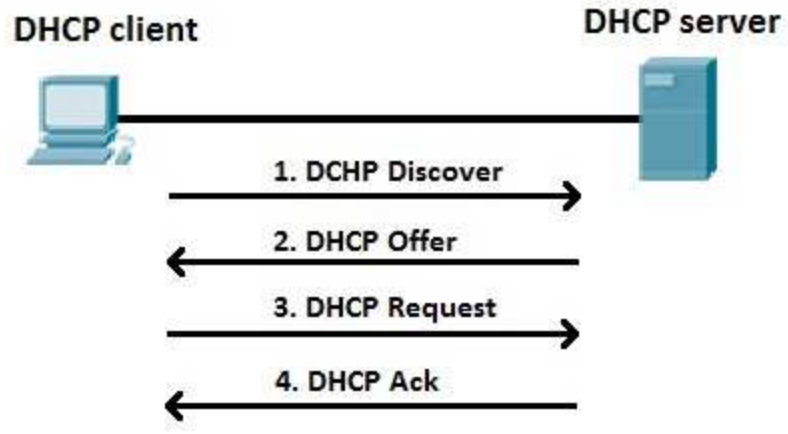


KUVA 3. 802.1x-protokolla (13).

3.4.2 DHCP Snooping

DHCP Snooping -tekniikalla estetään laittomien DHCP-palvelimien asentaminen verkkoon. Kytkimille määritellään DHCP Snooping päälle ja määritellään portit, joiden lähettämät DHCP-paketit ovat luotettuja (trusted), eli portit, joiden takana on DHCP-palvelin tai UPLINK-liitäntä kytkinverkossa ylöspäin. Käyttäjien liityntäportit konfiguroidaan ei-luotetuiksi (untrusted), etteivät ne voi lähettää DHCP server-paketteja (14). DHCP Snooping pitää ottaa erikseen käyttöön jokaiseen haluttuun virtuaalilähiverkkoon.

Asiakaslaite lähettää DHCPDISCOVER-paketin saadakseen IP-osoitteen. Paketti välitetään kytkinverkon kautta DHCP-palvelimelle. Palvelin vastaa DHCPOFFER-paketilla ja jos paketti tulee luotetusta portista välittää kytkin paketin asiakaslaitteelle. Asiakaslaite vastaa DHCPREQUEST-viestillä hyväksyvänsä osoitteen ja palvelin vastaa joko DHCPACK (antaa IP-osoitteen) tai DHCPNAK (hylkää osoitepyynnön). (15.) (kuva 4.)



KUVA 4. DHCP-asiakkaan ja palvelimen välinen pakettien vaihto (15).

3.5 Verkon valvonta ja ylläpito

Osa järjestelmistä on jo tuotannossa olevia, ja osa tehtiin nimenomaan tätä projektia ajatellen, sekä tukemaan myös muuta verkkoinfrastruktuuria. Kaikille järjestelmille on yhteistä se, että pyrittiin hyödyntämään vapaan lähdekoodin ohjelmistoja jolloin kalliita lisenssikustannuksia ei tule. Näiden järjestelmien osalta on usein mahdollista ostaa myös maksullista tukea, mutta suosittujen ohjelmistojen osalta keskustelupalstoilta saa helposti apua mahdollisissa ongelmissa.

Valvontaympäristönä käytetään olemassa olevaa Zabbix-valvontaympäristöä, joka pyörii omana virtuaalipalvelimenaan CentOS käyttöjärjestelmässä. Tietokantana käytetään MySQL:ä ja käyttöliittymä on PHP:lla toteutettu. Zabbix-palvelinta käytetään alkuvaiheessa vain yksinkertaiseen ICMP-valvontaan, jolla saadaan hälytys esimerkiksi sähköpostiin jos jokin laite tippuu verkosta. Tulevaisuudessa tarkoitus ottaa myös enemmän ominaisuuksia käyttöön SNMP-protokollan avulla jolloin saadaan muun muassa palvelimien, kytkimien ja WLAN-kontrollereiden statistiikkaa kerättyä talteen. Zabbixiin päädyttiin koska se on ilmainen yrityskäyttöön suunniteltu vapaan lähdekoodin ratkaisu johon löytyy hyvin erilaisia agentteja, konfigurointimalleja eri aktiivilaittelle sekä muunmuassa applikaatioita puhelimille. Lisäksi sama järjestelmä on käytössä myös yhteistyökumppanilla.

Laitteistojen lokien talteen keräystä varten on myös tehty oma Syslog-palvelin, käytännössä tämä on Linux-pohjainen palvelin joka kerää laitteiden lähettämät lokitiedot ja tallentaa ne sekä varmuuskopioi. Lokit ovat luettavissa Linux-

tiedostojärjestelmän kautta, mutta haussa on graafinen vapaan lähdekoodin alusta josta lokit saataisiin helpommin luettua. Syslog-palvelimen alustana toimii Ubuntu 16.04 server.

IP-osoitteiden ja VLAN-tietojen ylläpitoa varten on käyttöön otettu PHPipam-palvelin. Aikaisemmin kyseiset tiedot ovat olleet joko työntekijöiden päässä, omana excel-taulukkona tai käsin kirjoitettuna paperilappuna, ja tästä johtuen esimerkiksi vapaiden IP-osoitteiden määrää ei tiedetä tarkasti. PHPipam pyörii samanlaisella CentOS-alustalla kuin Zabbix ja hyödyntää myös MySQL-tietokantoja sekä kuten nimestä voi päätellä PHP:ta. Alunperin ajatuksissani oli käyttää edellisestä työpaikasta tuttua IPplania, mutta koska kyseisen ohjelmiston kehitys näyttää loppuneen, päädyttiin etsimään vaihtoehtoja ja PHPipam todettiin parhaaksi nykyistä käyttöä sekä tulevaisuutta ajatellen.

Koska kytkimien hallintaverkosta on estetty liikenne internettiin, täytyy kuitenkin lokeja varten saada tarkat aikatiedot. Aikatietoa varten tehdään NTP-palvelin joka jakaa tarkkaa aikatietoa laitteille. Tiedot voi asettaa käsin jokaiseen laitteeseen erikseen, mutta tällöin aikaleimoissa on heittoja.

4 KÄYTTÖÖNOTTO JA DOKUMENTOINTI

4.1 Verkon rakenne

Verkko on rakennettu siten että pääjakajaan on asennettu keskipistekytkin joka on muodostettu kahdesta ZTE ZXR10 5960-TM-H -kytkimestä. Kytkimet on yhdistetty toisiinsa MINI-SAS-kaapeleilla ja laitteista on luotu yksi looginen kytkin. Jos jostain syystä toinen kytkimistä vioittuu, jatkaa toinen kytkimistä kuitenkin verkon ylläpitoa. Molemmissa fyysisissä laitteissa on samanlainen kalustus: kaksi vaihtovirtalähdettä, MINI-SAS-pinokortti, kaksi SFP-lisäkorttia joissa jokaisessa on neljä moduulipaikkaa. Yhteensä laitteissa on siis 16 kappaletta optisia 1 Gbit/s:n SFP-liitäntöjä sekä 40 kappaletta sähköisiä 1000BaseTx -liitäntöjä.

Pääjakajassa on lisäksi kaksi WLAN-kontrolleria, Cisco WLC 2504, jotka ovat 25 tukiaseman lisenssillä. Toinen kontrollereista on ensisijainen ja toinen toissijainen. Molempiin kontrollereihin on konfiguroitu fyysisesti erilliset hallinta- (management) ja liikenneliitännät (AP-manager ja data). Kontrollerit on yhdistetty pinossa eri kytkimiin joten jos pinon jompikumpi kytkin vioittuu säilyy WLAN-verkko toiminnassa pienellä katkolla.

Kohteessa on useita kerrosjakamoita joissa on jokaisessa oma kytkin, malliltaan ZTE ZXR10 5250-52TM. Kytkimissä on neljä kappaletta optisia 1 Gbit/s SFP-liitäntöjä sekä 48 kappaletta sähköisiä 1000BaseTx-liitäntöjä. Kytkimet on yhdistetty pääjakajan kytkinpinoon kahdella kuituparilla siten, että kuidut menevät molempiin fyysisiin laitteisiin. Tällöin toisen pinokytkimen, SFP:n tai kuidun vaurioituminen ei katkaise koko yhteyttä kerrosjakamoon. Kuituna on käytetty monimuotokuitua. Optiikkana käytetään 1000BaseSX-optiikoita jotka toimivat aallonpituudella 850 nm ja joiden maksimikantomatka on 550 metriä.

WLAN-tukiasemia on kaapeloitu kerrosjakamoiden kautta yhteensä 11 kappaletta. Tukiasemina käytetään Ciscon AIR-CAP1702i-, AIR-CAP2702i- ja AIR-AP2702i-malleja. 1700-sarjan tukiasemat on varustettu 3 x 3 MIMO-antenneilla sekä kahdella tilallisella virralla (Spatial Stream). CAP2702i ja AP2702i ovat lähes identtisiä varustettuna 3 x 3 MIMO-antenneilla ja kolmella tilallisella virralla jolla pystytään käyttämään 802.11AC-standardin

Beamforming-tekniikkaa. Erona se, että AP2702i-laitteet ovat ns. Universal Domainilla (UX) olevia jolloin ne eivät ole koodattuja tietylle maantieteelliselle alueelle.

AP2702i-laitteille täytyy ohjelmoida Cisco AirProvision -ohjelmalla oikea maakoodi. Käytännössä tämä tapahtui provisioimalla yksi tukiasema jo työpisteellä FI-maakoodille. Provisiointiin tarvittiin Android-käyttöjärjestelmällä oleva puhelin tai tabletti jolla on internet-yhteys, GPS-ominaisuus sekä Google Playstä ladattava Cisco AirProvision -sovellus. Sovellus tunnistaa mobiililaitteen GPS-tietojen perusteella sijainnin. Sen jälkeen sovelluksella voidaan konfiguroida tukiasemalle oikea maakoodi. Jos maakoodia ei laiteta tukiasema toimii vain 2,4 GHz:n taajuudella. Kun yksi tukiasema saatiin konttorilla provisioitua FI-maakoodille vietiin se kohteeseen. Tukiasema levittää NDP-protokollan avulla oikeat maakoodit muihin samassa verkossa oleviin UX-tukiasemiin. (16.) Tukiasemien virransyöttö hoidetaan PoE-tekniikalla käyttäen Ciscon PoE-virtalähteitä. Koska tukiasemia tulee vain muutamia jokaiseen jakamoon ei ollut kustannustehokasta ostaa PoE-kytkimiä.

Verkon aktiivilaitteille on tehty oma hallinta-VLAN, jonka liikenne on rajattua vain tiettyjen laitteiden välille. Lisäksi WLAN-tukiasemien AP-manager -VLAN on eriytetty täysin muusta verkossa. Kyseisessä verkossa on DHCP-palvelin, joka jakaa tukiasemille DHCP:lla osoitteet sekä DHCP Optio43:lla tiedon WLAN-kontrollereiden osoitteista ja nimistä.

4.2 WLAN-kontrollereiden vikasietoisuuden testaus

WLAN-kontrollereita on kohteeseen asennettu kaksi kappaletta. Molemmat ovat Cisco WLC 2504 -laitteita joissa on lisenssit 25 tukiasemalle. Laitteet on konfiguroitu Ciscon WLC HA N+1 -ohjeiden mukaisesti (17). Jokainen laite tulee konfiguroida erikseen. Ensisijainen laite on konfiguroitu primarylaitteeksi ja tälle on kaverina toissijainen laite, secondary. Laitteiden välille on luotu mobility group eli ne voivat jakaa tietoa asiakaspäätelaitteista keskenään (18). Molempiin laitteisiin on tehty samanlaiset WLAN-konfiguraatiot, käytännössä ainoat erot tulevat hallinta- ja WLAN-verkkojen IP-osoitteista sekä siitä että varalaite on asetettu ”HA-SKU secondary controller” -tilaan. Myös liittyineille tukiasemille kerrotaan kontrollereiden IP-osoitteet, nimet sekä tieto kumpi on ensisijainen ja kumpi toissijainen.

Tukiasemat saavat myös DHCP-palvelimelta DHCP Optio43 -lisätiedoilla kontrollereiden IP-osoitteet. Tämä ei ole tarpeellista jos sekä kontrollereiden AP-manager -liitäntä että tukiasemat ovat samassa virtuaaliverkossa. Tässä tapauksessa näin on mutta yksi tukiasema pääsi liittymään ensimmäisellä käynnistyskerralla toiseen aiemmin käytössä olleeseen kontrolleriin, joka ei ole suoraan organisaation hallinnassa. Tämä eksynyt tukiasema ei löytänyt oikeaa kontrolleria ilman Optio43:sta joten se jätettiin päälle DHCP-palvelimelle.

Testi suoritettiin seuraavasti: Tukiasemana käytettiin Cisco AIR-AP2702I-UXK9:ää ja kontrollerit oli konfiguroitu Cisco WLC HA N+1 -ohjeistuksen mukaisesti. Työasemana toimi DELL VOSTRO jossa on Intel Centrino Wireless N 2230 -piirisarja (802.11b/g/n standardeja tukeva, 2 x 2 MIMO antennikonfiguraatiolla oleva ja 2,4 GHz:n taajuusalueella toimiva piirisarja). Kone liitettiin Vierailijaverkkoon ja mitattiin aikaa, joka kului siitä kun ensisijaisen laitteen verkkoliitäntä laitetaan sulkuun ja tukiasema siirtyy varalaitteelle. Tämän jälkeen ensisijaisen laitteen verkkoliitäntä avataan ja mitattiin kulunut aika kun tukiasema siirtyi takaisin AP Fallback -ominaisuudella

Mittauksia tehtiin seitsemän kappaletta. Ensimmäinen mittaus suoritettiin Windows 7 -käyttöjärjestelmän omalla PING -työkalulla ja sekuntikellolla pingaamalla yhdyskäytävän osoitetta *ping 192.168.1.1 -t -w 100* -attribuuteilla. Loput mittaukset tehtiin PingPlotter -työkalulla asettamalla ping-intervalliksi 0,5 s. PingPlotterilla otettiin ylös tietty ajanjakso ja kyseisen ajanjakson pakettimäärä sekä pakettihävikki ja laskettiin näiden perusteella aika jolloin yhteys ei toiminut. Keskiarvoksi saatiin ensisijaiselta toissijaiselle siirtymän osalta 41,8 sekuntia. Tukiasemien siirtyessä takaisin ensisijaiselle kontrollerille keskiarvo oli 15,2 sekuntia. Keskiarvosta on molemmista poistettu epätodellisen oloiset luvut. Mittaustulokset ovat taulukossa 1.

TAULUKKO 1. WLC-kahdennuksen tukiasemien siirtyminen kontrollerilta toiselle.

Ensisijainen tippuu verkosta	Paketteja	Pakettihävikki %	Katkoaika s
1			41,0
2	318	49,4	78,5
3	216	34,3	37,0
4	106	69,8	37,0
5	142	58,5	41,5
6	238	31,1	37,0
7	199	57,8	57,5
Keskiarvo			**41,8**
Toissijaiselta ensisijaiselle siirtyminen			
1			6,0
2	61	50,8	15,5
3	205	15,1	15,5
4	190	15,3	14,5
5	184	16,3	15,0
6	136	21,3	14,5
7	158	20,9	16,5
Keskiarvo			**15,2**

4.3 Kytkinten runkolinkkien vikasietoisuuden testaus

Kytkinten runkolinkkien testausta tehtiin ennen tuotantoon laittoa laboratorio-oloissa. Kytkinten konfiguraatiot löytyvät liitteestä 2. LACP-protokollaa ei saatu toimimaan Ciscon ja ZTE:n välillä joten käytettiin staattista linkkiaggrekaatiota. Tämä ei ole suositeltu toimintatapa, koska konfigurointivirheet voivat lamaannuttaa verkon täysin.

Testattaessa simuloitua vikatilannetta, jossa toinen fyysisistä liitännöistä katkeaa todettiin että looginen yhteys säilyy. Muutamissa testeissä hävisi yksi ICMP-paketti. Konfiguraatiot ja kytkinten antamat tiedot linkkiaggregaatiosta löytyvät liitteestä 2.

4.4 DHCP Snooping -testaus

ZTE- kytkimelle annettiin seuraavat komennot:

set dhcp snooping-and-option82 enable
set dhcp snooping add port 1-24
set dhcp trunk 1 server

Tällä aktivoitiin DHCP Snooping ja asetettiin se portteihin 1–24 päälle. Luotetun palvelimen liitännäksi merkittiin *trunk 1.* Tämä liitäntä on LAG-liitäntä kohti seuraavaa kytkintä jonka takana on DHCP-serveri.

Seuraavassa vaiheessa kytketään kytkimen porttiin numero 2 DHCP-palvelin, joka jakaa omaa IP-osoiteavaruutta, sekä suljettiin LAG-liitäntä kohti toista kytkintä. Ensimmäisenä testattiin että suoraan DHCP-palvelimelta saadaan tietokoneelle IP-osoite. Tämä onnistui ja kone sai osoitteen 10.10.10.254. Seuraavaksi kytkettiin sama kone kytkimen porttiin numero 4 ja annettiin Windows -käyttöjärjestelmän komentokehoitteessa komento *ipconfig /renew*. Tämän jälkeen tutkittiin kytkimen antamaa lokia joka oli seuraavanlainen:

Fri Oct 14 15:49:01 2016 %DHCP-SNOOPING: DHCPREQUEST packet dropped from port 4 with VLAN 10 and reason: invalid ciaddr when entry is under create.

Fri Oct 14 15:49:24 2016 %DHCP-SNOOPING: DHCPINFORM packet dropped from port 4 with VLAN 10 and reason: can not find binding entry.

Fri Oct 14 16:05:12 2016 %DHCP:DHCPREQUEST packet dropped from port 2 with VLAN 10 and reason: port 2 is not server port.

Työasema ei saanut DHCP-palvelimelta osoitetta.

Tämän jälkeen avattiin LAG-liitäntä kohti toista kytkintä ja annettiin uudestaan *ipconfig /renew* -komento. Työasema sai lähes välittömästi osoitteen sallitulta DHCP-palvelimelta.

4.5 WLAN-verkon optimointi

Tukiasemia tilattiin ylimääräisiä kappaleita varalaitteiksi sekä mahdollista laajentamista varten. Tutkittaessa kontrollereiden lokeja todettiin, että tietyllä alueella on selkeästi ainakin yksi katvekohta jossa tukiasemat raportoivat :

Coverage hole pre alarm for client[2] 12:34:56:78:90:ab on 802.11b/g interface of AP cc:dd:7e:ee:ff:bb (ap). Hist: 0 0 0 0 0 0 0 84 101 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Tämä tarkoittaa sitä, että verkkoa käyttävän päätelaitteen vastaanomatta signaalin taso (RSSI) on ollut vähintään 5 sekuntia alle määritellyn raja-arvon. Kyseinen raja-arvo on oletuksena -80 dBm. (19.) Käyttäjiä haastattelemalla pyritään selvittämään kyseinen kohta ja lisätään kohteeseen yksi tukiasema.

Lisäksi kontrollerit hälyttävät useammasta luvattomasta tukiasemasta*:*

Rogue AP: 78:f8:82:00:00:00 detected on Base Radio MAC: cc:16:f0:e4:f0:00 Interface no: 0(802.11b/g) Channel: 1 RSSI: -93 SNR: 2 Classification: unclassified, State: Alert, RuleClassified : N, Severity Score: 0, RuleName: N.A. ,Classified AP MAC: 00:00:00:00:00:00 ,Classified RSSI: 0

Näiden käsittelylle on erilaisia mahdollisuuksia. Jos on tiedossa että kyseiset tukiasemat ovat esimerkiksi naapureille kuuluvia laitteita ne kannattaa merkitä harmittomiksi oman verkon ulkopuoleisiksi asemiksi. Jos taas laite on tunnistettu sisäverkon laite, joka on tietoisesti asennettu WLAN-tukiasemaksi, voidaan tukiasema merkitä harmittomaksi sisäverkon laitteeksi. (20.)

Jos epäillään, että luvaton tukiasema on vihamielinen ja sen kautta yritetään tehdä jotain luvatonta organisaation sisäverkossa, merkitään kyseinen tukiasema epäilyttäväksi. Tarvittaessa myös voidaan estää sen käyttöä eristämällä. Tällöin yksi tai useampi kontrollerin ohjaama tukiasema lähettävät niin sanottua deauth-hyökkäystä luvattomaan tukiasemaan liittyneille päätelaitteille. Deauth-hyökkäyksessä tukiasemat lähettävät luvattomaan tukiasemaan liittyneille päätelaitteille pakettikehyksiä, jotka tiputtavat päätelaitteen pois verkosta. Tämä on vain väliaikainen ratkaisu ja luvaton tukiasema tulee etsiä ja poistaa verkosta. (20.) Laitteen fyysinen sijainti löytyy MAC-osoitteen avulla kytkimiltä etsien. Pääkytkimen MAC-taulua tutkimalla

voidaan selvittää minkä runkoliitännän takana kyseinen laite näkyy. Tämän jälkeen tutkitaan kyseisen runkoliitännän päässä olevan kytkimen MAC-taulua ja saadaan selville portti johon häiriköivä tukiasema on kytketty.

Kontrollerilla pystytään automatisoimaan prosessi luvattomien tukiasemien tunnistamiseksi käyttämällä tukiasemia erilaisissa rooleissa. Normaalien paikallisten tukiasemien lisäksi yksi tukiasema konfiguroidaan samaan verkkoon tunnistamaan luvattomat tukiasemat. Tällöin tukiaseman radio sammutetaan ja tukiasema liitetään trunk-liitännällä kiinteään verkkoon. Tukiasema kuuntelee tällöin kaikkia VLANeja. Jos paikallinen tukiasema tunnistaa luvattoman tukiaseman se välittää tiedon kontrollerille. Kontrolleri välittää kaikkien luvattomien tukiasemien MAC-osoitteet tunnistimena toimivalle tukiasemalle, joka vertaa niitä kiinteän verkon ARP-tauluun. Jos vastaava MAC-osoite löytyy on kyseinen luvaton tukiasema kytkettynä organisaation kiinteään verkkoon ja se voidaan jäljittää. Jos taas kyseistä osoitetta ei löydy sisäverkosta voidaan todeta, että kyseinen laite on naapurustossa kuuluva laillinen WLAN. (21.)

Vastahyökkäysominaisuuksien käyttö tulee olla perusteltua ja vain todellisia uhkia vastaan. Toimenpiteet ovat tietoliikenteen häirintään joka on Suomessa rikos ja voi johtaa jopa vankeusrangaistukseen.

4.6 Käyttöönotossa koettuja ongelmia

Aikataululliset haasteet olivat välillä tiukat, koska kyseessä oli uudisrakennus, ei aktiivilaitteita päästy asentamaan hyvissä ajoin etukäteen. Kun lopulta tilat olivat valmiina ilmoitti laitetoimittaja, että heidän osaltaan osa laitteista myöhästyy alkuperäisestä arviosta. Lopulta fyysiset asennukset saatiin valmiiksi noin 2 viikkoa ennen ensimmäisiä käyttäjätestejä ja konfigurointiin meni viikko. Osaltaan myös oma päivätyöni hidasti valmistumista. Koska en pystynyt keskittymään vain tähän työhön, suurin osa ajastani meni muissa tehtävissä.

Osa tukiasemista oli ”universal domain” -koodattuja. Tämän takia kyseiset tukiasemat piti provisoida siten, että niiden aluekoodaus oli Suomi. Tämä mielestäni oli hieman hankalasti toteutettu Ciscon osalta, koska tätä provisiointia ei voinut tehdä suoraan WLAN-kontrollerin asetuksista, vaan provisointi oli tehtävä Cisco AirProvision -työkalulla ja mobiililaitteella.

Asiakkaan edustaja myös ilmoitti muutamista vikatilanteista verkossa, jossa käyttäjien kokema verkon toiminta oli hidastunut. Asiaa tutkittaessa Wireshark -ohjelmistolla todettiin, että muutamista IPv6-osoitteista tuli verkkoon todella paljon IPv6 Multicast Listener Discovery -paketteja. Pakettimäärät olivat kymmeniä tuhansia paketteja sekunnissa. Tämä alkoi vaikuttamaan myös kytkinten suorituskykyyn. Wiresharkin lokeista saatiin laitteiden MAC-osoitteet, jotka todettiin http://www.macvendors.com/ palvelun avulla Hewlett-Packard -työasemien osoitteiksi. MAC-osoitteiden avulla pystyttiin myös yksilöimään kytkinportit ja tätä kautta myös työasemat, jotka aiheuttivat kyseisen IPv6-ryhmälähetys myrskyn.

Asiaa tarkemmin tutkittaessa todettiin, että vika johtuu kyseisten työasemien verkkokorttien ajureista. Verkkokortit olivat INTEL I217-LM -piirisarjalla. Ajureissa olevan ohjelmistovirheen takia työaseman siirtyessä unitilaan se alkaa lähettämään IPv6 Multicast Listener Report -paketteja. Kyseistä ongelmaa ei ollut ennen uutta verkkoa johtuen siitä, että aiemmissa kytkimissä ei ole ollut IPv6-ominaisuutta tuettuna.

Myös yhtenä mielenkiintoisena vikana löydettiin viallinen SFP-moduuli lisättäessä kytkintä verkkoon. Kun keskipistekytkimen vapaaseen SFP-porttiin kytkettiin moduuli kaatui koko kytkin. Tuulettimet puhalsivat täydellä teholla ja kaikki ledit sammuivat. Onneksi vain pinon toinen kytkin kaatui. Samalla saatiin varmuus että kyseinen keskipistekytkin toimii varmistuksien osalta juuri kuten oli suunniteltu.

5 YHTEENVETO

Työn tärkeimpänä tavoitteena oli suunnitella ja toteuttaa kohteeseen luotettava, turvallinen ja helposti ylläpidettävä langaton lähiverkko. Käytännössä työn laajuus venyi kuitenkin koskemaan myös kiinteää lähiverkkoa sekä muutamia valvontajärjestelmiä, jotka olivat tarpeellisia. Lähtökohdat suunnittelulle ja toteutukselle olivat hyvät, koska kyseessä oli rakenteilla oleva kohde ja esimerkiksi kaapelointiin pystyttiin vaikuttamaan helposti.

Verkko saatiin toimintakuntoon ja tuotantoon aikataulussa, mutta muutamia kehityskohteita jäi tulevaisuuteen. Isoimpana asiana 802.1x-todennuksen käyttöönotto. Tätä työtä tehdessä kuitenkin sain ainakin pintaraapaisun kyseisestä todennustavasta ja pystyn toteuttamaan tarvittaessa todennuksen LAN-verkossa. Työ jatkuu kehittämisen ja verkon ylläpidon osalta koko ajan.

Yhteenvetoa kirjoitettaessa verkko on ollut tuotantokäytössä jo useampia kuukausia. Alun ongelmien jälkeen käyttäjien suunnalta ei ole juurikaan tullut valituksia. Muutamia yksittäisiä vikatilanteita on ollut, mutta nämä ovat olleet yleensä operaattorin verkossa.

Opinnäytetyö antoi itselle valmiuksia myös palvelimien kanssa toimimiseen ja myös pienen kipinän kotipalvelimen pyörittämiseen. Tämä toteutui siten, että valjastin yhden vanhan pöytäkoneen VMWARE ESXi 6.0 -virtualisointialustaksi, jossa virtuaalikoneina ajetaan sekä Ubuntu- että CentOS -palvelimia. Nämä ovat lähinnä oppimis- ja testauskäytössä tällä hetkellä, mutta tulevaisuudessa mahdollisesti myös kotiverkon tuotannossa.

LÄHTEET

1. Schneider, Kenneth S. Fiber Optic Communications for the Premises Environment. Telebyte. Saatavissa: http://www.telebyteusa.com/foprimer/foch4.htm. Hakupäivä 10.4.2016.

2. Common-network-topologies.png. Conceptdraw. Saatavissa: http://www.conceptdraw.com/How-To-Guide/picture/Common-network-topologies.png. Hakupäivä 6.11.2016

3. Lapukhov, Petr 2008. Private VLANs Revisited. Ine Blog. Saatavissa: http://blog.ine.com/2008/07/14/private-vlans-revisited/. Hakupäivä 21.4.2016.

4. Helping Define IEEE 802.11 and other Wireless LAN Standards. Intel. Saatavissa: http://www.intel.com/content/dam/www/public/us/en/documents/case-studies/802-11-wireless-lan-standards-study.pdf. Hakupäivä 10.4.2016.

5. Poole, Ian. Wi-Fi/WLAN Channels, Frequencies, Bands & Bandwidths. Radio-Electronics. Saatavissa: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php. Hakupäivä 27.11.2016.

6. Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä. 2016. Viestintävirasto. Saatavissa: https://www.viestintavirasto.fi/attachments/maaraykset/Viestintavirasto_15AJ2016M.pdf. Hakupäivä 11.12.2016.

7. Different Wifi Protocols and Data Rates. 2016. Intel. Saatavissa: http://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000005725.html. Hakupäivä 27.11.2016.

8. Geier, Eric 2013. All about beamforming, the faster Wi-Fi you didn't know you needed. PCWorld. Saatavissa: http://www.pcworld.com/article/2061907/all-about-beamforming-the-faster-wi-fi-you-didnt-know-you-needed.html. Hakupäivä 27.11.2016.

9. WLAN-salaus salaa vain radioliikenteen. 2014. Viestintävirasto. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409091046.html. Hakupäivä 10.4.2016.

10. Phifer, Lisa 2010. Top Ten Wi-Fi Security Threats. eSecurity Planet. Saatavissa: http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm. Hakupäivä 21.4.2016.

11. Niinimäki, Arttu 2012. WPA/WPA2-salausprotokollien erityispiirteet. Tampereen Teknillinen Yliopisto. Saatavissa: https://wiki.tut.fi/Tietoturva/Tutkielmat/WPAWPA2SalausprotokollienOminaispiirteet. Hakupäivä 21.4.2016.

12. Configuring IEEE 802.1x Port-Based Authentication. Cisco. Saatavissa: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.pdf. Hakupäivä 5.10.2016.

13. Cudbard-Bell Arran 2010. 802.1x_wired_protocols.png. Wikipedia. Saatavissa: https://en.wikipedia.org/wiki/IEEE_802.1X#/media/File:802.1X_wired_protocols.png. Hakupäivä 10.10.2016.

14. Banks, Ethan 2012. Five Things to Know About DHCP Snooping. Packetpushers. Saatavissa: http://packetpushers.net/five-things-to-know-about-dhcp-snooping/. Hakupäivä 10.10.2016.

15. DHCP & DNS. Study CCNA. Saatavissa: http://study-ccna.com/dhcp-dns/. Hakupäivä 4.12.2016.

16. Cisco Aironet Universal AP Priming And Cisco AirProvision User Guide. 2015. Cisco. Saatavissa: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html#pgfId-89802. Hakupäivä 29.10.2016.

17. N+1 High Availability Deployment Guide. 2016. Cisco. Saatavissa: http://www.cisco.com/c/en/us/td/docs/wireless/technology/hi_avail/N1_High

_Availability_Deployment_Guide/N1_HA_Overview.html. Hakupäivä 11.10.2016.

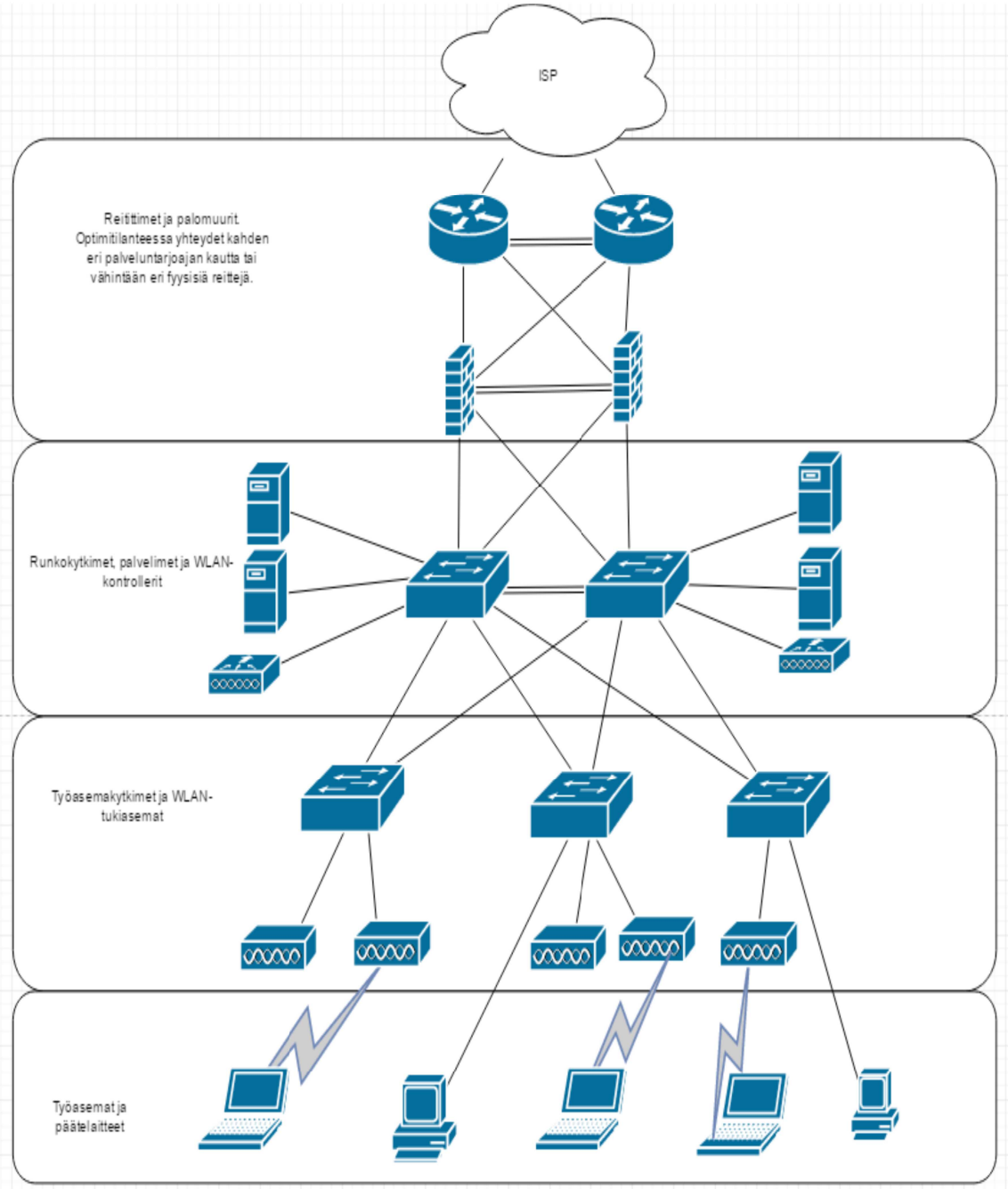
18. Wireless LAN Controller (WLC) Mobility Groups FAQ. 2008. Cisco. Saatavissa: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107188-mobility-groups-faq.html. Hakupäivä 21.12.2016.

19. Premachandran, Rajesh 2015. Difference between Coverage hole and Pre-Coverage hole. Cisco Support Community. Saatavissa: https://supportforums.cisco.com/document/52706/difference-between-coverage-hole-and-pre-coverage-hole. Hakupäivä 6.11.2016.

20. Rogue Management in a Unified Wireless Network. 2010. Cisco. Saatavissa: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html. Hakupäivä 6.11.2016.

21. Rogue Detection under Unified Wireless Network. 2007. Cisco. Saatavissa: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html. Hakupäivä 6.11.2016.

Vikasietoisen verkon periaatekuva **Liite 1**



Periaatekuva organisaation sisäverkosta. Verkko jaettu 4 segmenttiin sekä kaikki kriittiset komponentit kahdennettu: Reitittimet, palomuurit, runkokytkimet, palvelimet ja wlan-kontrollerit sekä kaikki runkoyhteydet. Fyysiset yhteydet voivat olla joko kuitu- tai kuparipohjaisia.

Kytkinten linkkiaggregaatiokonfiguraatio. **Liite 2 / 1**

Linkkiaggregaation luominen kytkimille

ZTE 5250

```
 set lacp enable
 set lacp aggregator 1 mode static
 set lacp aggregator 1 add port 25-26
 set lacp port 25-26 mode passive
 create vlan 10 name sisaverkko
 set vlan 10 add trunk 1 tag
 set vlan 10 enable
```

Cisco 2960

```
interface Port-channel1
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet0/6
 description to lacp_zte_26
 switchport mode trunk
 channel-group 1 mode on
!
interface GigabitEthernet0/7
 description to lacp_zte_25
 switchport mode trunk
 channel-group 1 mode on
```

ZTE 5250

```
testi-sw2(cfg)#show lacp
 Lacp is enabled.
 Lacp priority is 32768.
 Load-balance is based on L2 hash mode.
```

PortNum	GroupNum	GroupMode	LacpTime	LacpActive
25	1	Static	Long	False
26	1	Static	Long	False

Cisco 2960

```
kytkin#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -       Gi0/6(P)    Gi0/7(P)
```