KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Joni Hakkarainen & Pasi Vanhala

REDUNDANTTISUUS KONTROLLERIPOHJAISESSA LANGATTOMASSA LÄHIVERKOSSA

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

HAKKARAINEN, JONI & VANHALA, PASI

	Redundanttisuus kontrolleripohjaisessa langattomassa lähiverkossa
Opinnäytetyö	32 sivua + 9 liitesivua
Työn ohjaaja	yliopettaja Martti Kettunen
Toimeksiantaja	SimuNet-hanke
Huhtikuu 2011	
Avainsanat	WLAN, langattomat lähiverkot, vikasietoisuus, redundanttisuus, WLC, kontrolleri

Opinnäytetyön tavoitteena oli rakentaa Kymenlaakson ammattikorkeakoulun tiloihin vikasietoinen eli redundanttinen kontrolleripohjainen langaton lähiverkko. Työ on osa SimuNet-hanketta, koska opinnäytteen lopputuloksena tutkittu ja testattu laitteisto kytketään myöhemmin osaksi SimuNet-laboratoriota. Tarkoituksena oli saavuttaa riittävä redundanttisuus, jotta toisen keskitetyn verkko-ohjaimen eli kontrollerin vikaantuminen ei näkyisi käyttäjälle saakka kuin korkeintaan lyhyenä katkoksena. Erityisesti kiinnitettiin huomiota siihen, että langattoman lähiverkon käyttäjän ei tarvitse tehdä toimenpiteitä toiminnallisuuden palauttamiseksi.

Työssä käytettiin kahta reitittimiin asennettua kontrollerimoduulia ja itse reitittimet asetettiin kontrollerimoduulien aiheuttamien rajoitusten vuoksi siltaavaan tilaan. Lisäksi kytkentään kuului yksi Internetiä simuloiva reititin, yksi kytkin, virtuaaliselta Linux-koneelta ajettava DHCP-palvelin sekä neljä tukiasemaa.

Tavoitteisiin päästiin laitteiston aiheuttamista rajoituksista huolimatta. Lopullisessa kytkennässä kontrollerin vikaantumisesta käyttäjälle koituva katkos oli noin puoli minuuttia. Kyseessä on kuitenkin harvoin toistuva tapahtuma, joten katkoksen kesto on hyväksyttävissä.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

HAKKARAINEN, JONI & VANHALA, PASI

	Redundancy in Controller Based Wireless Local Area Network
Bachelor's Thesis	32 pages + 9 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	SimuNet Project
April 2011	
Keywords	WLAN, WLC, redundancy, controller, wireless local area network

The object of this thesis work was to build a duplicated controller based wireless local area network. The network was built in Kymenlaakso University of Applied Sciences' networking laboratory. The thesis work was a part of the SimuNet project because the network built and studied for the thesis work will become part of the SimuNet laboratory's network. The main goal was to achieve necessary redundancy so if the other controller fails, the failure will not have a significant effect on the end user. Attention was especially paid to eliminate the need for end user's actions to restore connectivity.

The network studied in the thesis work was built by using two router-based controller modules. Because of the limitations of these modules, the routers were configured as bridges. The network also uses a router to simulate the Internet, one switch, a virtual Linux-based DHCP server and up to four access points.

The goal was achieved despite the limitations of equipment used. In the final configuration the failover time was about 30 seconds. Controller failure is a rarely occurring event so the failover time is acceptable.

SISÄLLYS

KÄYTETYT KÄSITTEET JA LYHENTEET

AP	Access Point Tukiasema
Bug	Bugi Virhe ohjelmistossa
CUWN	Cisco Unified Wireless Network Ciscon kehittämä järjestelmäkokonaisuus langattomien verkkojen hallintaan
DHCP	Dynamic Host Configuration Protocol IP-osoitteiden jakamiseen käytettävä verkkoprotokolla
Daemon	Disk And Execution MONitor Palveluprosessi UNIXissa
DNS	Domain Name System Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi
Firmware	Laitteen ohjelmisto, joka on tallennettu sen häviämättömään muistiin.
IP	Internet Protocol Internet-protokolla
LAN	Local Area Network Lähiverkko
LAP	Lightweight Access Point Ciscon nimitys langattomalle tukiasemalle
LWAPP	Lightweight Wireless Access Point Protocol Protokolla, jolla tukiasemat ovat yhteydessä kontrolleriin
MAC-osoite	Media Access Control Verkkolaitteen fyysinen osoite
MIMO	Multiple-Input Multiple-Output Tekniikka, jossa lähetykseen ja vastaanottamiseen käytetään useampaa kuin yhtä antennia
MPLS	Multiprotocol Label Switching Menetelmä, jolla kuljetetaan IP-paketteja solmujen kautta ilman, että solmujen tarvitsee tehdä reititystä

OSI	Open Systems Interconnection Reference Model Viitemalli, joka kuvastaa tiedonsiirtoprotokollia seitsemäs-sä kerroksessa
PoE	Power over Ethernet Tekniikka, jolla voidaan syöttää käyttöjännite verkkokaa-pelin avulla
Power Injector	Laite, jolla voidaan syöttää käyttöjännite yhdelle laitteelle
RADIUS	Remote Authentication Dial In User Service Tunnistukseen käytettävä protokolla
RF	Radio Frequency Radiotaajuus
SNMP	Simple Network Management Protocol TCP/IP-verkkojen hallintaan käytettävä protokolla
Telnet	Yhteysprotokolla pääteyhteyksiin Internetin ylitse.
VCI	Vendor Class Identifier Mallikohtainen uniikki merkkijono
VPLS	Virtual Private LAN Service Palvelu, jonka avulla voidaan liittää useita eri puolella MPLS-verkkoa sijaitsevia Ethernet-lähiverkkoja L2-tasolla toisiinsa
VLAN	Virtual LAN Virtuaalinen lähiverkko
WLAN	Wireless Local Area Network Langaton lähiverkko
WLC	Wireless LAN Controller Kontrollerilaite, jolla hallitaan langattomia tukiasemia

1 JOHDANTO

Lähiverkkojen mobiliteetin tarve on jatkuvassa kasvussa. Nykyisin langattomalla tekniikalla saavutetaan riittäviä nopeuksia, mikä osaltaan lisää vielä langattomien verkkojen suosiota. Teollisuus- ja yritysverkoissa ei kuitenkaan ole järkevää käyttää kodeista tuttua yksittäisen langattoman tukiaseman mallia, vaan on syytä löytää paremmin hallittavissa oleva ja vikasietoinen eli redundanttinen ratkaisu. Keskitettyjä verkko-ohjaimia eli kontrollereja käyttämällä saavutetaan riittävä vikasietoisuus ja verkon hallinta helpottuu huomattavasti, kun jokaista tukiasemaa ei tarvitse konfiguroida yksitellen. Kontrollerien avulla tukiasemien konfigurointi tapahtuu keskitetysti.

Opinnäytetyön tavoitteena oli rakentaa vikasietoinen langattoman verkon ratkaisu Kymenlaakson ammattikorkeakoulun tietoliikennelaboratorioon käyttäen jo olemassa olevia laitteita. Vähimmäisvaatimuksena verkon tuli kestää toisen kontrollerin vikaantuminen ilman merkittävän katkoksen syntymistä. Redundanttisuutta varten käytettiin verkossa kahta kontrolleria. Käytetyt kontrollerit eivät olleet erillisiä laitteita vaan Ciscon 2800-sarjan reitittimiin asennettuja moduuleita. Tästä johtuen työ toteutettiin muuntamalla reitittimet, joihin kontrollerit oli asennettu, siltaavaan tilaan. Tämä tarkoitti käytännössä sitä, että reitittimet olivat vain kontrollerikäytössä, eikä reititystoimintoja voitu käyttää. Lisäksi työssä tarvittiin yhtä verkkokytkintä, yhtä Internet-yhteyttä simuloivaa reititintä, sekä Linux-pohjaista DHCP-palvelinta, joka asennettiin KyAMK:n tietoverkkotekniikan laboratorion virtuaalipalvelimelle. Käytössä oli myös kahdesta neljään tukiasemaa.

Työssä kuvattu kytkentä on osa suurempaa SimuNet-kokonaisuutta, johon liittyy myös useita muita opinnäytetöitä. SimuNet on Kymenlaakson ammattikorkeakoulun tiloihin rakennettu testi- ja T&K&I -verkko jolla pyritään simuloimaan todellisen verkko-operaattorin runkoverkkoa. SimuNet on myös eristetty koulun tuotantoverkosta. Kontrollerit on tarkoitus myöhemmin sijoittaa simuloidusti kahteen eri maantieteelliseen sijaintiin ja tähän tarvittavat SimuNet-verkon virtuaaliyhteydet ovat tärkeä osa tätä toteutusta, mutta ne jätettiin aikataulusyistä tämän opinnäytetyön ulkopuolelle.(1.)

2 802.11-STANDARDIT

Langattomat verkot koostuvat useista standardeista, joten IEEE-standardointiryhmä on koonnut kaikki langattomat standardit yhteisen 802.11-nimittäjän alle. Alkuperäinen IEEE 802.11 hyväksyttiin vuonna 1997, ja se on alun perin vuonna 1990 esitellyn standardin seuraaja. Standardi on vuosien myötä kokenut monia muutoksia, joissa on muun muassa nostettu nopeuksia. Uusin perusstandardi 802.11:ta on 802.11-2007, ja se sisältää kaikki nykyiset variaatiot. Alkuperäisen 802.11:n ominaisuuksia olivat 2,4 GHz:n taajuusalue, 1 Mbit/s tai 2 Mbit/s-nopeus ja kantavuus olosuhteista riippuen 50 metristä 180 metriin (sisätiloissa) ja ulkotiloissa jopa 300 metriä. Langattomien verkkojen ollessa kyseessä täytyy muistaa, että maksimikantamiin ja -nopeuksiin päästään vain harvoin, sillä verkot joutuvat etenkin sisätiloissa läpäisemään runsaasti eri materiaaleja ja erilaiset sähkölaitteet saattavat aiheuttaa häiriöitä.(2.)

Taulukko 1. 802.11-standardit tietoineen (2)

Standardi	**Ratifioitu**	**Teoreettinen maksiminopeus**	**Taajuusalue**	**Kanavia**	**Ei-päällekkäisiä kanavia**
802.11	1997	2 Mbit/s	2,4 GHz	14	3
802.11a	1999	11 Mbit/s	5 GHz	14	3
802.11b	1999	54 Mbit/s	2,4 GHz	12	12
802.11g	2003	54 Mbit/s	2,4 GHz	12	3
802.11n	-	300+ Mbit/s	2,4 GHz, 5 GHz	-	-

2.1 802.11a-standardi

802.11a on vuonna 1999 ratifioitu laajennus alkuperäiseen 802.11-standardiin. A-standardi toimii aiemmista standardeista poiketen 5 GHz:n taajuudella ja nopeus on 6 Mbit/s ja 54 Mbit/s välillä. 802.11a-standardin heikkous on pieni, noin 80 metrin kan-

tama, jossa yhteyden nopeus putoaa kantaman heikentyessä. Lisäksi yhteensopivuusongelmia on syntynyt käytetystä taajuusalueesta.(2.)

2.2 802.11b-standardi

802.11b on vuonna 1999 ratifioitu laajennus alkuperäiseen 802.11-standardiin. B-standardin mukaiset laitteet operoivat 2,4 GHz taajuudella ja kykenevät korkeintaan 11 Mbit/s nopeuksiin. B-standardin mukaiset laitteet voivat operoida joko, 1, 2, 5,5 tai 11 Mbit/s nopeuksilla. 802.11b-standardin mukaisten laitteiden kantavuus on sisätiloissa noin 50–180 metriä ja ulkotiloissa sama kuin alkuperäisessä 802.11-standardissa, eli jopa 300 metriä.(2.)

2.3 802.11g-standardi

802.11g ratifioitiin vuonna 2003, ja se käyttää b-standardin tavoin 2,4 GHz taajuutta. Nopeudeltaan 802.11g-verkko yltää samoihin lukemiin a-standardin kanssa mutta tästä poiketen taajuudesta ei synny yhteensopivuusongelmia ja kantomatka on huomattavasti korkeampi, eli sisätiloissa 50–180 metriä ja ulkotiloissa saatetaan päästä yli 300 metriin.(2.)

2.4 802.11n-standardi

Pitkään kehitetty 802.11n julkaistiin vihdoin vuonna 2009, mutta sitä ei vielä ole ratifioitu. N-standardi toimii 2,4:n ja 5 GHz taajuudella ja kykenee jopa 300 Mbit/s nopeuksiin. Huippunopeuksiin vaaditaan kuitenkin MIMO-yhteensopiva laite tai tuki 802.11n-standardin ominaisuudelle, jossa vierekkäiset kanavat sidotaan yhteen 40 MHz:n taajuudella.(2.)

3 REDUNDANTTISUUS

Redundanttisuus (engl. redundancy), joka on tärkeä osa vikasietoisuutta, on keino lisätä järjestelmän luotettavuutta. Siinä järjestelmän kannalta kriittiset komponentit on kahdennettu (duplicated) tai jopa kolmennettu (triplicated), jolloin vian sattuessa varalla oleva komponentti ottaa tehtävän hoitaakseen.

Nykyisin tietoverkossa palveluiden luotettavuus on ehdottoman tärkeätä, näin on myös langattomissa verkoissa. Palveluun ei saa tulla pitkää katkosta vaikka jokin laitteista vikaantuisi.

Työssä käytetyissä Ciscon WLAN-kontrollereissa redundanttisuus hoidetaan asentamalla verkkoon toinen (tai useampi) samanlainen kontrolleri, joka ottaa ensisijaisen kontrollerin (primary controller) tehtävät hoitaakseen, mikäli se vikaantuu. Lähtötilanteessa kaikki tukiasemat ovat rekisteröityneet ensisijaiselle kontrollerille. Ensimmäisen kontrollerin vikaantuessa tai yhteyden katketessa siihen tukiasemat automaattisesti siirtyvät toisen kontrollerin hallintaan. Tässä tilanteessa lyhyttä katkosta ei siis voida välttää. Voidaan kuitenkin minimoida failover-aika, eli aika, joka tukiasemilta kestää havaita katkos, siirtyä varakontrollerille ja olla jälleen asiakkaiden käytettävissä. Käytännössä failover-aika on pienimmillään 30 sekunnin luokkaa. Tätä alemmas ei ole järkevä mennä, sillä silloin tukiasemat havaitsevat pienetkin yhteyshäiriöt liian nopeasti ja siirtyvät toiselle kontrollerille vaikka häiriöstä johtuva katkos ei edes näkyisi asiakkaalle asti. Ensisijaisen kontrollerin palatessa takaisin toimintaan tukiasemat palaavat yhteyteen siihen.(3.)

4 KONTROLLERIN JA TUKIASEMAN YHTEYS

Langattomien verkkojen merkitys ja käyttöaste on nykyään niin suuri, että perinteisen tukiasemat eivät enää yksinään selviä verkon ylläpitämisestä. Ratkaisuna tähän ongelmaan Cisco Systems on kehittänyt CUWN-järjestelmän, jolla pyritään helpottamaan suurten langattomien verkkojen ylläpitoa. Kontrolleri, eli WLC on keskeinen osa CUWN-järjestelmää.(4.)

Kontrollerien käyttö mahdollistaa tukiasemien, eli LAP-yksiköiden sijoittamisen maantieteellisesti hyvinkin laajalle alueelle. Tukiasemat muodostavat tunneloidun yhteyden kontrolleriin ja kaikki konfigurointi suoritetaan keskitetysti kontrollerin kautta. Tarvittaessa tukiasemat myös lataavat kontrollerilta uudemman ohjelmiston. Keskitetty konfigurointi ja niin sanotut tyhmät tukiasemat mahdollistavat langattoman verkon helpon laajentamisen sekä ylläpidon.

Kun tukiasema kytketään verkkoon, seuraa monivaiheinen prosessi jossa tukiasema pyrkii löytämään kontrollerin. Tukiasema lähettää DHCP-palvelimelle pyynnön IP-

osoitteesta, mikäli osoitetta ei ole ennestään määritetty. Osoitteen saamisen jälkeen tukiasema aloittaa kontrollerin etsimisen lähettämällä LWAPP-kyselyn. Kontrolleri vastaa tähän LWAPP-vastauksella. Tukiasema valitsee LWAPP-vastausten perusteella kontrollerin johon liittyy ja lähettää kontrollerille LWAPP-liittymispyynnön. Seuraavaksi kontrollerin tulee vahvistaa liittyminen ja lähettää tukiasemalle liittymisvahvistuksen. Kun tukiasema vastaanottaa liittymiskutsun, seuraa vahvistusoperaatio jossa verrataan autentikointi- ja salausavaimia. Lopuksi tukiasema rekisteröityy kontrolleriin.(5.)

Edellä mainitussa operaatiossa on suurimpana ongelmana se, mistä tukiasema tietää mihin lähettää ensimmäisen LWAPP-kyselyn. Cisco on ratkaissut ongelman käyttämällä tukiasemissa erityistä hakuprosessia ja tiettyjä algoritmeja. Hakuprosessi alkaa tukiaseman pyytäessä itselleen IP-osoitetta DHCP-palvelimelta. Mikäli tukiasema on konfiguroitu käyttämään OSI-mallin toista kerrosta, lähettää se LWAPP-kyselyn sisällytettynä toisen kerroksen LWAPP-kehykseen. Mikä tahansa verkkoon yhteydessä oleva kontrolleri, joka on konfiguroitu toisen kerroksen LWAPP-tilaan vastaa kyselyyn toisen kerroksen LWAPP-vastauksella. Mikäli tukiasema ei ole konfiguroituna käyttämään OSI-mallin toista kerrosta tai jompikumpi ei saa LWAPP-viestejä, siirtyy tukiasema lähettämään OSI-mallin kolmannen kerroksen mukaisia LWAPP WLC –pyyntöjä. Kolmannen kerroksen LWAPP-kysely alkaa kyselyviestillä samassa aliverkossa oleville kontrollereille. Kolmatta kerrosta käyttävät kontrollerit vastaavat tukiasemalle LWAPP-kyselyn unicast-vastauksella. Jos tämä epäonnistuu, alkaa prosessi alusta IP-osoitteen pyytämisellä.(5.)

On myös mahdollista konfiguroida DHCP-palvelin antamaan tukiasemille kontrollerin osoitteen. Tämä tapahtuu käyttämällä erityistä Option 43 -valintaa DHCP:n konfiguraatiossa. Tällöin DHCP-palvelin lähettää kontrollerin osoitteen sisällytettynä tukiasemalle lähetettävään DHCP-vastaukseen.(5.)

Alla esimerkki tukiaseman onnistuneesta liittymisestä kontrollerille:

Mar 1 00:00:10.890: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
**Mar 1 00:00:10.920: bsnUnlockDevice: not bring radio up: radio 1 is in admin disable state*
**Mar 1 00:00:10.965: %SSH-5-ENABLED: SSH 2.0 has been enabled*

**Mar 1 00:00:10.966: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up*
**Mar 1 00:00:11.274: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset*
**Mar 1 00:00:11.745: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed state to up*
**Mar 1 00:00:11.968: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down*
**Mar 1 00:00:12.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset*
**Mar 1 00:00:12.278: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to down*
**Mar 1 00:00:12.526: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up*
**Mar 1 00:00:13.526: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up*
****Mar 1 00:00:19.839: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0 assigned DHCP address 172.16.10.59, mask 255.255.255.0, hostname LWAP2***

**Mar 1 00:00:29.809: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset*
**Mar 1 00:00:29.820: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up*
**Mar 1 00:00:29.991: Logging LWAPP message to 255.255.255.255.*

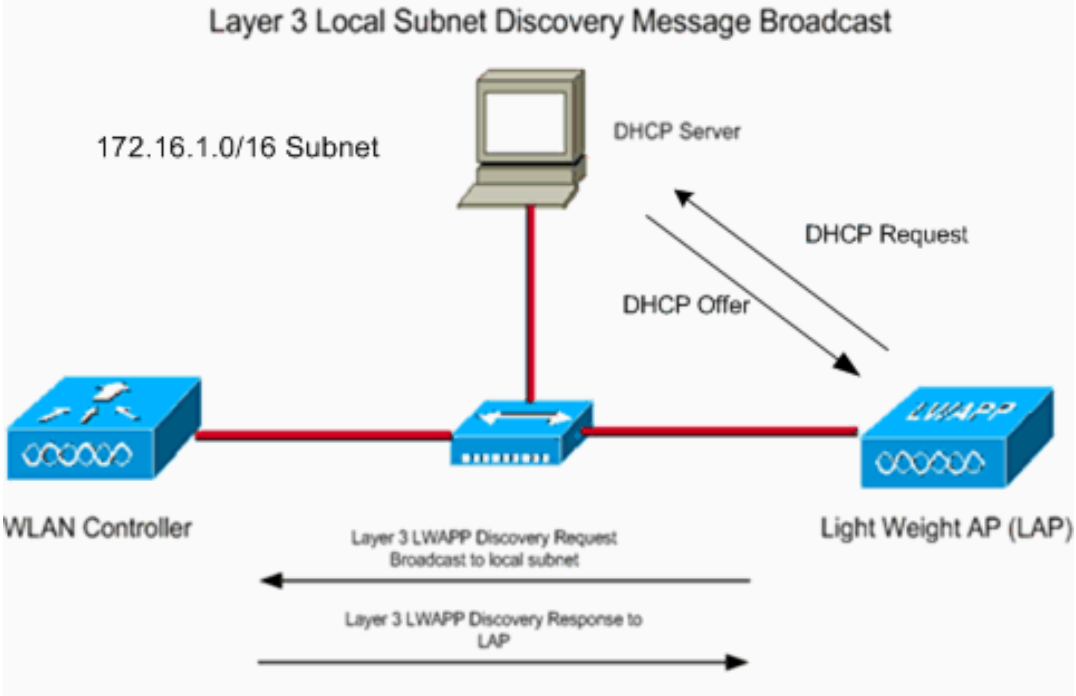
**Mar 1 00:00:30.047: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - CLI initiated*
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

Translating "CISCO-LWAPP-CONTROLLER"...domain server (255.255.255.255)
**Mar 1 00:00:49.790: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER*

**Mar 1 00:00:58.791: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-LWAPP-CONTROLLER*
****Mar 1 00:01:10.793: %CAPWAP-3-ERRORLOG: Go join a capwap controller***
****Apr 5 08:34:29.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 172.16.10.10 peer_port: 5246***
**Apr 5 08:34:30.001: %CAPWAP-5-CHANGED: CAPWAP changed state to*
****Apr 5 08:34:31.927: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 172.16.10.10 peer_port: 5246***
****Apr 5 08:34:31.929: %CAPWAP-5-SENDJOIN: sending Join Request to 172.16.10.10***
****Apr 5 08:34:31.929: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN***
****Apr 5 08:34:32.019: %CAPWAP-5-CHANGED: CAPWAP changed state to CFG***
**Apr 5 08:34:32.223: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset*
****Apr 5 08:34:32.233: %CAPWAP-5-CHANGED: CAPWAP changed state to UP***
**Apr 5 08:34:32.234: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to administratively down*

**Apr 5 08:34:32.234: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up*
****Apr 5 08:34:32.242: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller Primary***

Myös DNS-palvelimen käyttö tukiasemien ja kontrollerin yhteyden muodostuksessa on mahdollista. Tällöin tulee konfiguroida Option 15 -valinta DHCP-palvelimen konfiguraatioon. Tällöin tukiasemat saavat tiedon verkon nimestä sekä DNS-palvelimen IP-osoitteesta sisällytettynä DHCP-vastaukseen. Tukiasemat lähettävät DNS-palvelimelle nimikyselyn CISCO-LWAPP-CONTROLLER.localdomain (localdomain kuvastaa verkon nimeä, esimerkiksi ictlab.kyamk.fi). Vastauksena kyselyyn DNS-palvelin antaa tukiasemille kontrollerin osoitteen ja näin ollen tukiasema pystyy lähettämään OSI-mallin kolmannen kerroksen mukaisen unicast-LWAPP -kyselyn kontrollereille. Kaikki kontrollerit jotka saavat pyynnön, vastaavat tukiasemille unicast-löytymisviestillä.(5.)



Kuva 1. Tukiaseman rekisteröityminen kontrollerille (4)

5 KONTROLLERITEKNIIKAN HYÖDYT

Perinteiset WLAN-ratkaisut rakentuvat suurilta osin perinteisistä tukiasemista, jotka toimivat itsenäisesti. Näitä perinteisiä tukiasemia, joita hallinnoidaan ja konfiguroi-

daan erillisinä, kutsutaan myös ”fat” tukiasemiksi. Ajan kuluessa ja yrityksen kasvaessa, palkatessa uutta henkilöstöä tai muuttaessa toisiin tiloihin on myös langattoman verkon vastattava näihin vaatimuksiin ja haasteisiin. Taulukkoon 2 on koottu joitakin langattoman verkon tilanteita, ja se, kuinka ne hoidetaan perinteisessä tukiasemaratkaisussa.(6.)

Taulukko 2. Langattoman yritysverkon vaatimuksia.(6)

Tilanne	**Kuvaus**	**Perinteinen tukiasemaratkaisu**
Hallinnointi ja seuranta	Kustannustehokas hallinta, seuranta ja levittäminen	Käytä skriptiä tai SNMP-ratkaisua WLAN:in monitorointiin ja konfiguroi jokainen tukiasema erikseen.
Päivityskustannukset	Uusien tukiasemien lisääminen verkkoon ja vanhojen ohjelmistojen päivittäminen	On asennettava erikseen jokin kolmannen osapuolen verkonhallintaohjelmisto, lisäkustannus.
Vierailijaverkko	Mahdollisuus tarjota asiakkaille, toimittajille ja partnereille pääsy kontrolloituun ja rajoitettuun langattomaan verkkoon.	Jokaiseen tukiasemaan on erikseen määriteltävä vierailija-VLAN, joka on kuljetettava koko verkon läpi. Ei käyttäjäystävällinen ja vaikea ylläpitää.
RF Suunnittelu	Ymmärtää, kuinka levittää langaton verkkoa muualle rakennukseen.	Käytettävä kolmannen osapuolen suunnitteluohjelmistoa, lisäkustannus.
Kuormantasaus	Automaattinen kuormantasaus tukiasemien välillä.	Erilliset tukiasemat ilmoittavat kuormansa, mutta toiset eivät huomio sitä
Nopea ja turvallinen verkkovierailu (roam)	Saumaton siirtyminen tukiasemalta ja VLAN:ilta toiselle.	Lisättävä tukiasema, joka tukee siltausta ja helpottaa roamausta.
Katkeamaton kantavuus	Langattoman ympäristön välitön omaksuminen	Normaalisti ei tuettuna perinteisissä tukiasemissa.
Vieraan AP:n tunnistaminen	Kyky tunnistaa vieraita tukiasemia ja yhteyksiä	Yksittäistä tukiasemaa voidaan käyttää tunnistuksessa, mutta se heikentää tukiase-

	verkossa.	man suorituskykyä.

Yrityksen kasvaessa on otettava huomioon kolme oleellista seikkaa, jotka ovat levityskustannusten pienentäminen, hallinnan yksinkertaistaminen ja turvallisuus.

5.1 Levityskustannusten pienentäminen

Merkittävä lisäkustannus uusien tukiasemien levittämisessä ympäristöön on esiasennuksen yhteydessä suoritettava site-survey (mihin uudet tukiasemat sijoitetaan), uusien kaapelien sekä sähkön vetäminen tukiasemille ja valmiin infrastruktuurin konfiguroiminen uusia tukiasemia varten.(6)

WLAN-kontrollerit poistavat site-surveyn tarpeen kokonaan, sillä niissä on usein mukana kehittynyt suunnitteluohjelmisto ja/tai algoritmi, jolla lähetystehot saadaan säädettyä sopivaksi jokaiselle tukiasemalle. Lisäksi tukiasemat saavat sähkönsä PoE-kytkimen kautta, tai tarvittaessa voidaan käyttää erillistä Power Injectoria. Tukiasemia ei tarvitse suoraan kytkeä kontrolleriin, vaan ne voidaan sijoittaa mihin päin verkkoa tahansa. Tällöin kontrolleri säätää automaattisesti lähetystehon, suojausasetukset ja kanavajaon optimoidakseen parhaan suorituskyvyn ja kantavuuden.(6.)

5.2 Hallinnan yksinkertaistaminen

Hallinnan ja vianmäärityksen yksinkertaisuus pohjautuu itsekonfiguroiviin ja itsekorjaantuviin langattomiin verkkoihin. Käyttäjien sekä tukiasemien kaikkien ominaisuuksien, kuten paikan, MAC-osoitteen, kanavan, valmistajan ja statuksen tunteminen helpottaa myös osaltaan verkon ylläpitoa ja vianselvitystä.

Koska kontrolleri on tietoinen verkon RF-ominaisuuksista, on sen helppo havaita häiriöt tukiasemien välillä ja täten säätää niiden lähetystehoa ja kanava-asetuksia automaattisesti. Samalla periaatteella toimii myös tukiasemien tehon lisäys. Kontrollerin huomatessa jonkun tukiaseman hajonneen tai kadonneen verkosta, voi se nostaa muiden tukiasemien lähetystehoa, jolloin hajonneen tukiaseman jättämä aukko paikataan.

5.3 Turvallisuus

Langattoman verkon täytyy samanaikaisesti pystyä autentikoimaan työntekijät ja muut käyttäjät erinäisin tavoin, kuten 802.1x ja captive portal. Langattoman verkon käyttäjiä ei voida kohdella verkossa samoin kuin langallisessa verkossa.

Langattomien verkkojen tapauksessa salausta ei saa lopettaa tukiasemalle, vaan sen on kuljettava omassa putkessaan lankaverkkoa pitkin, eristettynä kuitenkin muusta liikenteestä, kunnes kaikki palomuurin politiikat ovat käytössä.

Lisäksi vieraan tukiaseman havaitseminen ja pysäyttäminen sekä kaikkien hyväksymättömien langattomien yhteyksien pysäyttäminen on tärkeä osa WLAN-turvallisuutta. Kontrollerin täytyy osata päättää, tunnistetaanko tukiasema vieraaksi vai ainoastaan tunkeilevaksi.

Captive Portal on WWW-sivujen kautta toimiva tunnistautumistapa. Se vaatii käyttäjän laitteelta vain WWW-selaimen. Menetelmä on usein käytössä vierailijaverkoissa, jolloin yhdistävät koneet näkevät verkon avoimena. Verkossa liikennöinti on kuitenkin mahdotonta ennen WWW-sivulla tapahtuvaa kirjautumista. Käyttäjä uudelleenohjataan pakotetusti tälle kirjautumissivulle, kun hän pyrkii jollekin toiselle sivulle.

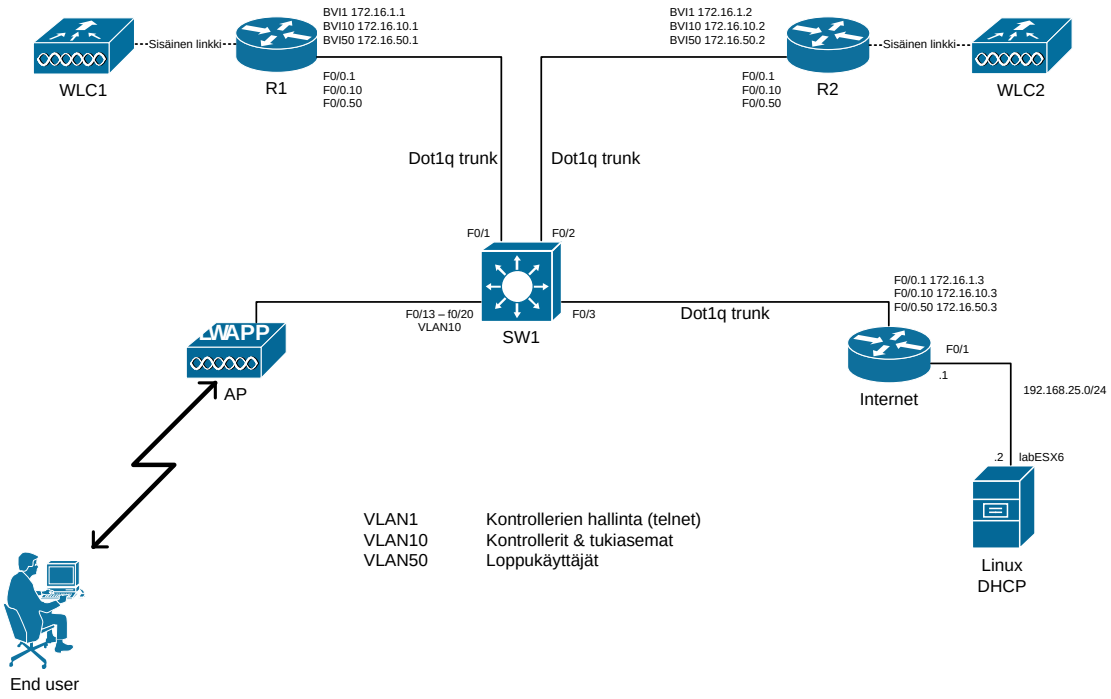
6 VERKKO-OPERAATTORIN NÄKÖKULMA

Kontrollerit voivat sijaita maantieteellisesti eri paikassa kuin itse tukiasemat. Tämä antaa operaattoreille mahdollisuuden asentaa laitteet omaan palvelintilaansa ja yksi suurikapasiteettinen kontrolleri hoitaa monen pienen ja keskisuuren yrityksen langattomat tukiasemat. Käytännössä tämä tapahtuu luomalla kontrolleriin tarvittava määrä VLAN-verkkoja ja SSID-tunnisteita. Tämän jälkeen jokainen SSID ja tukiasemaryhmä liitetään käyttämään haluttua VLANia, jotka sitten tuodaan asiakasyrityksen käyttöön Internetin läpi.

7 KONTROLLERIT AMMATTIKORKEAKOULUN TILOISSA

Työssä käytetyt kontrollerit eivät olleet erillisiä laitteita vaan Ciscon NM-AIR-WLC6 -moduuleita, jotka oli asennettu Ciscon 2811-reitittimiin. Tästä johtuen kontrollerirei-

tittimet tuli muuntaa silloiksi. Sillaksi muuntamisessa reitittimestä pudotetaan kaikki OSI-mallin kolmannen kerroksen mukaiset ominaisuudet. Tämä tapahtuu käskyllä *no ip routing*. Tällä ratkaisulla menetetään kaikki reititystoiminnot mutta pystytään kiertämään laitteiston aiheuttamat ongelmat. Siltauksessa reitittimestä tehdään käytännössä kytkin, ja liikenne kulkee FastEthernet-portista sisään ja kohti sisäistä wlan controller -porttia. Siltaus käynnistetään antamalla laitteelle *bridge irb* -komento. Lisäksi reitittimien FastEthernet- ja wlan-controller -porteille tuli luoda aliliityntäportit 1, 10 ja 50. Nämä puolestaan tuli määritellä vastaaviin bridge-groupeihin. Lisäksi tulee vielä määritellä BVI-liitynnät bridge-groupeille näitä vastaavilla numeroilla sekä antaa näille IP-osoitteet. Nämä toimenpiteet suoritettiin molemmille kontrollerireitittimille. Lisäksi tuli määrittää kytkimelle tarvittavat portit oikeaan VLANiin.



Kuva 2. Valmis kytkentä osoitteineen

Taulukko 3. Siltauskäskyjä

no ip routing	Käsky sammuttaa reitityksen.
bridge irb	Bridge irb on käsky, jolla OSI-mallin toisen kerroksen mukainen laite saadaan siltaamaan kolmannen kerroksen liikennettä. Bridge irb -käsky vaaditaan muun muassa BVI- ja bridge group -käskyihin.(7.)

bridge-group	Bridge-group -käskyn avulla valitaan mitkä liityntäportit kuuluvat siltauksen piiriin. Bridge-groupit määritellään numeroin väliltä 1-255 ja tämä numero määrittää mikä BVI milläkin bridge-groupilla on käytössä.(7),(8)
Interface BVI	BVI eli Bridge Group Virtual Interface on OSI-mallin kolmannen kerroksen mukainen virtuaalinen liityntäportti, joka on yhteydessä bridge groupiin. Koska laite, johon BVI luodaan, ei toimi OSI-mallin kolmannen kerroksen mukaisesti, ottaa BVI nämä toiminnot vastuulleen. BVI, kuten muutkin siltaukseen liittyvät käskyt, vaatii IRB-käskyn antamisen reititinlaitteelle.(7),(8)

Taulukko 4. Työssä käytetyt osoitteet ja DHCP-avaruudet selityksineen

R1 BVI1	172.16.1.1	WLC1 hallinta (CLI)
R1 BVI10	172.16.10.1	Tukiasemia varten luotu virtuaalinen liitäntä, jolla reitittimen f0/0.10 ja kontrollerin wlan-controller1/0.10 on sillattu toisiinsa
R1 BVI50	172.16.50.1	Käyttäjiä varten luotu virtuaalinen liitäntä, jolla reitittimen f0/0.50 ja kontrollerin wlan-controller1/0.50 on sillattu toisiinsa
WLC1 ap-manager	172.16.10.10	Access Pointit ohjataan tähän DHCP-optionilla
WLC1 management	172.16.10.11	WLC1 web-hallinta
R2 BVI1	172.16.1.2	WLC2 hallinta (CLI)
R2 BVI10	172.16.10.2	Sama kuin R1 vastaava
R2 BVI50	172.16.50.2	Sama kuin R1 vastaava

WLC2 ap-manager	172.16.10.12	Access Pointit ohjataan tähän DHCP-optionilla
WLC2 management	172.16.10.13	WLC2 web-hallinta
Internet f0/0.1	172.16.1.3	172.16.1.0/24 yhdyskäytävä
Internet f0/0.10	172.16.10.3	172.16.10.0/24 Tukiasemien yhdyskäytävä
Internet f0/0.50	172.16.50.3	172.16.50.0/24 Käyttäjien yhdyskäytävä
Internet f0/1	192.168.25.1	Liityntä Linuxin suuntaan
Linux	192.168.25.2	DHCP-palvelin
Pool 10	172.16.10.100–172.16.10.250	Access Pointien osoiteavaruus
Pool 50	172.16.50.100–172.16.50.250	End-user -osoiteavaruus

Normaalisti Ciscon IOS olettaa, että kontrollerin hallintaan käytettävä IP-osoite on annettu wlan-controller1/0 -liityntäporttiin, mutta tämä ei siltauksen vuoksi ollut mahdollista. Peruskonfiguroinnin jälkeen osoite siis poistettiin kyseisestä liityntäportista ja jatkossa yhteys muodostettiin telnetiä tai web-hallintaa käyttäen. Peruskonfiguroinnin yhteydessä kontrollerille annettiin käskyt *network telnet enable* joka mahdollistaa telnet-yhteyksien käyttämisen sekä *network webmode enable* joka mahdollistaa web-hallinnan käytön. Lisäksi Ciscon IOS vaatii telnet-yhteyksiä varten salasanojen määrityksen itse reitittimelle.

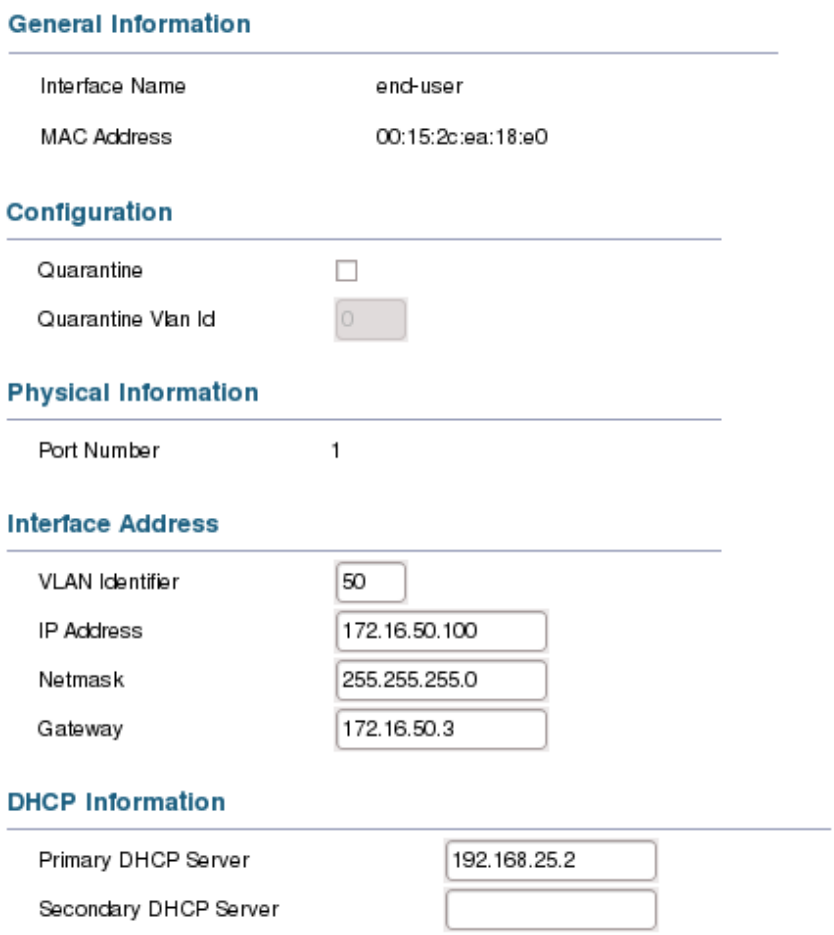
7.1 Kontrollerien konfiguroiminen web-hallinnan kautta

Kontrollerien hallinta on huomattavasti yksinkertaisempaa selkeän web-hallinnan kautta, kuin komentoriviä käyttäen. Tämä korostuu varsinkin päivitettäessä laiteohjelmisto versiosta 5.x versioon 6.0. Yhteensopivuussyistä 802.11a-radiot kytkettiin pois päältä tukiasemista ja työssä käytettiin vain 802.11b/g-radioita.

Ainakin version 6.0 laiteohjelmistolla havaittiin ohjelmistovirhe, jonka vuoksi kaikki toimenpiteet eivät web-hallinnan kautta onnistuneet. Kyseisestä ohjelmistovirheestä kerrotaan tarkemmin kappaleessa 7.1.1.

7.1.1 End-user -liitännän luominen

Ensimmäinen tehtävä on luoda loppukäyttäjille oma liitäntä nimeltä end-user, jonka tehtävänä on ohjata loppukäyttäjät oikeaan DHCP-avaruuteen. Tämä tapahtuu Controller-päävalikon alla sijaitsevalta Interfaces-sivulta.



Kuva 3. End-user -liitännän asetukset

Toissijaiselle kontrollerille määritetään vastaavasti IP-osoitteeksi 172.16.50.101.

End-user -liitännän luominen web-hallinnan kautta aiheuttaa virheen, sillä web-hallinta vaatii IP-osoitteen olevan kontrollerin kanssa samasta verkosta. Liitännän luominen kuitenkin onnistuu, mutta osoitteeksi on ensin annettava jokin muu kuin ha-

luttu. Komentorivin kautta ongelma ei ilmene, joten hienosäätö on suoritettava tätä kautta.

7.1.2 End-user -liitännän yhdistäminen SSID:hen

Seuraava vaihe on liittää juuri luotu end-user -liitäntä haluttuun langattomaan verkkoon. Tämä tapahtuu WLANs-päävalikon Edit-alasivun General-välilehdeltä.

Kuva 4. end-user -liitäntä liitettynä juggernaught-WLAN:iin

Tämän jälkeen muutetaan vielä Security-välilehden takaa löytyvät turva-asetukset haluttuun muotoon. Tämän työn tapauksessa käytettiin ennalta jaettua WPA2-avainta. Tämä tehtiin, koska sopivaa RADIUS-palvelinta ei ollut käytettävissä.

7.2 Redundanttisuuden konfiguroiminen

Kytkennän toimiessa halutulla tavalla yhden kontrollerin osalta oli aika lisätä toinen kontrolleri ja tehdä kytkennästä redundanttinen. Toisen reitittimen ja kontrollerin lisääminen kytkentään oli helppo, sillä konfiguraatio oli IP-osoitteita lukuun ottamatta täysin sama kuin ensimmäinen reitittimen ja kontrollerin tapauksessa.

Jotta redundattisuus saavutetaan, on muutama kohta käytävä läpi:

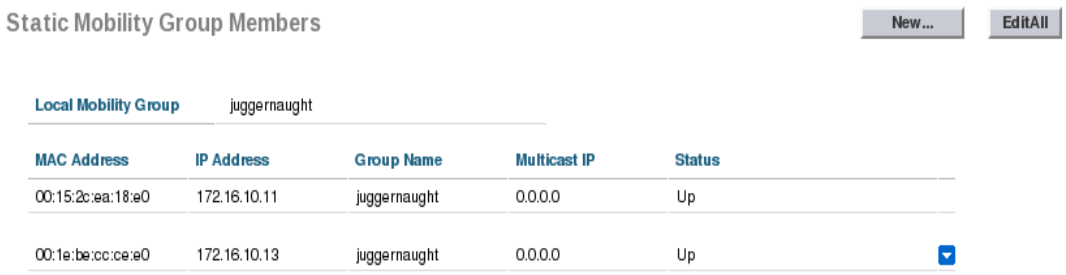
- Mobility groupin konfigurointi kontrollereille
- Ensisijaisen ja toissijaisen kontrollerin määrittämien tukiasemille
- Tukiasemien palaaminen ensisijaiselle kontrollerille

7.2.1 Mobility Group

Mobility, tai roaming, on langattoman asiakkaan kyky pysyä saumattomasti yhteydessä siirryttäessä tukiasemalta toiselle turvallisesti ja mahdollisimman pienellä viiveellä. Seuraavassa on kerrottu, kuinka tämä konfiguroidaan kontrollereille.

Ennen kuin kontrollerit voidaan lisätä mobility groupiin, on niiden nähtävä toisensa verkossa. Tämän voi varmistaa ping-komennolla kontrollerien web-hallinnan kautta toisen kontrollerin IP-osoitetta. Lisäksi jokaiselle kontrollerille on konfiguroitava sama virtuaalinen IP-osoite, joka tässä työssä on 1.1.1.1. Näiden toimenpiteiden jälkeen kontrollerit voidaan liittää mobility groupiin.

Mobility groupin konfigurointi tapahtuu helpoiten web-hallinnan kautta ”Controller”-päävalikon alta löytyvästä ”Mobility Management” -linkistä. Lisätään uusi mobility group, johon kirjoitetaan toisen kontrollerin IP- sekä MAC-osoite. Tämän jälkeen operaatio toistetaan toisella kontrollerilla, johon kirjoitetaan vastaavasti ensimmäisen kontrollerin tiedot. Mobility Groupin toimivuuden voi varmistaa web-hallinnan pääsivulta, johon ilmestyy ilmoitus data ja control pathin muodostumisesta.

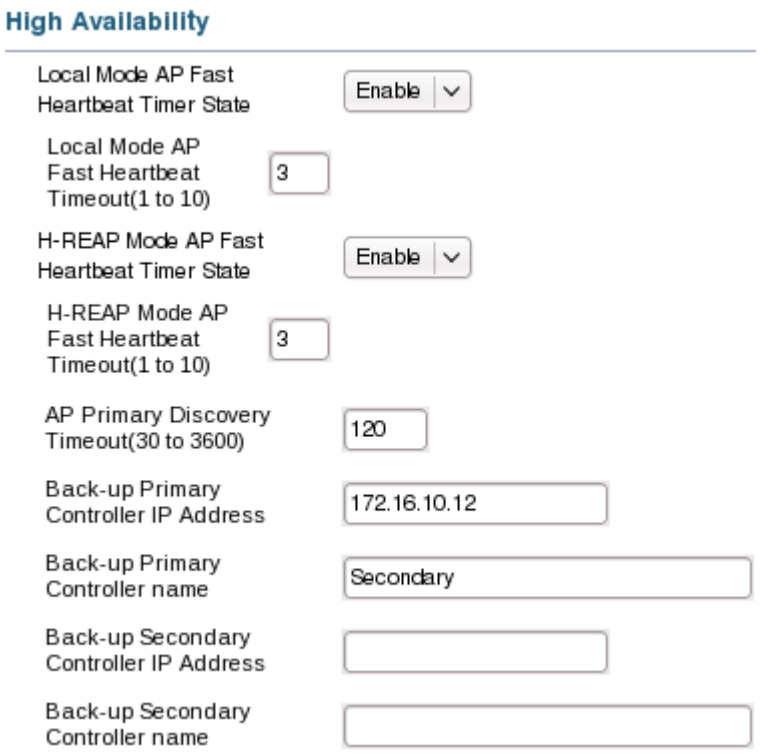


Kuva 5. Primary Kontrollerin Mobility Group -jäsenet

7.2.2 Korkean saatavuuden varmistaminen

Tämä toimenpide määrittää sen kontrollerin, johon tukiasemat ensisijaisesti kytkeytyvät. Päävalikon ”Wireless”-kohdasta valitaan ”Access Points -> Global Configurati-

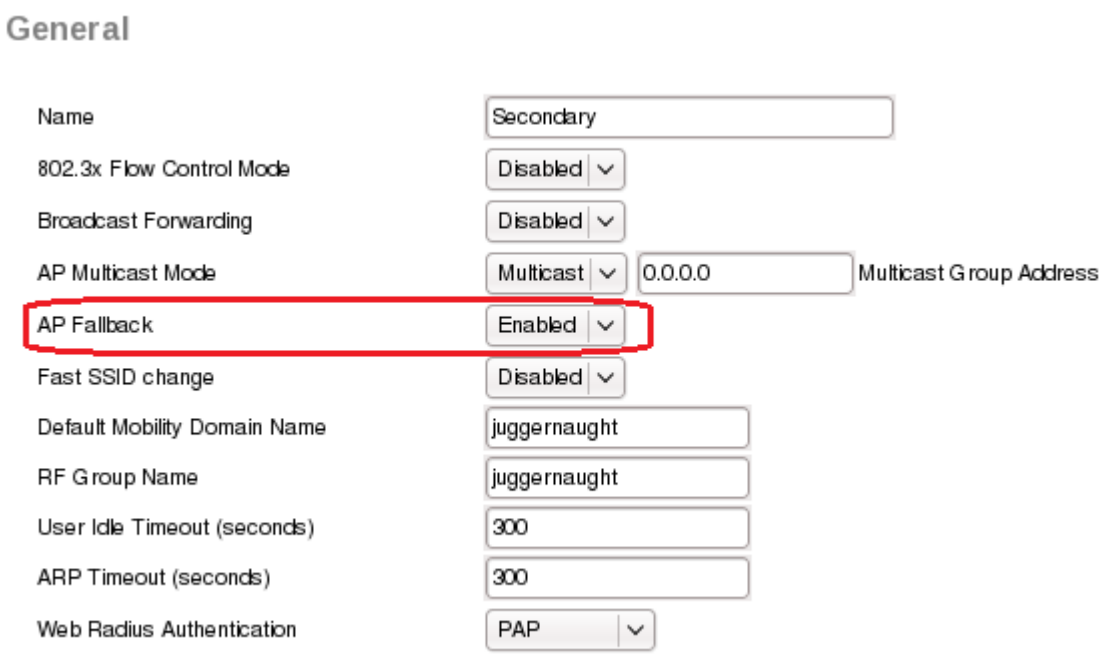
on”, jonka alle määritetään kontrollerien nimet niille varattuihin kenttiin. Tämä tehdään molemmille kontrollereille keskenään ristiin; eli ensisijaiselle (Primary) kontrollerille määritetään toissijainen (Secondary) kontrolleri varalle ja toissijaiselle vastaavasti ensisijainen. Kuvassa 6 on ensisijaisen kontrollerin asetuksista.



Kuva 6. Korkean saatavuuden määrittäminen tukiasemille

7.2.3 Tukiasemien palaaminen ensisijaiselle kontrollerille

Viimeisessä vaiheessa konfiguroidaan tukiasemien takaisin paluu ensisijaiselle kontrollerille. Tämä tapahtuu päävalikon ”Controller”-kohdan takaa löytyvästä ”General”-linkistä, josta kytketään AP Fallback päälle.



Kuva 7. Toissijaisen kontrollerin AP Fallback kytkettynä päälle

Toiminnan kannalta on riittävä, kun fallback-ominaisuus kytketään päälle vain toissijaisella kontrollerilla. Suositus on kuitenkin kytkeä se päälle myös ensisijaisella kontrollerilla, sillä sitä voidaan käyttää toissijaisena joillekin toisille tukiasemille. Tämä tietysti riippuu tilanteesta.

7.3 DHCP-palvelin

Kytkennässä käytettävää DHCP-palvelinta ajettiin tietoverkkotekniikan laboratorion LabESX-palvelimella pyörivällä Fedora-Linuxilla. Palvelin määritettiin jakamaan osoitteet kahdesta eri avaruudesta; toinen oli loppukäyttäjille ja toinen tukiasemille. Tukiasemat saavat osoitteita väliltä 172.16.10.150 – 172.16.10.250 ja loppukäyttäjät 172.16.50.50 – 172.16.50.200. Lisänä yllä oleviin osoiteavaruuksiin DHCP:n konfiguraatioon oli määritettävä vielä tyhjä avaruus 192.268.25.0/24-verkolle; eli mitään osoitteita ei oikeasti jaettu tästä avaruudesta. Ilman tätä lisäystä DHCP daemon palautti käynnistysvaiheessa virheilmoituksen.

Tukiasemien osoiteavaruuteen määriteltiin lisäksi DHCP optiot 43 ja 60. Ensin mainittu on vendor-specific information, jolla kerrotaan tukiasemille mistä osoitteesta kontrolleri, tai tässä tapauksessa kontrollerit, löytyvät. Sitä tarvitaan silloin, kun kontrollerit ja tukiasemat sijaitsevat eri aliverkossa. Optio 60 taas on Vendor Class Identi-

fier. VCI on mallikohtainen uniikki merkkijono, jolla laitteet tunnistetaan. Koulun tiloissa kaikki tukiasemat olivat Cisco Aironet 1230 sarjaa, jolloin käytettiin VCI-arvoa ”Cisco AP c1200”.

Kuva 8. Cisco Aironet 1230 AG Series

7.4 Testaus

Itse kytkennän ja sen redundanttisuuden toimivuutta testattiin poistamalla toinen kontrolleri verkosta ja seuraamalla kontrollerien web-hallinnan kautta tukiasemien siirtymistä toimivalle kontrollerille. Tällä simuloitiin toisen kontrollerin tavoittamattomuutta.

Katkoksen pituutta käyttäjän näkökulmasta testattiin yksinkertaisella pingillä. Tätä tarkoitusta varten ladattiin erillinen ping-työkalu nimeltä hrPING[9], sillä se tarjoaa aikaleiman jokaisesta vastauksesta. hrPINGiä ajettiin t-, T- ja s 250- parametreillä, jotka käskevät ohjelman jatkamaan pingausta kunnes käyttäjä keskeyttää, tulostavat aikaleiman ja määrittävät 250 millisekunnin välin paketeille. Tämä toimenpide suoritettiin kuudella eri asetusvariaatiolla ja jokaisella kahdesti. Lisäksi testi toistettiin kummallakin kontrollerilla, jolloin testiajoja tuli yhteensä 24 kappaletta. Jokaisen ajon tulokset tallennettiin logi-tiedostoon, josta katkoksen pituus laskettiin sekunnin tarkkuudella ja neljän ajon keskiarvo kirjattiin muistiin.

Taulukko 5. Katkoksen pituus eri asetusvariaatioilla

Käytetyt asetukset	**Katkoksen pituus (s)**
Vakioasetus (Hearbeat ajastimet poissa, eikä toissijaista kontrolleria määriteltynä)	46
Heartbeat-ajastin 5	33
Heartbeat-ajastin 3	31
Heartbeat-ajastin 3 & Anchor interval 1	31
Heartbeat-ajastin 3 & AP Discovery Time 30	31
Heartbeat-timer 3 & Backup kontrolleri asetettu	22

Kuten taulukosta 5 voidaan huomata, ei ensimmäisen ja viimeisen asetusvariaation välillä tapahtuneiden muutosten tuoma nopeutus ollut merkittävä. Tosin on myös huomattava, että viimeisessä kohdassa käytetään heartbeat-ajastinta asetuksella 3, jonka huomattiin tuovan selkeä etu verrattuna vakioasetukseen. Muutaman sekunnin vaihtelu johtuu todennäköisesti virhemarginaalista, sillä käytettävä mittausmenetelmä oli vain suuntaa antava.

8 TULOKSET JA PÄÄTELMÄT

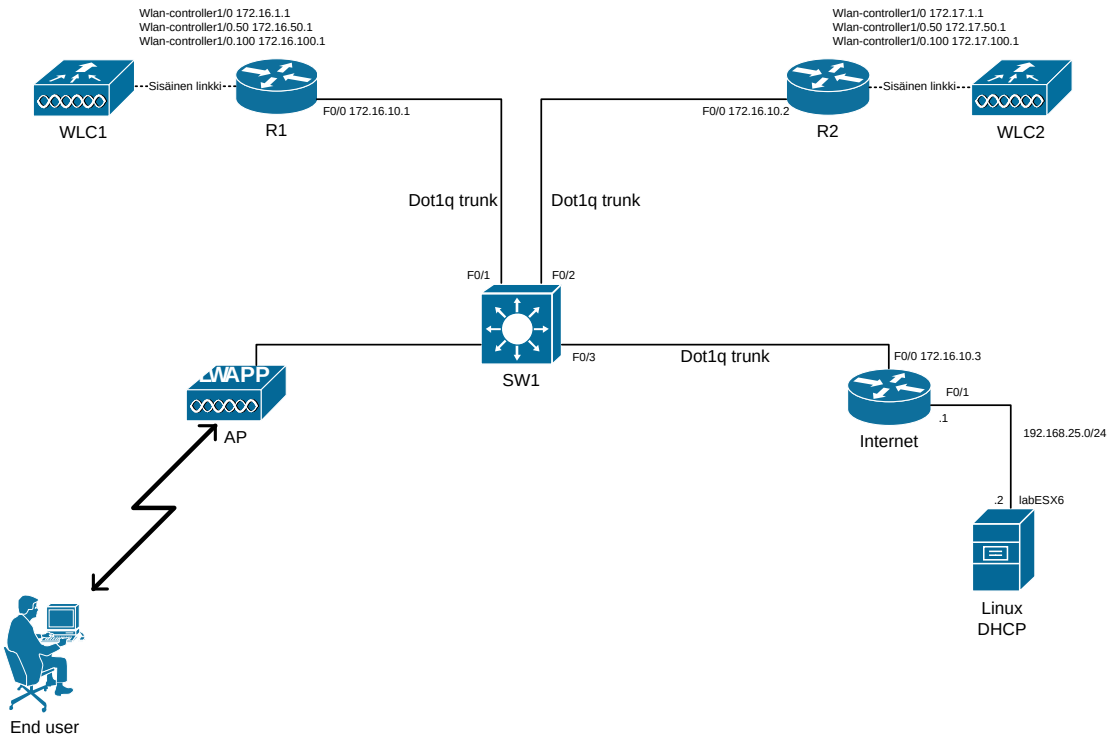
Työ suoritettiin onnistuneesti laitteistorajoituksista huolimatta. Näiden rajoitusten kiertämiseen ja ongelmien selvitykseen kului kuitenkin tarpeettoman paljon aikaa. Työn valmistumisen jälkeen kontrollerit toimivat redundanttisesti ja kestävät toisen kontrollerin vikaantumisen. Pienillä säätötoimenpiteillä saatiin käyttäjille näkyvä katkos minimoitua noin puolen minuutin mittaiseksi. Vaikka katkos käyttäjälle näkyykin, ei kontrollerin vikaantuminen normaalitilanteessa ole kovinkaan yleistä.

Työssä kohdattiin joitakin ongelmatilanteita, alle on koottu niitä ja niihin löytyneitä ratkaisuja.

8.1 Kontrollerien päivitys

Jo työn alkuvaiheessa ilmeni, että kontrolleriohjelmistossa on ohjelmistovirhe (Ciscon tunnus CSCta09996), joka ajoittain estää kontrollerien siirtymisen varakontrollerille.(10) Ciscon sivuja tutkimalla huomattiin uudemman 6.0.199.4- ohjelmistoversion sisältävän korjauksen kyseiselle bugille. Kontrollerien päivitystä varten varmistettiin Ciscon sivuilta, että 6.0-ohjelmiston voi asentaa ongelmitta 5.2-ohjelmiston päälle. Ennen päivitysprosessin aloittamista kopioitiin olemassa olevat konfiguraatiot talteen PC:lle käyttämällä TFTPD32-ohjelmaa. Itse päivitys onnistui kontrollerien web-hallinnan kautta. Päivityspaketti oli kooltaan noin 90MB joten päivittämiseen kului aikaa 10–15 minuuttia molemmilla kontrollereilla. Päivittäminen poisti bugin ja web-hallinnan ulkoasu muuttui selkeämmäksi.

8.2 Koekytkentä



Kuva 9. Koekytkentä

Työn alkupuolella rakennettu koekytkentä ei käyttänyt siltausta vaan kontrollereihin oli asetettu eri osoitealueet. Tässä koekytkennässä tukiasemat siirtyivät ongelmitta kontrollerilta toiselle, mutta samalla niihin kytkeytyneiden asiakaskoneiden IP-osoite

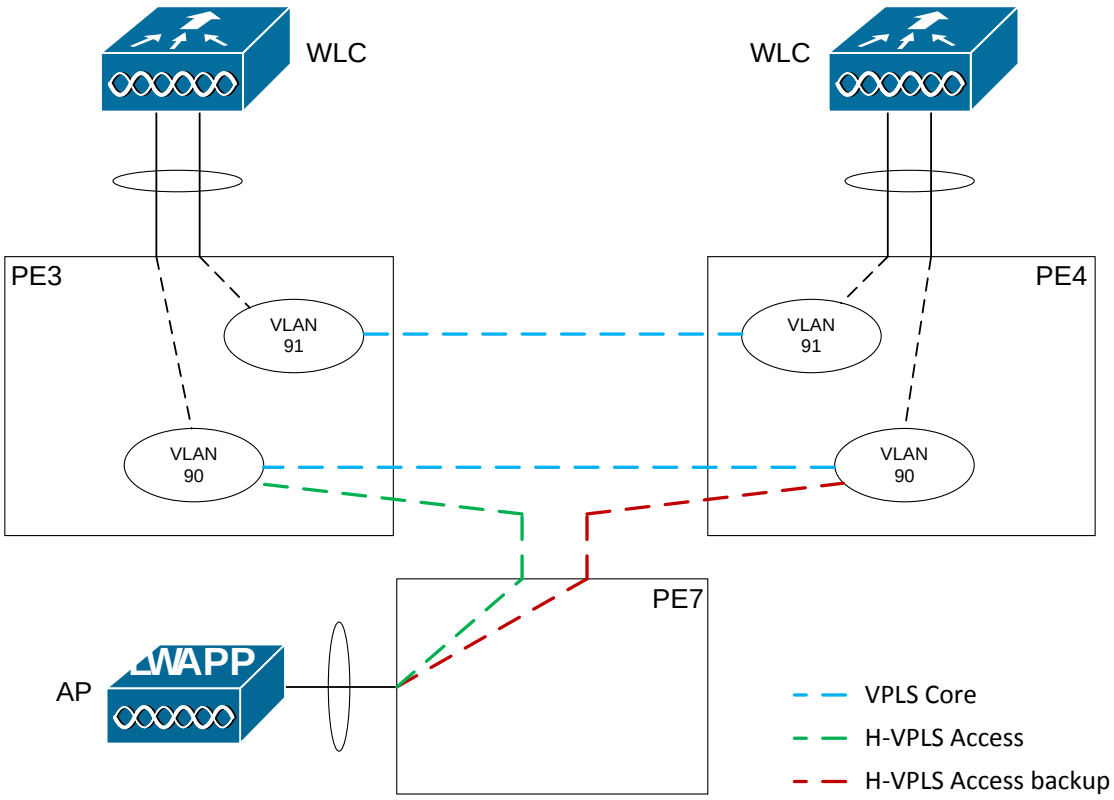
vaihtui, johtuen kontrollereissa käytetyistä eri osoiteavaruuksista. Tästä seurasi puolestaan se, että asiakaskoneiden täytyi uusia IP-osoite verkon käytön jatkamiseksi. Tämä ei kuitenkaan verkon redundanttisuutta ajatellen ollut optimaalisin vaihtoehto. Koekytkentä oli kuitenkin tärkeä osa työtä, sillä se paljasti sen, että reitittimet, joissa kontrollerimoduulit sijaitsivat, oli muutettava siltaavaan toimintatilaan.

8.3 Yhteyshäiriöt

Lopullisen siltausta käyttävän kytkennän valmistumisen jälkeen huomattiin, että kontrollerien web-hallintaan ei päässyt kirjautumaan Linux DHCP-palvelimen Internet-selainta käyttämällä. Wireshark-verkkoanalysaattorilla sekä Ciscon IOS:in tarjoamilla debug-komennoilla tutkittiin verkon liikennettä ja huomattiin, että kontrollerien yhdyskäytäväksi tuli asettaa Internet-reitittimen FastEthernet 0/0-portin IP-osoite kontrollerin oman IP-osoitteen sijaan. Huomattiin myös, että tukiasemat eivät kyenneet liittymään kumpaankaan kontrolleriin. Tämä korjaantui asettamalla kytkimelta tarvittavat portit (FastEthernet 0/13-20) oikeaan virtuaalilähiverkkoon (VLAN 10).

9 JATKOKEHITYS

Työssä tutkittua ja rakennettua verkkoa voi ja on tarkoitus jatkokehittää SimuNet-testaus-, tutkimus- ja tuotekehityslaboratorion tarpeisiin. Työtä aloitettaessa oli vielä tarkoitus sisällyttää SimuNetiin siirtäminen työn piiriin, mutta tämä kariutui lopulta ajanpuutteeseen. Teoriassa kytkentä voidaan kuitenkin siirtää pienin muutoksin SimuNet-laitteisiin, joten pohjatyö on jo tehty. SimuNetiin siirtäminen onkin ehdottomasti tärkein jatkokehityskohde, sillä SimuNetillä voidaan simuloida Internetiä ja kontrollereiden toimintaa eri maantieteellisissä sijainneissa huomattavasti paremmin kuin mihin työssä käytetty yhden reitittimen "Internet" kykenee. Tällöin kontrolleriverkon topologia on kuvan 10 mukainen.



Kuva 10. SimuNet-verkon topologia kontrollerien osalta (11)

Tulevaisuutta ajatellen olisi myös tärkeää tutkia, miten IPv6-osoitteet saadaan toimimaan kontrollerien kanssa. Nykyisellään kontrollerit eivät nimittäin salli edes IPv6-osoitteiden läpivientiä. On epäselvää miten IPv6-tuki voidaan toteuttaa, mutta todennäköisin ja helpoin ratkaisu on ohjelmistopäivitys kontrollereihin. Ei ole kuitenkaan varmaa, että Ciscolla olisi suunnitelmissa tuoda tällaista päivitystä ammattikorkeakoulun tiloissa sijaitseviin kontrollereihin. Tästä syystä myös vaihtoehtoisten toteutustapojen tutkinta olisi tärkeää.

Siltauksen korvaaminen paremmalla tekniikalla on myös potentiaalinen jatkokehityksen kohde. Siltauksella kytkentä toimii hyvin ja varmasti, mutta siinä menetetään kaikki reititystoiminnot kontrollerilaitteista. Eräs kokeilemisen arvoinen vaihtoehtoinen tekniikka olisi käyttää sopivaa kerroksen kaksi VPN-ratkaisua (L2VPN). Ratkaisussa sillattavat yhteydet voisi yrittää tuoda esim. Ethernet-over-MPLS yhteydellä suoraan kontrollerin käyttämään Ethernet-porttiin ja näin säästää alkuperäinen reititystoinnallisuus.(11.)

LÄHTEET

1. Kettunen, Martti. 29.10.2009. Simunet. Saatavissa: http://www.ictlab.kyamk.fi/index.php?option=com_content&view=article&id=47&Itemid=54 [viitattu 5.4.2011].

2. Halonen, Juho-Miika. 2010. Keskitetysti hallittavan langattoman verkon suunnittelu. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/12890/Juho-Miika_Halonen.pdf?sequence=1 [viitattu 29.3.2011].

3. WLAN Controller Failover for Lightweight Access Points Configuration Example. 2009. Saatavissa: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008064a294.shtml [viitattu 15.3.2011].

4. Wireless LAN Controller (WLC) FAQ. 2009. Saatavissa: http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml [viitattu: 15.3.2011].

5. Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC). 2008. Saatavissa: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00806c9e51.shtml [viitattu: 15.3.2011].

6. The Benefits of Wireless LAN Controller in Small and Mid-sized Business Networks. 2007. Saatavissa: http://netgear.de/images/Wireless_LAN_White_Paper22-17318.pdf [viitattu 15.3.2011].

7. Cisco IOS Bridging Command Reference. 2009. Saatavissa: http://www.cisco.com/en/US/docs/ios/bridging/command/reference/br_a1.html [viitattu 22.3.2011].

8. How bridge group is differentiated from vlan - Cisco Support Community. 2010. Saatavissa: https://supportforums.cisco.com/docs/DOC-11262 [viitattu 22.3.2011].

9. PING UTILITY hrPING v3.10 – cFos. Saatavissa: http://www.cfos.de/ping/ping_e.htm [viitattu 22.3.2011].

10. Cisco 4.2.209.0 Controller Code Release. Saatavissa: http://www.my80211.com/cisco-field-alerts/2010/6/3/cisco-422090-controller-code-release.html [viitattu 29.3.2011].

11. Oinonen, Riku. 2011. Virtuaaliset lähiverkkopalvelut operaattoriverkon sisäisessä käytössä. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Reitittimen R1 konfiguraatio

```
hostname R1
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5 $1$vM5/$R6DjKTA0Ab09FQcQQEwMD.
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
no ip routing
no ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
archive
log config
hidekeys
bridge irb
interface FastEthernet0/0
no ip address
no ip route-cache
duplex auto
speed auto
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
interface FastEthernet0/0.10
encapsulation dot1Q 10
no ip route-cache
bridge-group 10
interface FastEthernet0/0.50
encapsulation dot1Q 50
no ip route-cache
bridge-group 50
interface FastEthernet0/1
no ip address
no ip route-cache
shutdown
duplex auto
speed auto
interface Serial0/0/0
no ip address
no ip route-cache
shutdown
```

no fair-queue
clock rate 2000000
interface Serial0/0/1
no ip address
no ip route-cache
shutdown
clock rate 2000000
interface ATM0/3/0
no ip address
no ip route-cache
shutdown
no atm ilmi-keepalive
interface wlan-controller1/0
no ip address
no ip route-cache
interface wlan-controller1/0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
interface wlan-controller1/0.10
encapsulation dot1Q 10
no ip route-cache
bridge-group 10
interface wlan-controller1/0.50
encapsulation dot1Q 50
no ip route-cache
bridge-group 50
interface BVI1
ip address 172.16.1.1 255.255.255.0
interface BVI10
ip address 172.16.10.1 255.255.255.0
no ip route-cache
interface BVI50
ip address 172.16.50.1 255.255.255.0
no ip route-cache
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
bridge 1 protocol ieee
bridge 1 route ip
bridge 10 protocol ieee
bridge 10 route ip
bridge 50 protocol ieee
bridge 50 route ip
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
line con 0
logging synchronous

line aux 0
line 66
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
password cisco
login
scheduler allocate 20000 1000
end

Reitittimen R2 konfiguraatio

```
hostname R2
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5 $1$vM5/$R6DjKTA0Ab09FQcQQEwMD.
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
no ip routing
no ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
archive
 log config
  hidekeys
bridge irb
interface FastEthernet0/0
no ip address
 no ip route-cache
 duplex auto
 speed auto
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 no ip route-cache
 bridge-group 50
interface FastEthernet0/1
 no ip address
 no ip route-cache
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 no ip route-cache
 shutdown
 no fair-queue
 clock rate 2000000
```

```
interface Serial0/0/1
 no ip address
 no ip route-cache
 shutdown
 clock rate 2000000
interface ATM0/3/0
 no ip address
 no ip route-cache
 shutdown
 no atm ilmi-keepalive
interface wlan-controller1/0
 no ip address
 no ip route-cache
interface wlan-controller1/0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
interface wlan-controller1/0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
interface wlan-controller1/0.50
 encapsulation dot1Q 50
 no ip route-cache
 bridge-group 50
interface BVI1
 ip address 172.16.1.2 255.255.255.0
interface BVI10
 ip address 172.16.10.2 255.255.255.0
 no ip route-cache
interface BVI50
 ip address 172.16.50.2 255.255.255.0
 no ip route-cache
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
bridge 1 protocol ieee
bridge 1 route ip
bridge 10 protocol ieee
bridge 10 route ip
bridge 50 protocol ieee
bridge 50 route ip
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
line con 0
 logging synchronous
line aux 0
line 66
```

```
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login
scheduler allocate 20000 1000
end
```

Internet-reitittimen konfiguraatio

```
hostname Internet
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
dot11 syslog
ip source-route
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
vtp domain CISCO
vtp mode transparent
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 ip helper-address 192.168.25.2
 duplex auto
 speed auto
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.3 255.255.255.0
 ip helper-address 192.168.25.2
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.3 255.255.255.0
 ip helper-address 192.168.25.2
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.50.3 255.255.255.0
 ip helper-address 192.168.25.2
interface FastEthernet0/1
 ip dhcp relay information trusted
 ip address 192.168.25.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
```

```
router ospf 1
 log-adjacency-changes
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.50.0 0.0.0.255 area 0
 network 192.168.25.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

DHCP-palvelimen (Linux) konfiguraatio

```
# Globaalit asetukset
ddns-update-style interim;
allow bootp;
option space LWAPP;
option LWAPP.controller code 241 = array of ip-address;

subnet 192.168.25.0 netmask 255.255.255.0 {
 }

# Access Pointit
subnet 172.16.10.0 netmask 255.255.255.0 {
  authoritative;
  range dynamic-bootp 172.16.10.50 172.16.10.200;
  option routers 172.16.10.3;
  option broadcast-address 172.16.10.255;
  option log-servers 192.168.25.2;
  default-lease-time 600;
  max-lease-time 7200;


  class "LWAPP" {
    match option vendor-class-identifier;
  }

  subclass "LWAPP" "Cisco AP c1200" {
    vendor-option-space LWAPP;
    option LWAPP.controller 172.16.10.11, 172.16.10.13;
  }
}

# loppukäyttäjät
Subnet 172.16.50.0 netmask 255.255.255.0 {
  authoritative;
  range dynamic-bootp 172.16.50.150 172.16.50.250;
  option routers 172.16.50.3;
  option broadcast-address 172.16.50.255;
  option log-servers 192.168.25.2;
  default-lease-time 600;
  max-lease-time 7200;
}
```