Ville Gråsten

KESKITETTY VERKONHALLINTA
Cisco WLAN-kontrollerilla ja WCS:llä

Opinnäytetyö
Tietotekniikan koulutusohjelma

Toukokuu 2011

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** 13.5.2011
Tekijä(t) Gråsten Ville	**Koulutusohjelma ja suuntautuminen** Tietotekniikan koulutusohjelma

Nimeke

Keskitetty verkonhallinta: Cisco WLAN-kontrollerilla ja WCS:llä

Tiivistelmä

Opinnäytetyöni tarkoituksena oli tutkia keskitettyä verkonhallintaa langattomissa lähiverkoissa, rakentamalla testiverkko Mikkelin ammattikorkeakoulun laboratorioon. Verkon hallinnointiin käytettiin tässä työssä Cisco Systemsin WLAN-kontrolleria ohjaamaan tukiasemia ja WCS-ohjelmistoa ohjaamaan kontrolleria ja tätä kautta koko verkkoa keskitetysti.

Teoriaosuudessa perehdytään osa-alueisiin, jotka liittyvät keskeisesti verkonhallintaan. Osuudessa tarkastellaan myös erilaisia tapoja hallinnoida verkkoa sekä millaisia työkaluja tähän on käytettävissä. Osuudessa käsitellään myös, verkonhallintaan varten kehiteltyjä protokollia, kuten SNMP ja sen eri versiot, jota myös käytettiin testiverkon hallinnointiin. Osuudessa käydään näiden lisäksi läpi tapahtumien seurantaa kehitettyjä protokollia sekä LWAPP-protokollaa, joka mahdollistaa tukiasemien hallinnoinnin kontrollerilla.

Käytännön osuudessa perehdytään toimenpiteisiin, joita on tehtävä, ennen kuin tukiasemia voidaan hallita WLAN-kontrollerilla ja WCS-ohjemalla. Tämän lisäksi tarkastellaan miten näiden käyttöönotto tapahtuu ja millaisia ominaisuuksia niistä löytyy hallintaa varten.

Testiverkolla saavutettiin keskitetty tukiasemien hallinta ja havainnollistettiin, kuinka WLAN-kontrolleria ja WCS-ohjelmaa käytetään asetusten muokkaamiseen ja mahdollisten vikojen ilmaisemiseen verkossa.

Asiasanat (avainsanat)

Verkonhallinta, Langattomat lähiverkot, WLAN-kontrolleri, WCS, SNMP

Sivumäärä	**Kieli**	**URN**
44	Suomi	

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Koivisto, Matti	Mikkelin ammattikorkeakoulu

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the bachelor's thesis** 13. May 2011
Author(s) Gråsten Ville	**Degree programme and option** Information Technology

Name of the bachelor's thesis

Centralized Network Management with Cisco WLAN controller and WCS software

Abstract

The purpose of this bachelor's thesis was to research network management in wireless networks by building a test network for the laboratory of Mikkeli University of Applied Sciences. The management of the network was carried out with Cisco System's WLAN controller to control the access points and WCS software to control the WLAN controller and this way the whole network.

The theory part of this bachelor's thesis introduced the areas essential to network management. The part also told different ways to manage networks and what kinds of tools where available for it. This part also covered the protocols designed to network management such as SNMP and its various versions which were used to manage the test network. In addition to these, the part also included protocols developed for monitoring events and the LWAPP protocol enabling the access points management with the WLAN controller.

The practical part introduced the necessary operations to be done before the management of the access points would be possible with the controller and the WCS software. This part also dealt with the installation process and told about the features that are available for network management.

Centralized network management of the access points was achieved with the test network and it also demonstrated how the WLAN controller and the WCS software could be used to change settings and track possible faults in the network.

Subject headings, (keywords)

Network management, Wireless networks, WLAN controller, WCS, SNMP

Pages	**Language**	**URN**
44	Finnish	

Remarks, notes on appendices

Tutor	**Bachelor's thesis assigned by**
Koivisto, Matti	Mikkeli University of Applied Sciences

SISÄLTÖ

1 JOHDANTO 1

2 VERKONHALLINTA 2

3 VERKONHALLINTATAVAT 4

3.1 Merkkipohjainen hallinta 4

3.2 Graafiset hallintatyökalut 6

3.2.1 Cisco SDM 6

3.2.1 Selain hallinta 8

3.3 Etähallinta SHH:lla 9

4 VERKONHALLINTAPROTOKOLLAT 10

4.1 SNMP 11

4.1.1 SNMPv1 13

4.1.2 SNMPv2 14

4.1.3 SNMPv3 15

4.2 Tapahtumien seuranta 16

4.2.1 SDEE 17

4.2.2 Syslog 18

4.3 LWAPP 18

5 TESTIVERKKO JA SEN HALLINTA 20

5.1 Kontrollerin käyttöönotto 22

5.2 Tukiaseman IOS-päivitys 23

5.3 Kontrollerilla hallinta 28

5.4 SNMP ja sen käyttöönotto kontrollerissa 31

5.5 WCS 32

5.6 WCS:llä hallinta 35

5.7 Tukiaseman IOS:n palautus 39

6 PÄÄTÄNTÖ 40

LÄHTEET 42

LYHENTEET

ISO	International Organization For Standardization
WLAN	Wireless Local Area Network
WCS	Cisco Wireless Control System
SSH	Secure Shell
I/O	Input/Output
SDM	Secure Device Manager
CLI	Command-line interface
VPN	Virtual Private Network
IP	Internet Protocol address
SSL	Secure Sockets Layer
UPD	User Datagram Protocol
TCP	Transmission Control Protocol
SSC	Self Signed Certificate
MIC	Manufacturing Installed Certificate
LAP	Lightweight Access Point
AP	Access Point
IOS	Internetwork Operating System
RADIUS	Remote Authentication Dial In User Service
TACAS+	Terminal Access Controller Access-Control System Plus
TELNET	Terminal emulation program for TCP/IP networks
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
WAN	Wide Area Network
LAN	Local Area Network
ACL	Access Control List

1 JOHDANTO

Lähiverkkojen monipuolisuus ja koko kasvavat koko ajan yritys, oppilaitos, kuin myös yksityisellä puolella. Nykyisin verkoissa on entistä enemmän, langallisia kuin langattomiakin laitteita. Laitteiden määrän ja laitteissa olevien ominaisuuksien kasvaessa niiden ylläpito hankaloituu ja ongelmatilanteita saattaa syntyä, joten on syytä keskittyä myös laitteiden hallintaan.

Langaton lähiverkko voi koostua pienimmillään vain yhdestä tukiasemasta, jolloin erillistä hallintaa ei niinkään tarvita, mutta kun siirrytään esimerkiksi oppilaitoksiin tai yritysmaailmaan laitteita voi olla useampia ja yksittäisen laitteen ylläpito voisi osoittautua hankalaksi ja aikaa vieväksi, joten laitteiden keskitetty hallinta voi olla tarpeen. Keskitetyllä hallinnalla pystytään reagoimaan ongelmatilanteisiin nopeammin, seuraamaan liikennettä ja kartoittamaan verkkoa tulevaisuutta varten. Hallinnalla voidaan myös suorittaa etäpisteestä, jolla voidaan pienentää ylläpitokustannuksia.

Työni tavoitteena on rakentaa testiverkko kevään 2011 aikana Mikkelin ammattikorkeakoulun laboratorioon käyttäen useampaa Cisco Systemsin langatonta tukiasemaa sekä tukiasemaohjainta, jolla voidaan hallita kaikkia tukiasemia yhtä aikaa keskitetysti. Tarkastelen lisäksi sitä kuinka tukiasemaohjainta voidaan ohjata palvelimelle asennettavalla WCS-ohjelmistolla. Tarkoituksena on siis tutkia, kuinka verkkoa voidaan hallita yhdestä pisteestä keskitetysti ja millaisia työkaluja on käytettävissä, niin ohjelmallisia kuin laitepohjaisia ja kuinka niitä käytetään.

Työssä perehdytään verkonhallinnan teoriaan, kuten millaisia protokollia on kehitetty tätä varten ja miten niitä voi hyödyntää missäkin tilanteessa. Lisäksi käyn läpi laitteet ja ohjelmistot, joita työssä käytetään ja miten niiden konfigurointi ja asennus tapahtuu. Työssä perehdytään myös Ciscon Wlan-kontrollerin hallintaliittymän käyttöön ja sen sisältämiin ominaisuuksiin sekä tutustutaan palvelimelle asennettavaan WSC-hallintaohjelmaan. Tarkoituksena olisi siis selvittää, kuinka lähiverkon hallintatyökalut asennetaan, millaisia ominaisuuksia ne sisältävät ja kuinka niitä käytetään.

2 VERKONHALLINTA

Keskitetty hallinta helpottaa huomattavasti verkon ylläpitoa ja laajentamista. Usean yksittäisen laitteen sijasta voidaan hallitta verkkoa yhtenä kokonaisuutena. Hallintaan on kehitetty ISO-standardointi organisaation toimesta IEEE 802.1-standardi, joka määrittelee verkonhallintaan viisi osa-aluetta, jotka käsittelen tässä luvussa. Olen myös koostanut nämä kuvaan 1.
[1, s. 305-306; 2, s. 3; 3, s. 11.]

KUVA 1. Verkonhallinnan eri osa-alueet

Vikojen hallinnalla tarkoitetaan lähiverkossa olevien laitteiden vikojen kartoittamista, mahdollista eristämistä, vian korjaamista sekä niiden ehkäisemistä. Vikojen hallintaa varten tulisi luoda jonkinlainen järjestelmä, joka ilmoittaa tapahtumista verkon ylläpitäjälle ja kirjaa ne ylös, jolloin mahdollisiin korjaustoimenpiteisiin voidaan ryhtyä nopeasti. Erilaisilla verkonhallintatyökaluilla voidaan tutkia verkon antamia hälytyksiä ja raportteja vioista. Vikojen hallinnalla pyritään siis kasvattamaan verkon luotettavuutta ja ongelmatilanteiden mahdollisimman nopeaa ratkaisemista, jotta ylimääräi-

siä katkoja ei ilmaantuisi. Jotkin verkkolaitteet sisältävät diagnostiikkatestejä, joilla voidaan ennaltaehkäistä mahdollisia vikoja. [1, s. 303; 3, s. 11-12.]

Käytön hallinnalla pyritään seuraamaan verkon resurssien ja palveluiden käyttöä eri lähteistä, jotta niitä voidaan esimerkiksi käyttää laskutuksen perustana ja mahdollisesti siirtää enemmän resursseja sitä tarvitseville. Verkon käytön seuraamiseksi pitää hallinnoijan määrittää mitä tietoja verkosta kerätään ja milloin. Käytön hallinnalla kerättyjä tietoja voidaan myös hyödyntää tulevaisuudessa, esimerkiksi verkon laajentuessa osataan laittaa lisäyhteyksiä enemmän kaistaa vaativille alueille. [2, s. 4-5; 3, s. 12.]

Kokoonpanon hallinnalla kerätään tietoja ja dokumentoidaan verkossa olevista laitteista, kuten: kytkimistä, reitittimistä ja tukiasemista, sekä niiden sisältämistä lisäkorteista, sovittimista ja muista lisälaitteista. Tietoja ei ainoastaan kerätä pelkistä fyysisistä laitteista, vaan myös laitteiden sisältämistä ominaisuuksista, ohjelmistoversioista ja asetuksista, kuten reitittimen reititystiedoista, sekä muista tarvittavista tiedoista, jotta niitä ei tarvitsisi erikseen käydä tarkistamasta jokaiselta laitteelta ja että ne pysyisivät ajan tasalla. Kokoonpanon hallinta sisältää tarvittavat tiedot laitteiden asetusten luontiin ja myös niiden poistamiseen, sekä muokkaamiseen vikatilanteissa ja hallittujen muutosten luomisessa. [1, s. 304; 3, s. 12-13.]

Suorituskyvyn hallinnan päätarkoituksena on kerätä tietoja ja analysoida verkon suorituskykyä. Lähiverkossa voi olla useita laitteita, jotka käyttävät samanaikaisesti esimerkiksi samaa kaistaa tai levytilaa, jolloin näiden kuormitusta on hyvä seurata. Saatavilla olevan kaistan tarve voi olla joissakin tapauksissa jatkuvaa ja tarvitaan hyvinkin suuria kaistoja mm. reaaliaikaiset sovellukset, kun taas toisaalla kaistaa käytetään vain Internetin selaamiseen, jossa tarvittava kapasiteetti on paljon pienempi, joten oikeanlainen kapasiteetin jako voi olla hyvinkin kriittistä ja tärkeää. [1, s. 304; 3, s. 13.]

Suorituskyvyn hallinta koostuu kahdesta pääseikasta hallinta ja valvonta. Valvonnalla tarkoitettaan verkon liikenteen seuraamista, kun taas hallinnalla keskitytään mahdollisiin toimenpiteisiin valvonnassa kerätyillä tiedoilla. [3, s. 13.]

Turvallisuuden hallinnalla tarkoitetaan työkaluja, joilla voidaan määrittää ja seurata verkon ylläpitäjien oikeuksia järjestelmässä, jotta hallintatiedot olisivat turvattu ulko-

puolisilta. Turvallisuuden hallinnassa tärkeintä on siis kerätä ja tallentaa tietoja esimerkiksi siitä kuka on kirjautunut hallinta-asemalle ja milloin, jotta tietoa voidaan myöhemmin analysoida. Turvallisuuden hallinta ei niinkään sisällä järjestelmän sisäisten käyttäjien oikeuksien määrittelyä, vaan keskittyy siihen kenellä ja mistä on oikeus päästä käsiksi järjestelmän laitteisiin ja hallinta-asemiin, sekä niiden sisältämiin hallintatietoihin. [1, s. 304-305; 2, s. 6.]

3 VERKONHALLINTATAVAT

Lähiverkkoja voidaan hallita monella eri tavalla, laitteiden määrästä ja niiden ominaisuuksista riippuen. Ominaisuuksien näkökulmasta oleellinen seikka on se tukeeko laite graafista vai komentorivipohjaista käyttöliittymää. Hallinta voi tapahtua yksinkertaisimmillaan käyttäen komentorivejä, eli merkkipohjaisena. Tässä tapauksessa toiminta etenee seuraavasti. Kun on tarvetta hallinnoida vain yhtä laitetta, hallittavan laitteen kuten: kytkimen, reitittimen tai tukiaseman ja hallintatyöaseman välille luodaan yhteys, käyttäen joko paikallista hallinta- eli console-yhteyttä tai etäyhteyttä Telnet tai SSH-protokollalla.

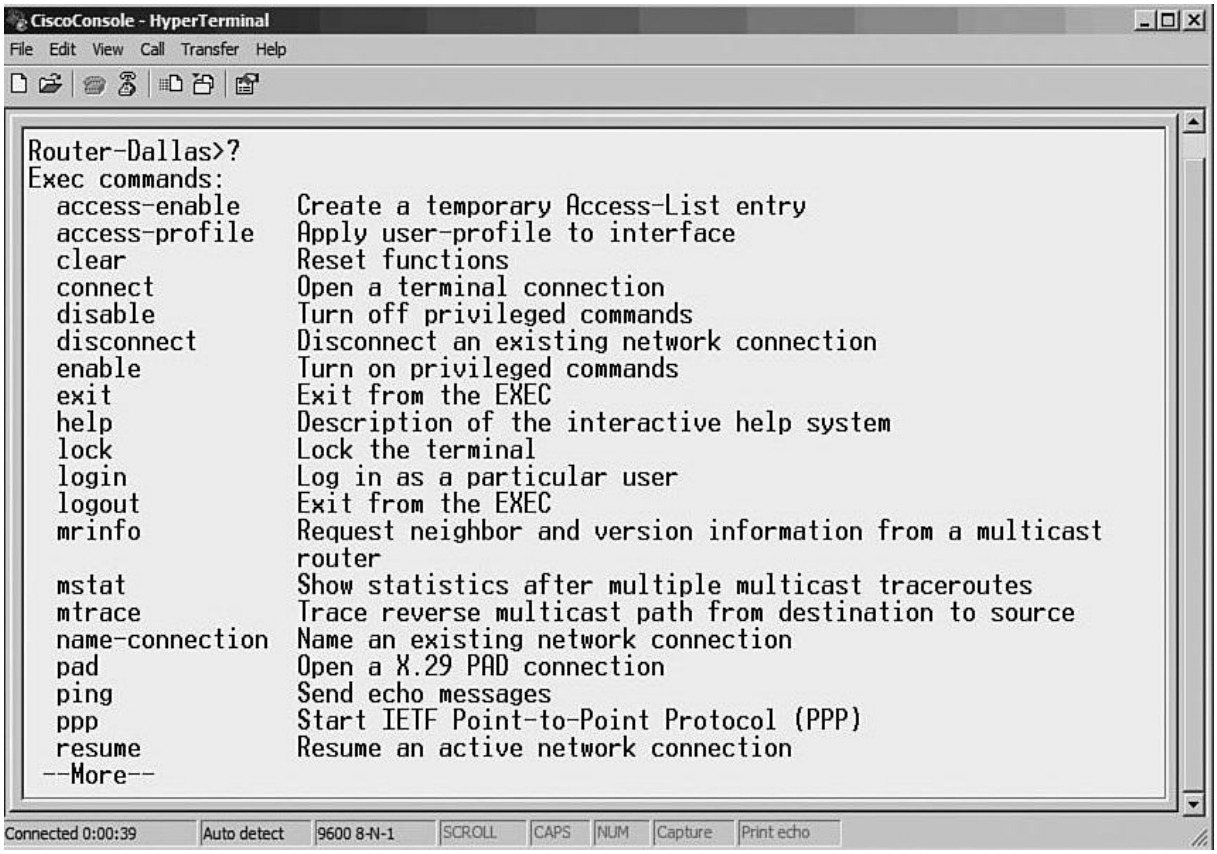
Merkkipohjainen hallinta voi osoittautua joissain tapauksissa hankalaksi ja aikaa vieväksi, jolloin voidaan myös käyttää graafisia hallintaliittymiä, kuten Ciscon SDM tai selainpohjaista-hallintaa, jotka ovat helpompia ja nopeampia käyttää. Monet yksityiskäyttöön suunnatut verkkolaitteet käyttävät juuri selainpohjaista hallintaliittymää sen helppokäyttöisyyden takia.

3.1 Merkkipohjainen hallinta

Merkkipohjaisella hallinnalla voidaan suorittaa kaikki tarvittavat konfiguroinnit laitteeseen ja sitä voidaan myös käyttää vian etsintää ja ehkäisemään ongelmia käyttämällä esimerkiksi debug-komentoa hallittaessa reititintä. Merkkipohjainen hallinta on hyvin tehokas tapa hallita laitetta, mutta vaatii osaamista.

Merkkipohjaisessa hallinnassa laitetta ohjataan komentorivipohjaisesti. Hallittavaan laitteeseen voidaan olla suorassa yhteydessä tietokoneelta käyttäen tietyn tyyppistä console-kaapelia, joka käyttää I/O-sarjaliikennettä esim. COM tai LPT1-tulostin port-

tia, kaapelityyppi saattaa vaihdella laitteesta riippuen. Console-yhteyttä varten tarvitaan myös terminaali-emulointi-ohjelma tietokoneelle esimerkiksi HyperTerminal (kuva 2), johon komennot voidaan syöttää.



KUVA2. Merkkipohjainen HyperTerminal on yhdistettynä Cisco Systemsin reitittimeen

Lähiverkon laitteita voidaan hallinnoida merkkipohjaisesti myös etäyhteydellä verkon ylitse, käyttäen Telnet:ä tai SSH:ta. Telnet-yhteys luodaan käyttäen TCP/IP-protokollaa ja IP-osoitteilla. Yhteyttä varten täytyy hallittavaan laitteeseen luoda käyttäjätunnus ja salasana tunnistusta varten. Tunnuksia voidaan luoda useampia ja antaa näin käyttöoikeudet laitteeseen, kun taas console-yhteydellä käyttäjiä voi olla ainoastaan yksi. Telnet-yhteys voidaan luoda monella eri ohjelmalla ja tavalla esimerkiksi Windowsin komentokehotteella tai käyttämällä HyperTerminal ohjelmaa. Hallinnoitavan laitteen ja päätelaitteen välistä liikennettä ei Telnet-yhteydessä ole suojattu, joten Internetin yli tapahtuvaa hallinnointiin se ei sovellu, mutta suljetuissa verkoissa sitä voidaan käyttää. [4.]

SSH (Secure Shell) on samankaltainen etähallintatyökalu kuin Telnet, mutta SSH:ssa yhteys on täysin suojattu. Yhteys voidaan muodostaa samaan tapaan kuin Telnetissä IP-osoitteilla ja luodaan käyttäjille tilit, joissa on salasana ja käyttäjätunnus. SSH:ssa myös käyttäjätunnus ja salasana ovat suojattuja. Yhteyden muodostamiseen voidaan käyttää esimerkiksi HyperTerminalia kuten Telnetissäkin. Hallinnoitavan laitteen ja päätelaitteen välinen yhteys on myös kryptattu ja suojattu, toisin kuin Telnetissä. [5.]

3.2 Graafiset hallintatyökalut

Graafiseen hallintaan on olemassa eri vaihtoehtoja, niiden tarkoituksena on tehdä hallinnasta käyttäjäystävällisempää poistamalla merkkipohjaisen konfikuroinnin tarve kokonaan. Hallinta voidaan toteuttaa tietokoneelle asennettavalla erillisellä ohjelmistolla tai suoraan käyttämällä Internet-selainta. Erillisiä graafisia ohjelmistoja on monelta eri valmista moneen eri käyttöön. Cisco System on kehittänyt reitittimien hallintaa tarkoitetut Cisco SDM (Security Device Manager) ohjelman. Hallintaan ei välttämättä tarvita ohjelmistoa, jos laite tukee selainpohjaista käyttöä, jolloin hallintaan riittää vain Internet-selain.

3.2.1 Cisco SDM

SDM on Cisco Systemsin kehittämä graafinen hallintatyökalu Ciscon reitittimille, niiden asetusten määrittelyyn ja laitteen toimintojen seurantaan. SDM on Java-pohjainen selaimella suoritettava hallintatyökalu. SDM sisältää ohjattuja toimintoja, joiden avulla käyttäjä voi luoda haluamiaan asetuksia reitittimeen, kuten reitittimen suojauksen. SDM:ään löytyy paljon ohjemateriaalia Internetistä. [6.]

SDM:n ohjailuilla työkaluilulla voidaan tehdä asetuksia askel kerrallaan, eli ohjelma antaa ohjeita käyttäjälle mitä seuraavaksi pitää tehdä, kuvassa 3 on menossa ohjattu toiminto reitittimen sarjaportin määrittelemiseksi. Ohjelmalla voidaan konfiguroida reitittimen tietoturva-asetuksia, sekä LAN- ja WAN-porttien asetuksia. SDM:llä voidaan myös ohjata palomuuria ja sillä voidaan luoda VPN-yhteyksiä. Konfiguroinnin aikana tapahtuneista mahdollisista virheistä ohjelma osaa ilmoittaa käyttäjälle ja myös ehdottaa korjaustoimenpiteitä. Ciscolla on SDM:ää varten laaja verkkotukipalvelu, josta löytyy avusteita laitteen käyttämiin termeihin ja ominaisuuksiin, sekä millaisia

tietoja mihinkin kohtaan pitää laittaa. SDM sisältää valmiita asetusarvoja palomuuriin ja VPN-yhteyteen, jotka ovat International Computer Security Association ja Cisco Technical Assistance Centerin suosittelemia. Suojausasetusten vahvuuksia ja heikkouksia voidaan testata niille suunnatuilla työkaluilla. [6.]

KUVA 3. WAN-asetuksien ohjattu konfigurointi

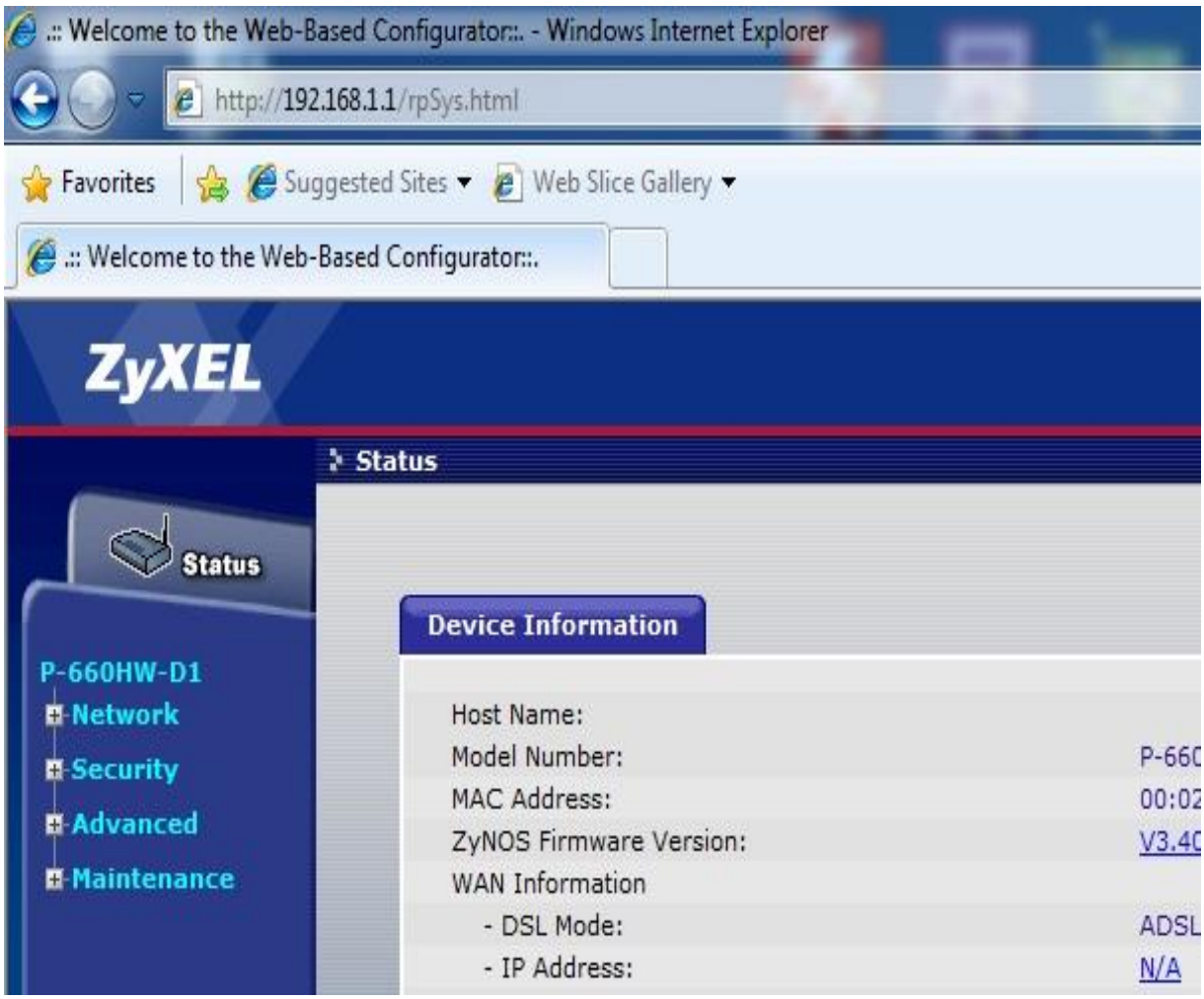
SDM:llä voidaan etäkäyttää ja siihen voidaan luoda pääsylistoja ACL-editorilla, jolloin useammalla käyttäjällä voi olla pääsyoikeudet laitteeseen ja näin ollen voivat seurata ja kofiguroida sitä. SDM:ä vois siis käyttää useampi henkilö, mutta sillä voidaan ohjata vain yhtä laitetta. Etäyhteys suojataan tässä tapauksessa SSL ja SSH-protokollalla, jolloin etäkäyttäjä voi olla yhteydessä laitteeseen turvallisesti Internetin ylitse käyttämällä nettiselainta. [6.]

SDM:n käyttöä varten reitittimen pitää tukea tätä ominaisuutta ja se voidaan myös ladata jälkeenpäin reitittimeen. Reitittimellä pitää käynnistää http- tai https-palvelin ja luoda käyttäjä tilit, sekä sallia Telnet ja SSH-yhteys. Käyttäjä tarvitsee hallinta tietokoneelle Java-pohjaisen SDM-asiakas-ohjelman ja selaimen, joka tukee ja sallii Java-komponentit.

Cisco on lopettanut SDM:n myynnin ja sen ylläpidosta luovutaan vuonna 2012. SDM:n korvaajana toimiin samankaltainen ohjelma CCP (Cisco Configuration Professional).[20.]

3.2.2 Selain hallinta

Useimmat koti- ja pienyrityskäyttöön suunnatut reitittimet, modeemit, kytkimet ja langattomat tukiasemat käyttävät selainpohjaista hallintaa. Selainpohjaisessa hallinnassa lähiyhteys muodostetaan hyvin samaan tapaan, kuin aiemmin mainittu console-yhteys, mutta tässä tapauksessa yhteys muodostetaan lähiverkkoliitännän kautta RJ-45 -kaapelilla ja TCP/IP-protokollalla. Selainpohjainen perushallinta voidaan toteuttaa myös verkon yli sallimalla etäyhteys laitteeseen. Työkalu on samankaltainen kuin SDM, mutta erillistä ohjelmistoa ei tarvitse asentaa tietokoneelle. Yhteyden muodostamiseen tietokoneen ja laitteen välille tarvitaan vain Internet-selain, johon syötetään laitteelle asetutettu hallinta IP-osoite, kuten kuvassa 4 on laitettu.



KUVA 4. Selaimella hallittava Zyxelin tukiasema/adsl-modeemi

3.3 Etäyhteys SSH:lla

Etähallintaa voi suorittaa monella tapaa ja se on hyvin tehokasta verrattuna paikanpäällä tapahtuvaan hallintaan. Yleisimmillään laitteen esimerkiksi ADSL-modeemin etähallinta voidaan suorittaa selaimella ja SSL-suojauksella, käyttäen HTTPS-protokollaa, sekä asettamalla laitteelle julkinen IP-osoite hallintaa varten. Käytettäessä komentorivipohjaista etähallinta liittymää ensimmäisenä tulee mieleen Telnet, joka on yksi tapa luoda yhteys, mutta siinä ei ole minkäänlaista suojausta. Telnetille vaihtoehtona on SSH, josta mainitsin jo aiemmin merkkipohjainen hallinta osiossa 3.1. SSH tarjoaa vahvan suojauksen etähallintaan autentikoinnilla ja tiedon kryptauksella.

SSH:sta on olemassa kaksi versiota SSHv1, eli ensimmäinen versio ja SSHv2, eli uudempi versio. SSHv1 sisältyy Ciscon IOS julkaisuihin. [7, s. 138-139.]

SSH terminal-line access ominaisuuden tuomia hyötyjä esimerkiksi reitittimiin tai tukiasema ohjaimeen on että se voidaan yhdistää laitteeseen, johon on jo kytketty laitteita console-porttiin, kuten reitittimiä tai kytkimiä. Helppo ja turvallinen liittäminen mistä tahansa. Reitittimeen liitetyillä modeemeilla voidaan luoda suojattu yhteys. Voidaan luoda käyttäjä tunnistus, jokaiselle linjalle, käyttäen TACACS+ tai RADIUS:sta. [7, s. 138-139.]

Useimmat laitteet voivat toimia joko SSH-asiakkaana tai SSH-palvelimena. SSH-asiakasohjelma tarjoaa laite autentikoinnin ja salauksen ja sillä on tarkoitus luoda yhteys toisiin laitteisiin jossa on SSH-palvelinohjelmisto. Esimerkiksi kaksi reititintä voidaan liittää toisiinsa niin että toinen toimii asiakkaana ja toinen palvelimena. Tieto voidaan salata DES kryptauksella ja käyttäjä voidaan tunnistaa, joko TACACS+:lla tai RADIUS-protokollalla ja myös paikallisesti tallennetuilla käyttäjänimillä ja salasanoilla. [7, s. 139.]

4 VERKONHALLINTAPROTOKOLLAT

Tietoliikenneverkkojen kehityksen jälkeen verkot olivat jo 1970-luvun lopulla suuria ja monimutkaisia ja ovat vain kasvaneet ja monimutkaistuneet lisää sen jälkeen. Nykyisissä verkoissa on useita toisiinsa liitettyjä lähiverkkoja, jolloin ne alkavat olla vaikeasti hallittavia. Tätä varten on kehitetty verkonhallintaan erityisiä protokollia. Ensimmäinen hallintaprotokolla oli SNMPv1, jonka oli tarkoitus olla vain väliaikainen hallintaprotokolla. Käytännössä SNMPv1 oli kuitenkin hyvä, joten sitä vain kehitettiin eteenpäin uudemmissa versioissa, sen sijaan että olisi siirrytty kokonaan uuteen protokollaan. [8.]

SNMP: lisäksi on muutamia muita tärkeitä hallintaprotokollia kuten SDEE ja Syslog, jotka ovat tarkoitettu järjestelmässä tapahtuvien poikkeusten esimerkiksi verkossa tapahtuvien väärinkäytösten ja tunkeutujien seurantaan ja ilmaisuun antamalla hälytyksiä näistä tapahtumista. Toisin kuin SNMP:ssä hallitsija ei voi vaikuttaa toimenpiteillä SDEE:ssä ja Syslogissa, vaan nämä protokollat ovat ainoastaan ilmaisuun tarkoitettuja.

Yksi tärkeä protokolla langattomien verkkojen hallintaan on LWAPP, jolla voidaan yhdistää useita tukiasemia isoissa verkoissa yhden hallintatukiaseman alaisuuteen, eli WLAN-kontrollerin alaisuuteen ja näin ollen saavutetaan keskitetty hallinta.

Seuraavassa osiossa perehdyn tarkemmin edellä esitettyihin verkonhallintaprotokolliin.

4.1 SNMP

SNMP (Simple Network Management Protocol) on IETF:n määrittämä valmistajariippumaton verkonhallintaprotokolla. Protokolla määrittelee hallintaohjelmien toiminnot ja kertoo miten tieto on määritelty ja lähetetty. Protokolla toimii OSI-mallin seitsemännessä kerroksessa ja kuuluu TCP/IP-protokolla-sarjaan. Se käyttää tiedonsiirrossa pääasiallisesti ”yhteydetöntä” UPD/IP-yhteyttä, jolla raportoitava tieto saadaan kuljetettua vaikka verkko olisi kuormitettu ja yhteyden katkettua tieto voidaan varastoida ja lähettää uudestaan, kun yhteys on taas päällä. SNMP on hallintatyökalu reitittimille, kytkimille ja tukiasemille ja sen tarkoitus on tutkia näiden laitteiden tapahtumia ja mahdollisia vikoja, sekä lähettää niistä raportteja hallinta-asemalle. SNMP:llä voidaan myös korjata vikoja asettamalle laitteelle uusia parametreja etähallinnalla. SNMP:n tyypilliseen toimintaympäristöön kuuluu normaali hallintatyöasema tai palvelin NMS (Network Management Station), kohteissa olevat agentit ja hallintatietokanta MIB (Management Information Base). [1, s. 306-308; 9, s. 10.]

Agentit ovat hallittavilla laitteilla olevia ohjelmistoja, joilla mahdollistetaan yhteys hallinta-asemaan. Agentit keräävät haluttua tietoa hallittavasta laitteesta ja lähettävät ne hallinta-asemalle. Kun NMS lähettää pyynnön Get-request hallintavalle laitteelle se vastaa siihen Get-response -viestillä.. Laitteessa tapahtuvista muutoksista tai vioista voidaan myös lähettää sanoma agentin sisältämillä Trap- ja Inform-sanomilla. Agenttien lähettämä tieto säilötään muuttujina MIB:n tietokantaan. [9, s. 12.]

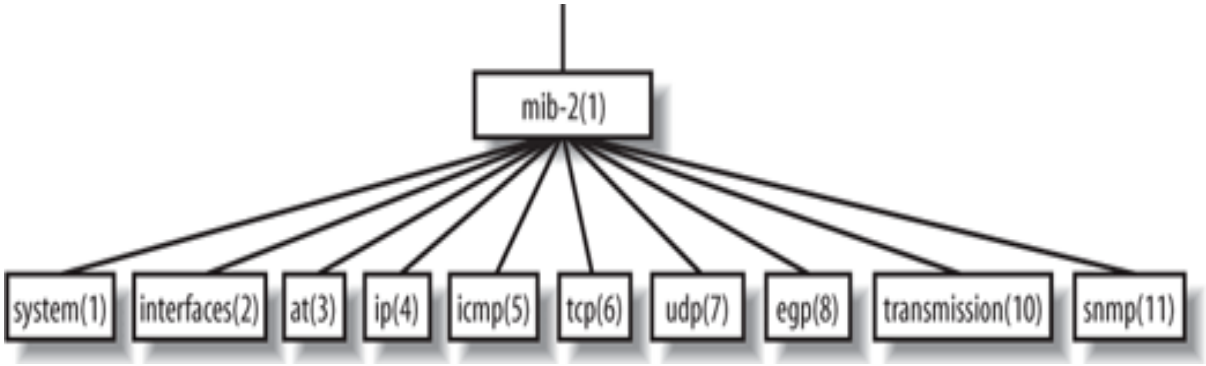
MIB on tietokanta tai taulukko hallittavien objektien rakenteesta sekä malli hallinnan rakenteesta. Tietokannassa on yli 1000 toimittajakohtaista objektia. Objektit ovat esityksiä verkon todellisesta rakenteesta. Objektien tarkoitus on kerätä tietoa esimerkiksi lähetettyjen ja vastaanotettujen pakettien määrästä reitittimen tietyssä LAN-portissa,

jonka se säilöö ja lähettää NMS:lle. MIB ilmoittaa hallittavan laitteen datan muuttujina. Muuttujat voidaan tunnistaa OID (Object Identifier) numeroilla. MIB:stä on olemassa kahta tyyppiä MIB I ja MIB II. Lisäksi MIB:n on olemassa laajennus RMON. [1, s. 309-310; 9, s. 13.]

RMON:in tarkoitus on laajentaa MIB:tä, sillä MIB ei tarjoa kuin tietoja sen alaisuudessa olevalta agentilta. RMON:lla saadaan kerättyä koko verkon liikenne keskitetysti. RMON:sta on kehitetty myös toinen versio RMON2, joka tarjoaa seurantaa OSI-mallin ylempiin kerroksiin esimerkiksi sähköpostin tai selain-liikenteen seuraamiseen. [9. s. 25-30.]

MIB:n olioiden luomiseen on luotu säännöt SMI (Structure of Management Information). Siinä määritellään olioiden rakenne, nimi ja millaista koodausta tulee käyttää MIB:n luomiseen. [2, s. 13.]

Kuvassa 5 on osa MIB rakenteesta, jossa esimerkiksi agentin lähettämä OID numero 4 tarkoittaa objektia ip(4), joka taas tarkoittaa lähetettyjen ja vastaanotettujen IP-pakettien määrää.



Kuva 5. Osa MIB:n rakenteesta [10.]

4.1.1 SNMPv1

SNMP:n ensimmäinen versio ilmestyi vuonna 1988 ja sen virallinen julkaisu tuli vuonna 1990 RFC 1157 suosituksella. Versio määritti (NMS) hallinta-aseman ja agenttien (MIB) välistä kommunikaatiota, joka tapahtuu OSI-mallin seitsemännessä

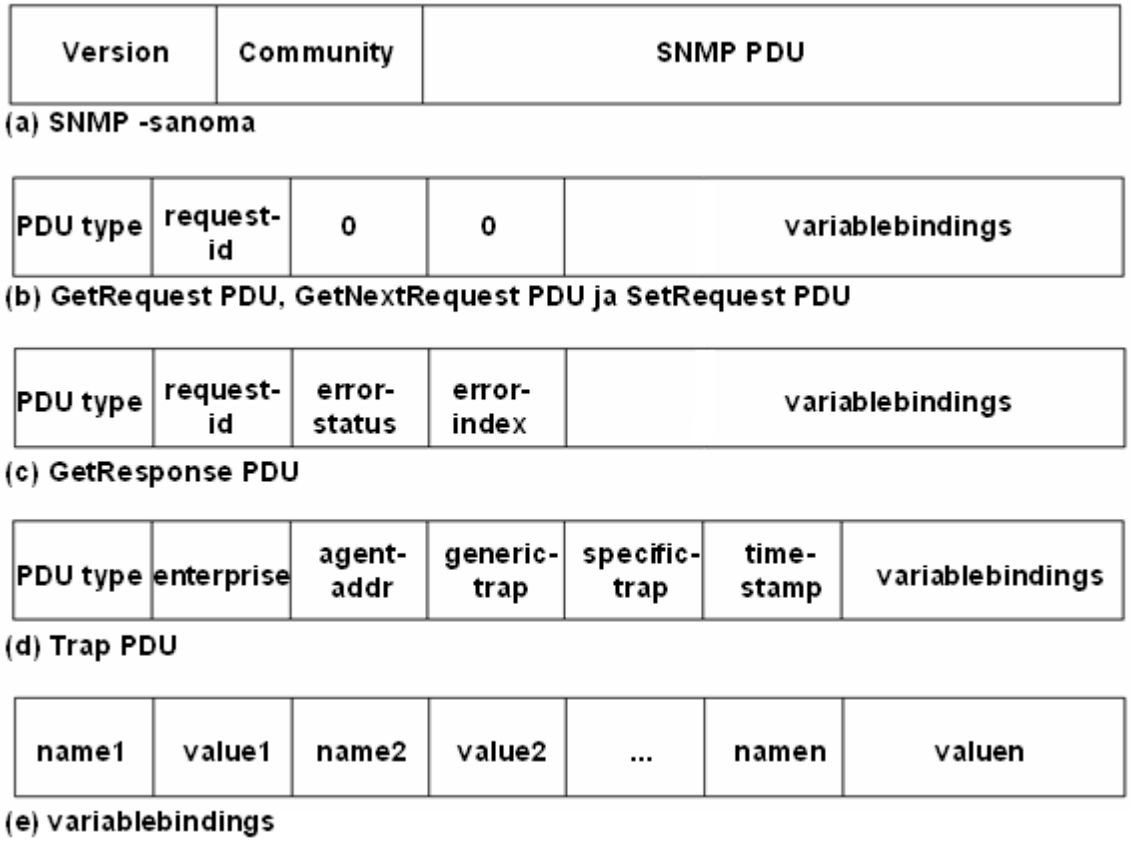
kerroksessa. SNMP käyttää TCP/IP-liikennettä ja UDP-protokollaa käyttäen portteja 161 ja 162. Portti 161 on varattu agentille, jota se käyttää vastaanottamaan Get- ja Set-operaatioita. Portti 162 on taas NMS:lle varattu vastaanottoportti Set-operaatooille. Lähettämiseen voidaan käyttää mitä tahansa porttia. [9, s. 14-15.]

SNMP:n sisältämät operaatiot ovat Get, Set ja Trap. Get-operaatio tarkoittaa sitä, että hallintalaite pyytää agentilta jotain arvoa. SNMPv1:ssä Get-operaatioita on kahdenlaisia Get ja GetNext. GetNext komento lähettää eri arvon kuin Get komento jolloin hallintalaite saa MIB:n rakenteen selville. Set-operaatio taas tarkoittaa että hallintalaite asettaa agentille jonkin arvon tai poistaa sen. Set-operaatio lähetetään NMS:tä agentille PDU:n, johon on sisällytetty päivitettävän objektin nimi OID ja uusi arvo objektille. Agentti vastaa Set-pyyntöön sen onnistuessa tai jos pyyntö epäonnistuu se lähettää virheilmoituksen. Trap-operaatio tarkoittaa että agentti lähettää arvon hallintalaitteelle itsestään esimerkiksi jos reitittimen jokin johto irtoaa Trap voi lähettää hallintalaitteelle siitä ilmoituksen. Kuvassa 6 on SNMPv1 käyttämien eri PDU-pakettien muodot. [9, s. 15-16.]

Get-, Set- ja Trap-operaatiot:

- **Get**: Tarkoittaa että hallintalaite pyytää agentilta jotain arvoa.
- **Set**: Tarkoittaa että hallintalaite asettaa agentille arvon
- **Trap**: Agentti lähettää arvon hallintalaitteelle itsestään. [9, s. 15.]

Turvallisuudeltaan SNMv1 on heikko. Tunnistus tapahtuu käyttäen Community string-tyyppistä salasanaa, joka ei suojaa tietoa millään tavalla ja on helppo hakkeroida. Community string-avain voidaan määritellä joko read-only tai read-write tyyppiseksi, jolloin read-only avaimella käyttäjä voi käyttää ainoastaan Get-operaatioita ja read-write avaimella käyttäjälle sallitaan sekä Get- että Set-operaatioita. [9, s. 16-17.]



Kuva 6. SNMPv1:n eri PDU-paketien muodot [9, s. 17.]

4.1.2 SNMPv2

SNMPv2 kehitettiin vuonna 1993 ensimmäisen version jatkoksi. Toinen versio ei itsessään sisällä minkäänlaista hallintaa, vaan tarjoaa rungon johon hallintaohjelmistoja voidaan kehittää. Toiseen versioon on myös kaksi lisä-laajennusta SNMPv2c ja SNMPv2u. Tietoturvallisuudeltaan SNMPv2 on samankaltainen, kuin aiempi versio, eli käyttäjät tunnistetaan Community string-avaimilla. Tämä onkin SNMPv2 yksi heikkouksista ensimmäisen version tapaan. Vasta kolmannessa versiossa on paneudutttu turvallisuuteen. [11, s. 705; 9, s. 18-19.]

SNMPv2 tuomia uudistuksia ensimmäiseen versioon on GertBulk- ja Inform-operaatiot. GetBulk:n tarkoitus on pyytää agenteilta isoista taulukoista mahdollisimman paljon kerättävää tietoa NMS:lle. Inform taas on trap-operaatio, jossa hallinta asema lähettää agentille kuittauksen saadusta informaatiosta ja jos agentti ei saa kuittausta se yrittää lähetystä uudelleen, näin varmistetaan tiedon kulku. SNMPv2:ssa on

myös parannettu suorituskykyä ja luotettavuutta, kuten yllämainittu Inform-operaatio, myös hallinta-asemien välistä kommunikaatiota on paranneltu. [9, s. 19.]

Ominaisuuksiltaan SNMPv2 sisältää Proxy-agentin, jonka tarkoitus on kääntää viestit SNMPv2 muodosta aiempaan SNMPv1 muotoon, koska SNMP:n versiot 1 ja 2 eivät ole suoraan yhteensopivia. Toinen tapa kääntää viesti versioiden välillä on kaksikielinen NMS. Proxy-agentti pystyy myös kääntämään ja lähettämään operaatioita laitteille, jotka eivät tue SNMP:tä. [9, s. 20.]

4.1.3 SNMPv3

SNMPv2:ssa ilmenneiden toiminnallisten ja turvallisuuteen liittyvien vajavuuksien johdosta on SNMP:tä kehitetty eteenpäin kolmannessa versiossa SNMPv3. Protokolla standardoitiin vuonna 2002 RFC 3411–3418 mukaisesti. Standardin tärkeimpiä ominaisuuksia on parempi tietoturva verrattuna aiempiin standartteihin. [7, s. 288.]

SNMPv3:n sisältämät tietoturva ominaisuudet ovat *Message integrity*, joka takaa että tieto on alkuperäisessä muodossaan siirron jälkeen, eli kukaan ei ole päästy muokkaamaan sitä siirron aikana. *Authentication*, joka määrittelee mistä tieto on lähtöisin ja varmistaa että se on oikealta lähettäjältä. *Encryption*, joka salaa siirrettävän tiedon, jotta ulkopuoliset eivät voi tulkita viestejä millään tavalla. [7, s. 288.]

SNMPv3 sisältää erilaisia turvallisuusmalleja ja tasoja, jotka voidaan havainnollistaa taulukosta 1. Turvallisuusmallilla tarkoitetaan käyttöön otettavaa turvallisuustavan valitsemista käyttäjälle ja käyttäjäryhmille sopiviksi. Eri tasoilla taas tarkoitetaan kuinka korkea turvallisuustaso asetetaan mallille. Yksittäisille käyttäjille ja ryhmille voidaan asettaa tasosta riippuen joko autentikointisalasana tai salaussana, myös molempia voidaan käyttää yhtä aikaa. SNMPv3 ominaisuuksiin kuuluu myös laitteiden konfiguroinnit, eli laitteen asetuksia voidaan muokata set-komennoilla. [7, s. 280.]

Taulukko 1. SNMP eri versioiden käyttämät suojausmallit [7, s. 289.]

Versio	Taso	Autentikointi tapa	Tiedon salaus	Käytäntö
SNMPv1	noAuth noPriv	Community string	Ei salata	Community string tunnistus
SNMPv2c	noAuth noPriv	Community string	Ei salata	Community string tunnistus
SNMPv3	noAuth noPriv	Käyttäjänimi	Ei salata	Käyttäjänimi tunnistus
SNMPv3	Auth noPriv	MD5 tai SHA	Ei salata	MD5 tai SHA tunnistus
SNMPv3	Auth Priv	MD5 tai SHA	DES [3]	MD5 tai SHA tunnistus ja DES-salaus

SNMPv3:n tuomia etuja aiempiin versioihin on että tieto voidaan kerätä turvallisesti laitteelta ilman, että kukaan pääse sitä muuttamaan eikä tieto pääse korruptoitumaan. Tieto on luottamuksellista. Verkon yli siirrettävät ohjaustiedot voidaan salata niin, että ne eivät näy verkossa. [7, s. 289.]

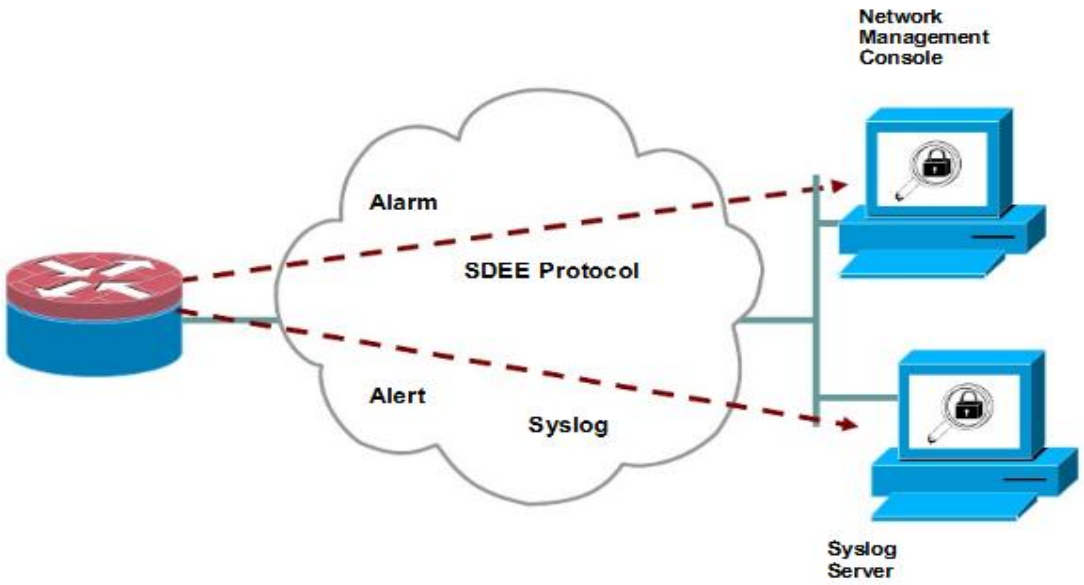
4.2 Tapahtumien seuranta

Laitteiden tapahtumien seurantaan on olemassa eri protokollia. Seurattavat laitteet voivat olla kytkimiä, reitittimiä, tukiasemia yms. Seurattavalle laitteelle tulee valita jokin tapa millä tapahtumia kerätään, sillä se voi vaikuttaa verkon suorituskykyyn ja ajoituksiin. Tapahtumia voidaan kerätä kahdella eri menetelmällä push tai pull. Kuvassa 7 on push-menetelmää käyttävä syslog ja pull-menetelmää käyttävä SDEE.[12, s. 87-88.]

Push-tapa tarkoittaa, että tapahtumat kerätään tiettyinä ajanhetkinä tai reaaliajassa halutulta laitteelta. Hallinta-asema tai serveri pitää tässä tapauksessa asettaa vastaan-

ottamaan näitä viestejä silloin kuin niitä ilmaantuu. Push-tapaa käyttää mm. Syslog, ACL-logi ja NetFlow. Syslogista kerrotaan lisää luvussa 4.2.2. [12, s. 88.]

Pull-tavassa tapahtumat kerätään hallittavaan laitteeseen ja hallinta-asema tai serveri voi käydä noutamassa halutut tapahtumat haluttuna hetkenä. Tapahtumien lähetys myös varmistetaan, että se saapuu perille toisin kuin push-tavalla. Pull-tapaa hyödyntää SDEE ja myös SNMP, josta kerrottiin luvussa 4.1. [12, s. 88.]



Kuva 7. SDEE ja Syslog toimintamalli [13.]

4.2.1 SDEE

SDEE (Security Device Event Exchange) on osa Cisco Systemsin IPS:ä (Intrusion Prevent System), kuten myös syslog. SDEE-standardi määrittelee viestien muodon ja protokollan mitä käytetään tapahtumien tässä tapauksessa hyökkäysyritysten välitykseen hallinta-asemalle. SDEE:n etuina on, että eri valmistajat pystyvät itse laajentamaan tuotteidensa ominaisuuksia, sillä SDEE perustuu XML, HTTP ja SSL/TLS standardeihin. [12, s. 88-89.]

SDEE on jo useimmissa laitteista kuten reitittimistä, palomuureista ja tukiasemaohjaimista. SDEE on aina käytössä niissä laitteissa joista se löytyy, mutta se ei vastaan-

ota viestejä laitteelta, jos sitä ei ole niin määritelty hallinta-asemalla tai clientissä. SDEE voi säilöä 200-1000 viestiä. [14.]

4.2.2 Syslog

Syslog-protokollan tarkoitus on lähettää tapahtumailmoituksia laitteelta verkon yli logia keräävälle syslog-serverille. Useimmat ohjelmat, prosessit ja käyttöjärjestelmät, kuten Windows ja Linux eroavat toisistaan, joten syslog-viestit voivat olla hyvinkin erilaisia riippuen sen lähteestä. Viestien eroavaisuuksista johtuen viestien sisällöstä ja sen muodosta ei voi tehdä suoria johtopäätöksiä, mutta syslog-protokolla ei olekaan viestien tulkitsemiseen tarkoitettu, vaan sen tarkoitus on vain siirtää tapahtumatiedot laitteelta serverille ilman minkäänlaista kuittausta tapahtumasta. [7, s. 280.]

Syslog perustuu hyvin yksinkertaiseen rakenteeseen ja on näin ollen nopeaa ja kevyttä liikennettä siirtää laitteelta serverille. Jotkin laiteet voivat lähettää syslog-viestejä vaikka vastaanottavaa syslog-palvelinta ei olisi ollenkaan. Jotkin laiteet voivat taas vastaanottaa syslog-viestejä vaikka näin ei olisikaan määritelty. Syslog käyttää UPD-protokollaa viestien siirtoon. Syslogille on myös määritelty tietty UPD-portti (514), jota se käyttää. [7, s. 280.]

Syslog-viestit koostuvat kolmesta osasta. Ensimmäinen osa, eli PRI sisältää koodinumeron, joka kertoo tiedon tärkeydestä. PRI kertoo myös laitetietoja. Toisessa osassa, eli HEADER:ssa kerrotaan tapahtuman ajankohta, sekä lähteen IP-osoite. Kolmannessa osassa, eli MSG kerrotaan mistä ohjelmasta tai prosessista sekä itse viesti sisältö. [7, s. 280.]

4.3 LWAPP

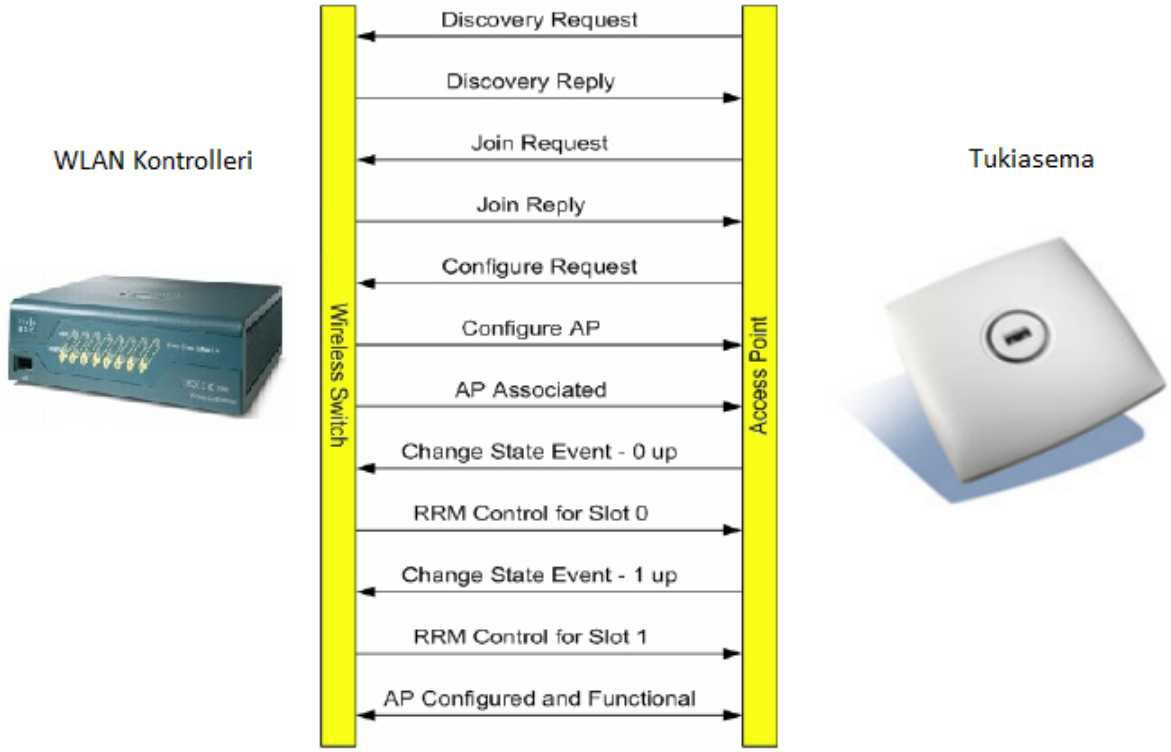
LWAPP (Lightweight Access Point Protocol) on IETF:n hyväksymä RFC 5412 mukainen protokolla, jonka tarkoituksena on määrittää langattoman tukiaseman ja tukiasemaohjaimen välistä liikennettä. LWAPP oli alun perin Airospacen kehittämä protokolla, joka myöhemmin siirtyi Cisco Systemsille. LWAPP on käytössä Ciscon vanhemmissa tukiasemissa ja ohjaimissa, uudemmat käyttävät LWAPP:n pohjautuvaa

CAPWAP-protokollaa, joka on yhteensopiva myös muiden laitevalmistajien kanssa ja aiemman LWAPP:n kanssa. CAPWAP:n ja LWAPP:n eroavat mm. niiden käyttämistä UPD-porteista, kun LWAPP käyttää 12222/12223 portteja CAPWAP taas käyttää 5246/5247 portteja. [15, s.14.]

Protokolla mahdollistaa useamman tukiaseman samanaikaisen hallinnan. Tukiasemia ei tarvitse konfiguroida erikseen vaan tukiasemaohjain hoitaa oikean konfiguraation kaikkiin tukiasemiin. Vianhaku, tukiasemien toiminnan tarkkailu ja verkon liikenteen seuranta helpottuu. [16, s.7.]

LWAPP toimi aiemmin OSI-mallin toisella kerroksella, joten LWAPP:in käyttämä ethernet-kehys rajoitti sen käytön yhden aliverkon alueelle. Sittemmin on siirtynyt käyttämään kolmatta kerrosta ja UPD/IP-protokollaa, joka mahdollistaa eri verkoista tapahtuvan kontrolloinnin. [17, s.33.]

Toimiakseen LWAPP:n tukiasemien pitää tukea LAP (Lightwight accesspoint) ominaisuutta. Osa laitteista on suoraan LAP:tä, mutta laitteet jotka eivät vielä ole voidaan muuntaa LAP:ksi IOS päivityksellä. Päivityksen jälkeen laitetta ei voi konfiguroida muuten kuin kontrollerin kautta. Kuvassa 8 on kontrollerin (WLC) ja tukiaseman (LAP) yhdistyminen, jossa tukiasema lähettää etsintä pyynnön verkossa olevalle WLAN-kontrollerille. Saatuaan vastauksen kontrollerilta tukiasema lähettää yhdistymis-pyynnön kontrollerille ja tämän hyväksyttyä se kontrolleri voi alkaa lähettämään konfiguroituja arvoja tukiasemaan.



Kuva 8. LWAPP-protokollan liikenne kontrollerin (WLC) ja tukiaseman (LAP) välillä [17, s. 34.]

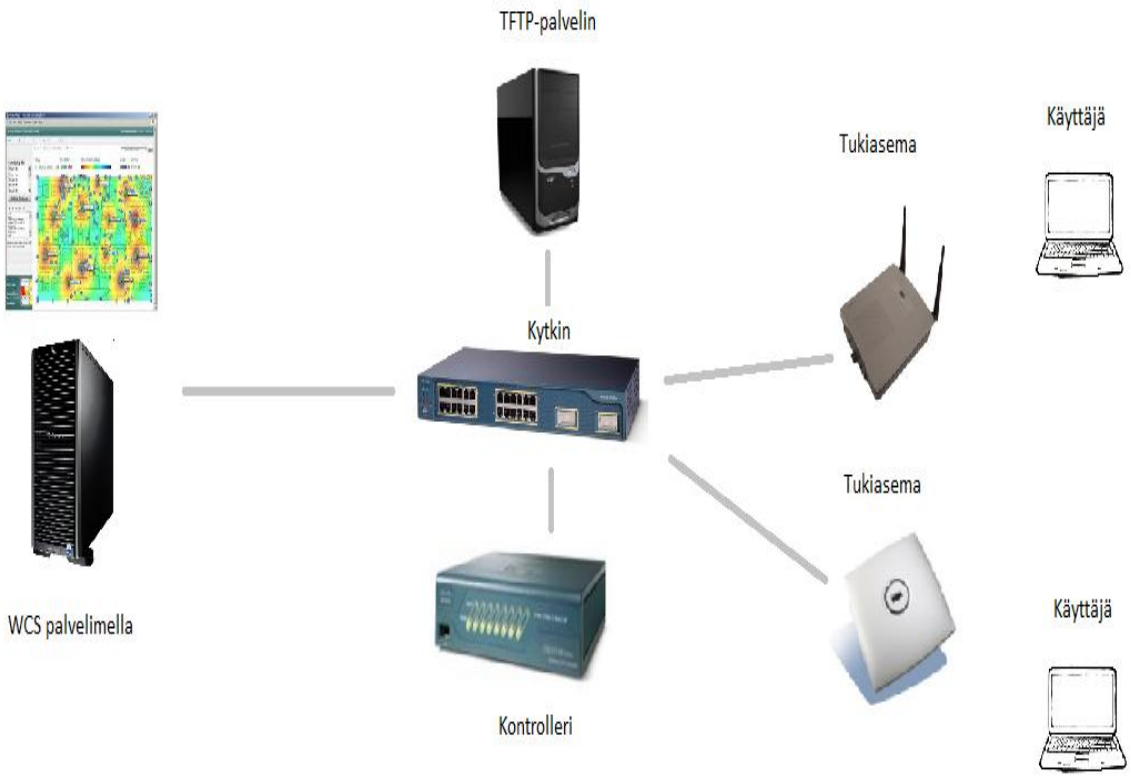
5 TESTIVERKKO JA SEN HALLINTA

Opinnäytetyöni tarkoituksena oli rakentaa koulun laboratorioon testiverkko, jossa pääsee tutkimaan Ciscon WLAN-kontrollerin ja WCS:n käyttöä, asennusta ja ominaisuuksia. Verkko koostuu kuvan 9 mukaisista laitteista, jossa WCS:n palvelimena toimiin tavallinen tietokone, johon on asennettu virtuaalinen Windows 2003-palvelin. TFTP-palvelimena toimii myös tavallinen tietokone, jossa on Cisco Systemsin TFTP-ohjelma. Lisäksi verkossa on kaksi tukiasemaa ja WLAN-kontrolleri. Kaikki laitteet on yhdistetty toisiinsa kytkimellä.

Tukiasemat tarvitsevat toimiakseen käyttöjärjestelmäohjelman, kuten tietokoneessa käytettävä Windows, jolla käyttäjän pystyy kommunikoimaan laitteen kanssa. Tätä käyttöjärjestelmää kutsutaan tukiasemissa nimellä IOS (Interwork Operating System).

Tässä työssä käytetään kahdentyyppisiä IOS-käyttöjärjestelmiä lightweight ja autonomous. näiden kahden erona on, että autonomous IOS:lla tukiasemaa pystytään

ainoastaan käyttämään itsenäisenä laitteena, jossa komennot syötetään suoraan laitteelle. Autonomous IOS on ns. ”normaali” käyttöjärjestelmä, joka löytyy tavallisista tukiasemista. Lightweight IOS:a käytetään WLAN-kontrollerin avulla, jolloin komennot syötetään kontrollerin kautta tukiasemaan. Lightweight muunnoksen jälkeen tukiasemalle voidaan syöttää vai tiettyjä komentoja suoraan, kuten laitteen nimen ja IP-osoitteen vaihtaminen laitteen uudelleen sijoitusta varten. Muut komennot syötetään kontrollerin kautta.



KUVA 9. Testiverkon rakenne

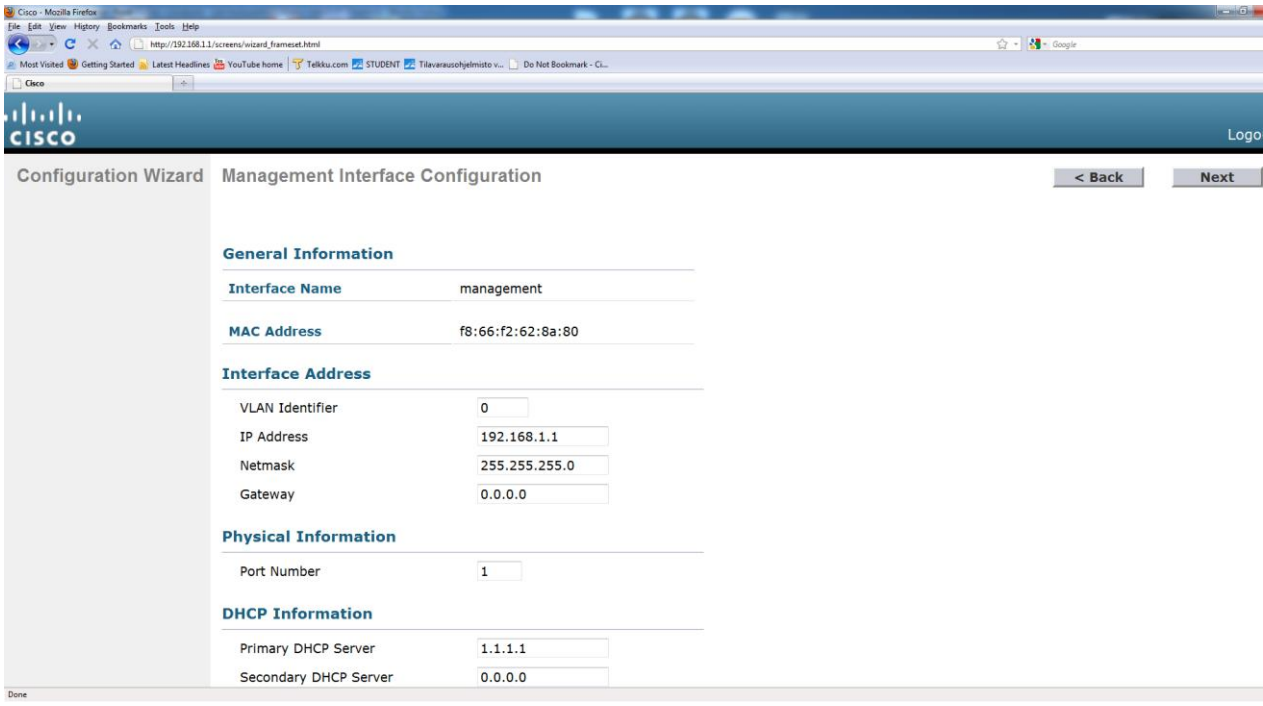
Työssä käytettiin seuraavanlaisia laitteita Cisco AP 1200-tukiasemia, Cisco AP 1130-tukiasemia ja Cisco 2106 WLAN-kontrolleri, sekä normaali kytkin yhdistämään laitteet toisiinsa.

Ohjelmistoina työssä käytettiin WCS-ohjelmaa kontrollereiden ja sitä kautta koko verkon hallintaan. MIB vieweriä SNMP:n tutkimiseen. hyper terminaliä console-yhteyttä varten. Virtuaalinen Windows 2003-palvelin asennettiin WCS-ohjelmistoa varten. Cisco TFTP-palvelinta käytettiin tukiasemien IOS:n palautukseen.

Tukiasemissa käytettävät autonomous, eli ”normaalit” IOS:t ovat *c1130-k9w7-tar.124-25d.JA.tar* 1130-sarjan tukiasemiin ja *c1200-k9w7-tar.123-8.JA2.tar* 1200-sarjan tukiasemiin. Lightweight IOS:t ovat *c1200-rcvk9w8-tar.123-11JX1.tar* 1200-sarjaan ja *c1130-rcvk9w8-tar.123-11JX1.tar* 1130-sarjaan.

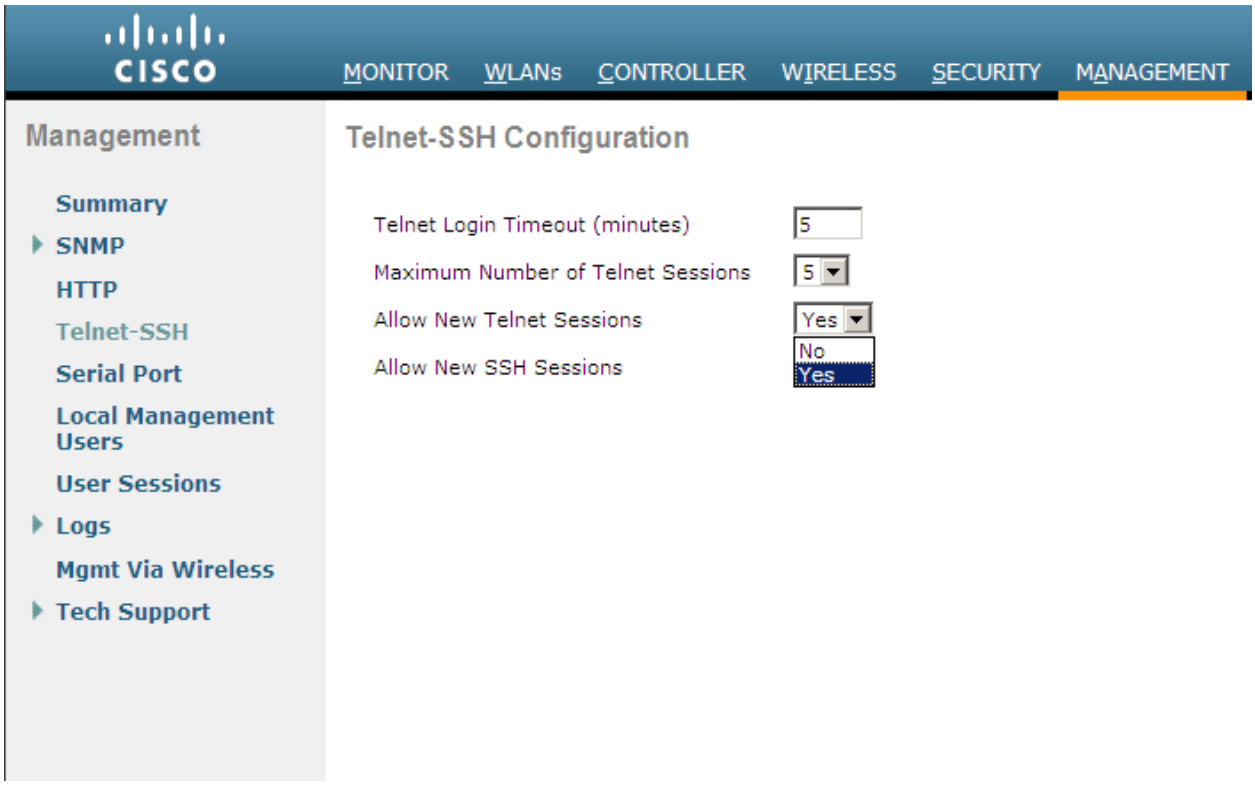
5.1 Kontrollerin käyttöönotto

Kontrolleria voidaan käyttää joko selaimella tapahtuvan hallinnan tai console-yhteyden avulla. Kontrollerin käyttöönotto tapahtuu helpoiten käyttämällä selainta, ottamalla yhteys hallinta IP-osoitteeseen, joka on oletuksena 192.168.1.1. Käytettäessä kontrolleria ensimmäisen kerran, käyttäjää avustetaan alkuun ohjatuilla toiminnoilla kuvan 10 mukaisesti. Alkutoimina kontrolleriin luodaan ylläpitäjän tili, muutetaan hallinta IP-osoite halutuksi ja valitaan maa-alue, joka on tärkeä että oikeat ja sallitut taajuusalueet tulevat käyttöön. Lisäksi luodaan muutamia muita perusasetuksia.



KUVA 10. Kontrollerin ohjattu alustus ja hallinta IP-osoitteen asettaminen

Alustustoimien jälkeen tärkeimpänä ominaisuutena kontrolleriin pitää sallia Telnet-yhteys Upgrade-toolia varten, jolla päivitetään tukiasemien IOS:t. Telnetin salliminen tapahtuu management-välilehdeltä telnet-ssh-kohdasta kuvan 11 mukaisesti. Mitään muita asetuksia ei tässä vaiheessa tarvitse välttämättä tehdä.



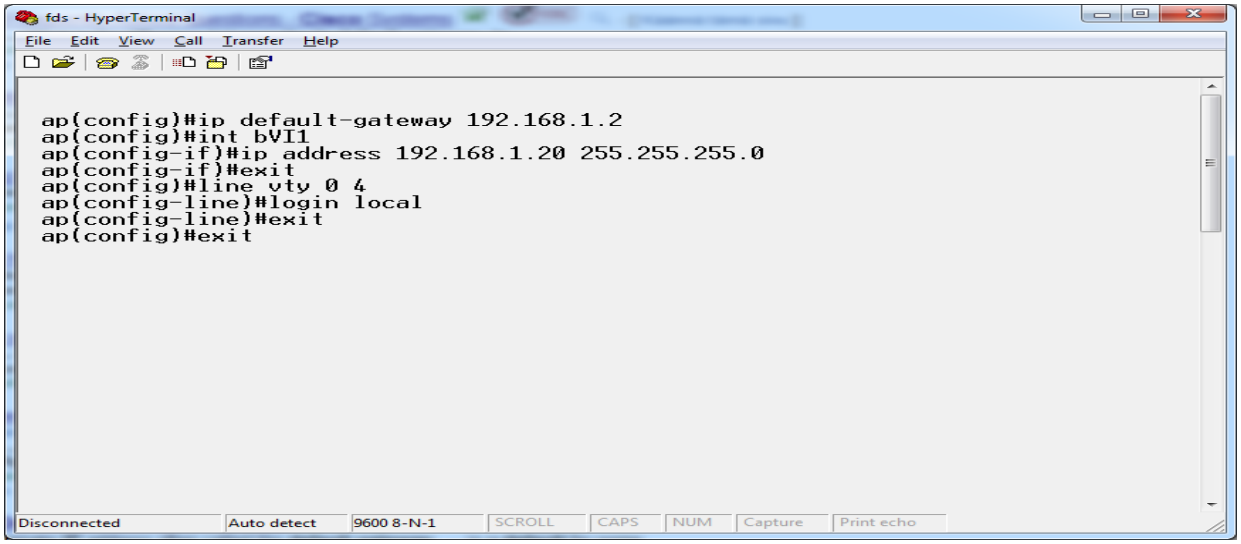
KUVA 11. Telnetin salliminen kontrollerissa

5.2 Tukiaseman IOS-päivitys

Toimiakseen WLAN-kontrollerin kanssa tukiasemat pitää muuntaa autonomous-ap:sta lightweight-ap-muotoon. Tämä tapahtuu päivittämällä tukiaseman IOS. Tätä varten Cisco Systems on kehittänyt *CiscoAironet-AP-to-LWAPP-Upgrade-Tool*-ohjelman, joka on kuvassa 15. Ohjelman avulla käyttäjä voi päivittää kuusi tukiasemaa yhtä aikaa. kaikkien yhtä aikaa päivitettävien tukiasemien tulee olla samanmallisia. Ohjelma toimii ainoastaan Windows XP-käyttöjärjestelmässä, josta pitää myös ottaa palomuuri pois käytöstä päivityksen ajaksi.

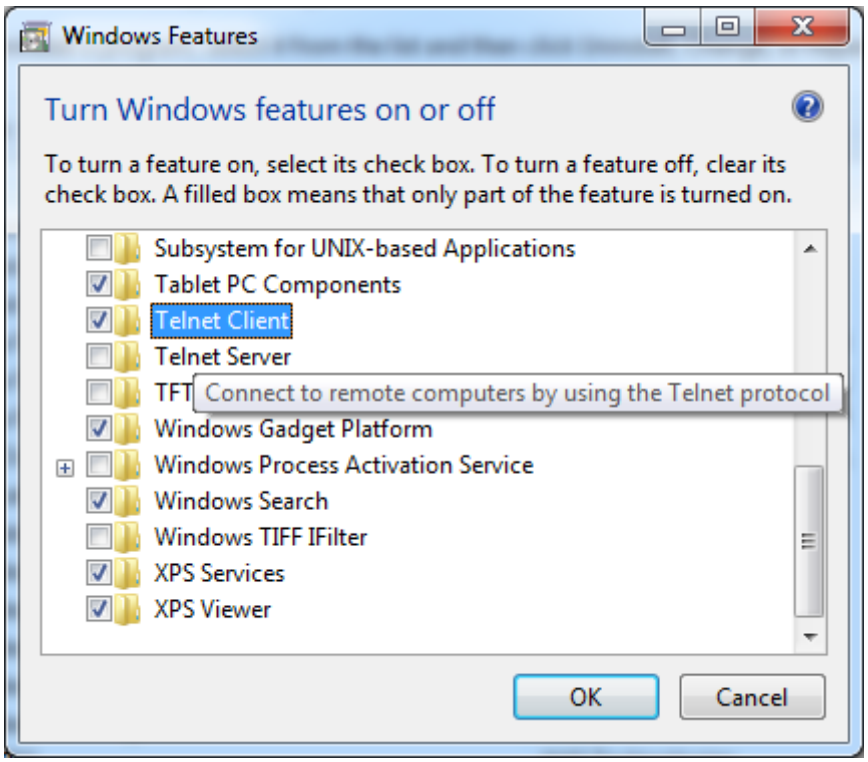
Ennen päivitysohjelman ajamista tarvitsee tukiasemiin ja kontrolleriin sallia telnet-yhteys. Kontrollerissa telnet sallitaan kuvan 11 mukaisesti ruksaamalla telnet-kohta. Tukiasemiin pitää telnetin lisäksi asettaa ip-osoite ja default-gateway. Kuvassa 12 on esimerkki näiden asetusten luomiseen. Käyttäjätunnuksena ja salasanana voidaan käyttää oletustunnuksia Cisco ja Cisco, nämä voidaan myös tarvittaessa luoda komennoilla:

ap#configure terminal
ap(config)#username xxx password xxx
ap(config)#line vty 0 4
ap(config-line)#
ap(config-line)#login local



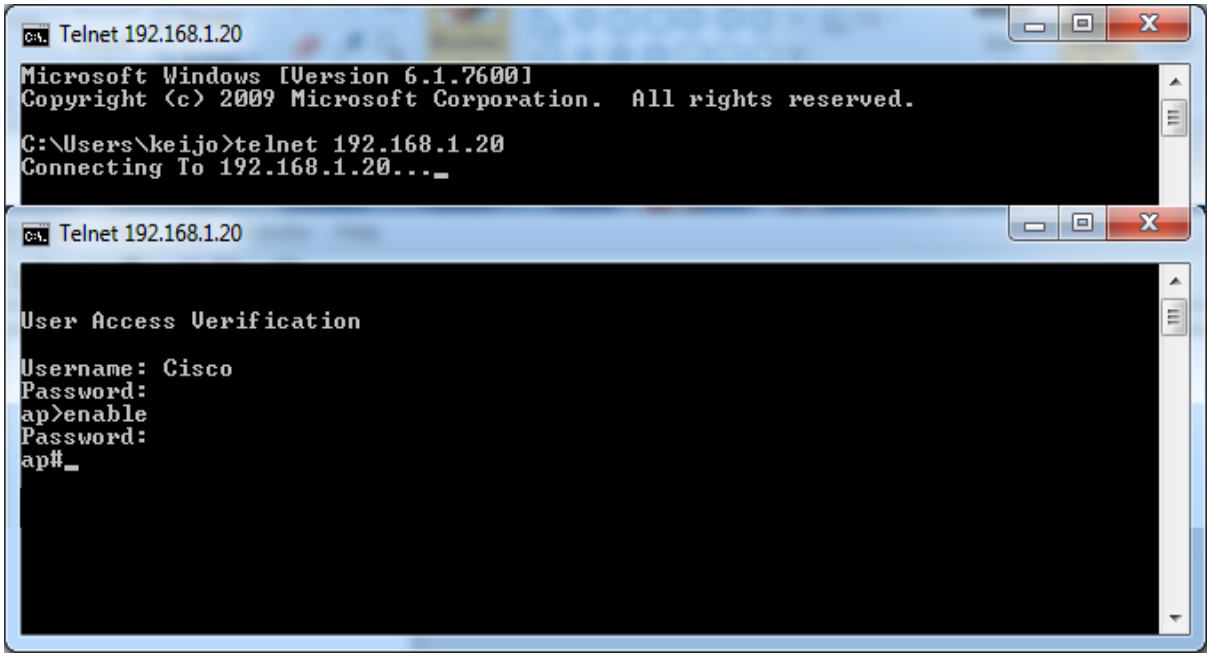
KUVA 12. Tukiaseman päivitykseen tarvittavat konfiguraatiot

Telnetin toimivuus on hyvä testata ennekuin päivitysprosessi alkaa. Toimivuus voidaan testata käyttämällä käyttöjärjestelmän Telnet-asiakasohjelmaa, joka on oletuksena käytössä Windos XP-järjestelmissä. Uudemmissa käyttöjärjestelmissä telnet pitää ottaa käyttöön ohjauspaneelista kuvan 13 mukaisesti.



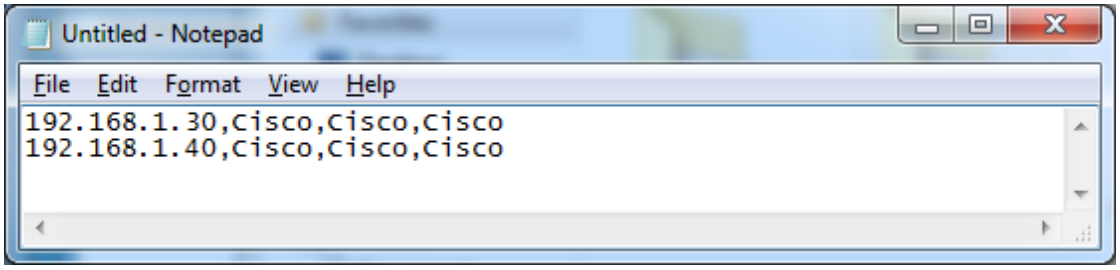
KUVA 13. Telnetin käyttöönotto

Telnet-yhteys voidaan tämän jälkeen luoda syöttämällä komentokehotteeseen telnet-komento ja sen perään ip-osoite, kuten kuvassa 14, jonka jälkeen syötetään käyttäjätunnus ja salasana ja näin saadaan varmistettua, että yhteys varmasti toimii päivityksen aikana.



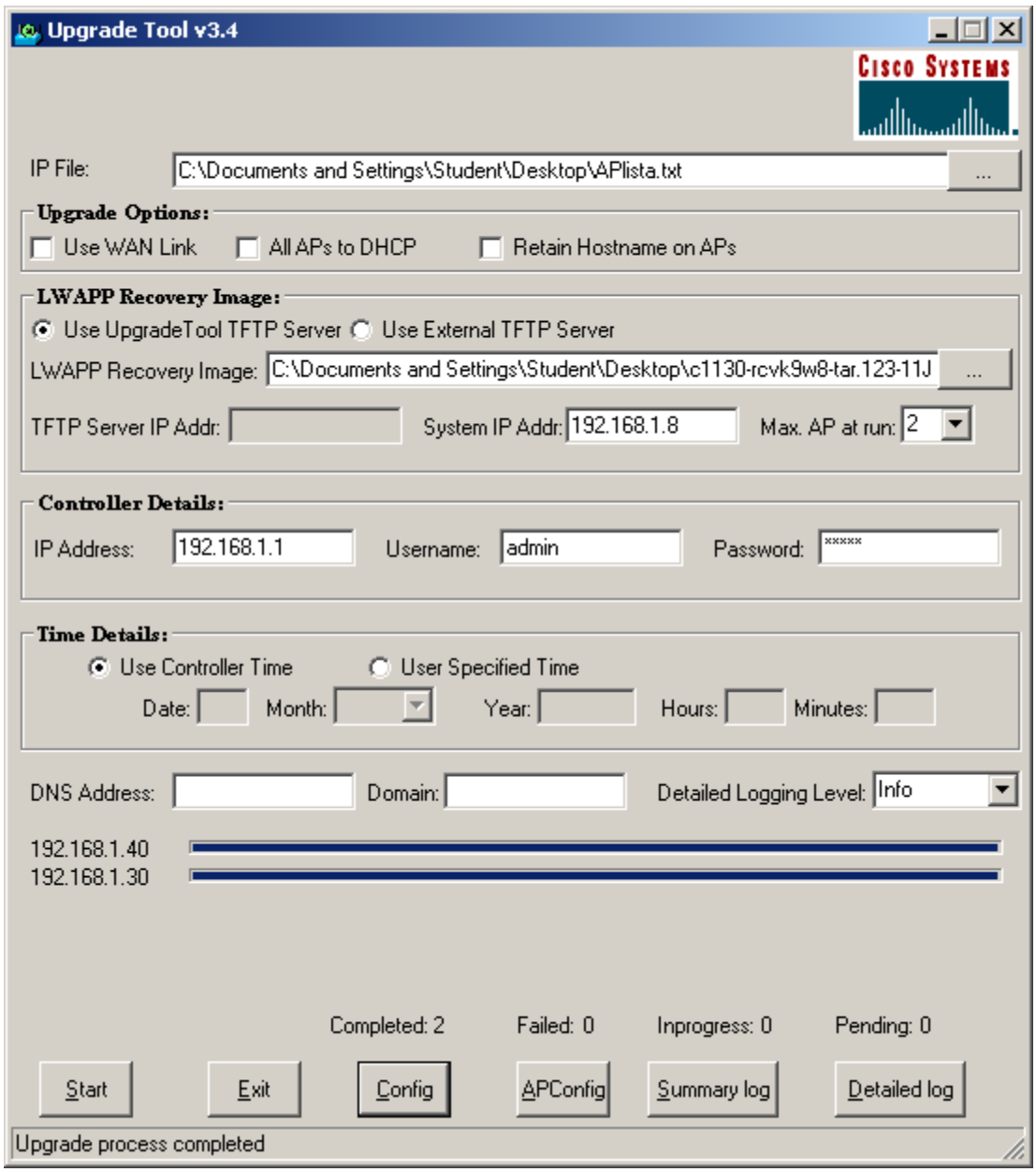
KUVA 14. Telnet-yhteyden testaaminen

Tukiaseman konfiguroinnin ja telnetin testauksen jälkeen voidaan upgrade-tool ajaa. Ohjelmaa varten pitää tehdä tekstitiedosto, jossa on tukiaseman ip-osoite, käyttäjätunnus, salasana, ja enable-secret-salasana. Enable-secret-salasanaa ei välttämättä tarvita, mutta voidaan halutessa laittaa, oletuksena tämäkin on Cisco. Listaan voidaan laitta kerralla kuuden tukiaseman tiedot. Kuvassa 15 on esimerkki listasta.



KUVA 15. Tukiasemien listaus tekstitiedostoon

Upgrade-tooliin tekstitiedosto lisätään IP File-kohtaan, kuvan 16 mukaisesti. Päivitettävä IOS tiedosto, tässä tapauksessa *c1130-rcvk9w8-tar.123-11JX1.tar* lisätään LWAPP Recovery Image kohtaa., josta se välittyy ensin kontrolleriin TFTP-protokollalla ja kontrollerista eteenpäin tukiasemiin. Upgrade-tool sisältää oman TFTP-palvelimen, mutta myös erillistä palvelinta voidaan käyttää haluttaessa. Seuraavaan kohtaan lisätään kontrollerin hallinta IP-osoite, joka on oletuksena 192.168.1.1, sekä salasana ja käyttäjätunnus, jotka ovat oletuksena admin ja admin. Seuraavassa kohdassa määritellään aika. Tässä kohdassa on hyvä käyttää Use Controller Time. Vanhempia tukiasemia päivitettäessä kellonajat pitää olla synkronoitu kontrollerin ja PC:n välillä, jossa upgrade tool on, jotta SSC-sertifikaatti saadaan luotua. Uudemmat tukiasemat käyttävät MIC-sertifikaatteja, jolloin se on jo valmiiksi sisällytetty tukiasemaan eikä sitä tarvitse luoda. SSC-sertifikaatteja tarvitaan, jos vanhemmat tukiasemat halutaan liittää WCS-ohjelmistoon. MIC-sertifikaatit siirtyvät automaattisesti WCS-ohjelmaan. DNS address kohta voidaan jättää tyhjäksi. MIC-sertifikaatti löytyy kaikista vuoden 2005 jälkeen tuotetuista Cisco Systemsin laitteista. [18.; 19.]

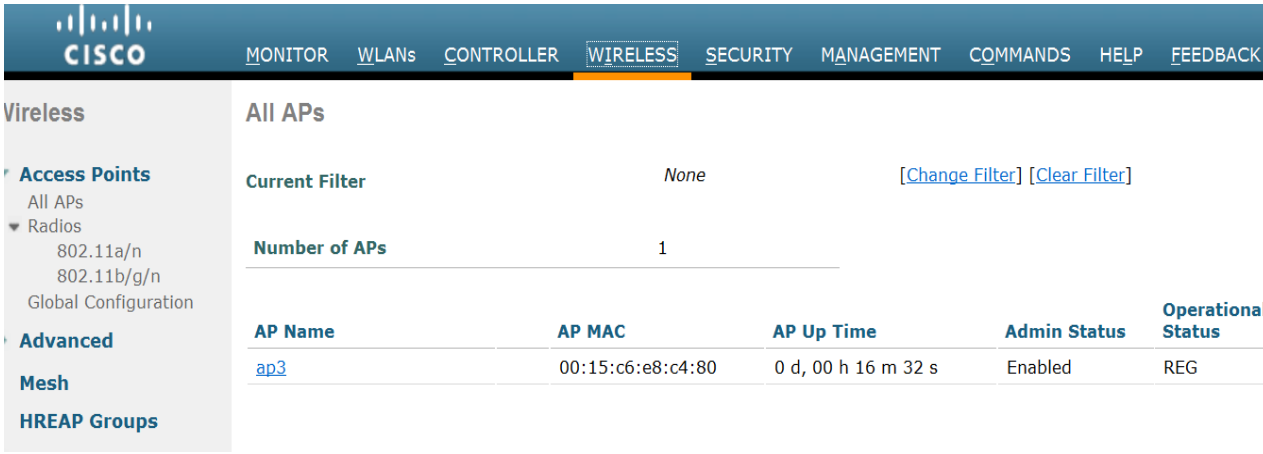


KUVA 16. Upgrade-tool

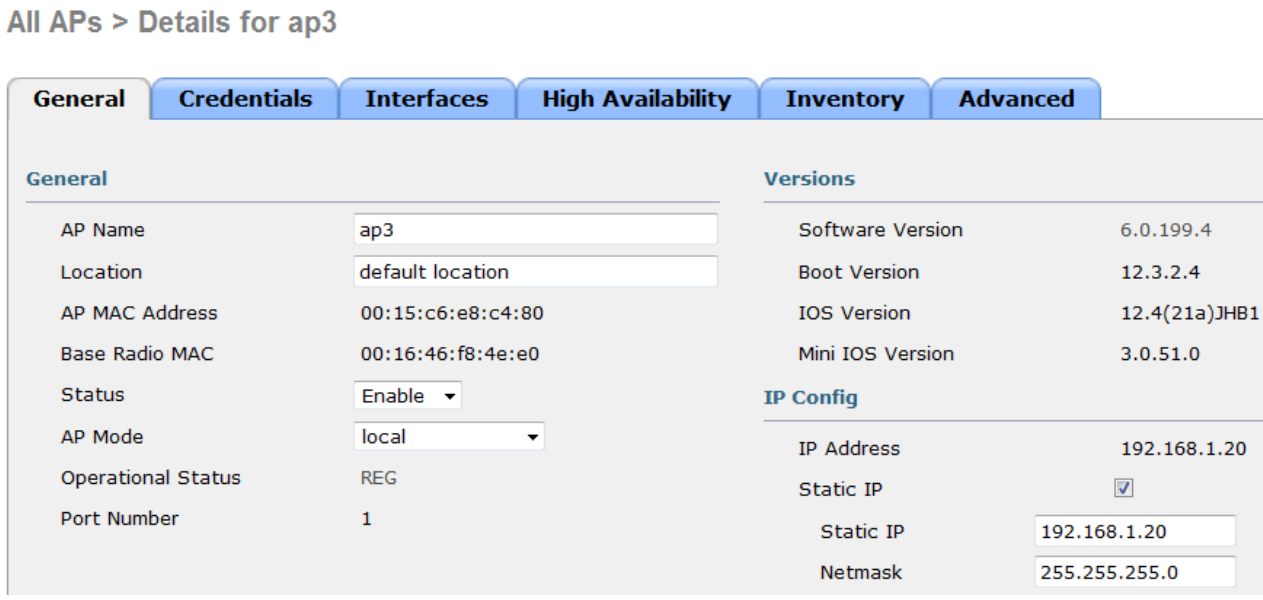
Päivityksen jälkeen tukiasemalle ei voi tehdä paljoakaan ilman kontrolleria, ainoastaan laitteen nimen, defaut-gatewayn ja IP-osoitteen pääsee muuttamaan console-yhteydellä esimerkiksi laitteen uudelleen sijoitusta varten, sekä muutamia peruskomentoja, kuten (show running-config) voidaan ajaa. Päivitettäessä vanhemmista IOS:sta LWAPP:n laitteet hävittävät oman IP-soitteen ja default-gatewayn ja ne joudutaan manuaalisesti lisäämään päivityksen jälkeen. Tässä työssä käytetyissä IOS:ssa tätä ei tarvinnut tehdä.

5.3 Kontrollerilla hallinta

Tukiasemien yhdistymisen jälkeen asemat listautuvat kontrolleriin wireless-välilehden alle kuvan 17 mukaisesti. Klikkaamalla tukiasemaan päästää sitä hallinnoimaan samaan tapaan, kuin normaalia tukiasemaa hallitaan selaimella. Kuvassa 18 näkyy kuinka tukiaseman asetuksia voidaan muuttaa.

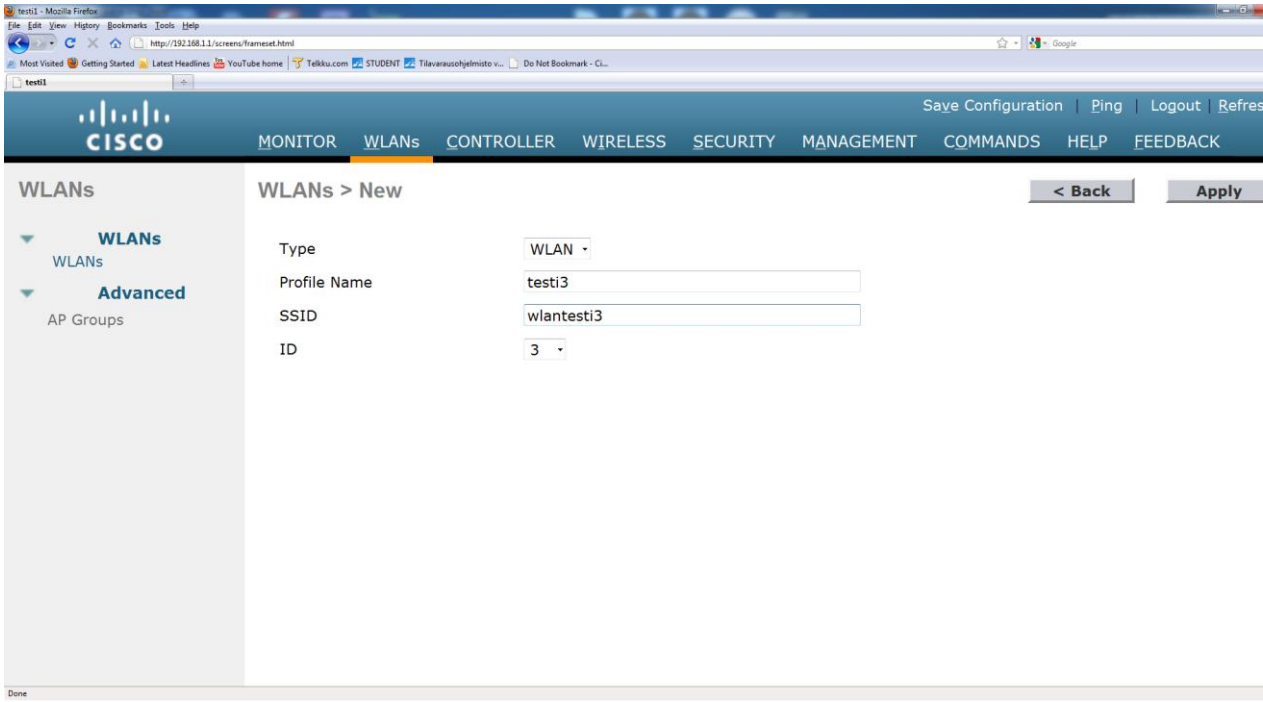


KUVA 17. Liitetyt tukiasemat



KUVA 18. Tukiaseman asetusten muokkaaminen

Langattomien verkkojen luonti tapahtuu WLAN-välilehden alta, jossa käyttäjä pääsee lisäämään SSID:n eli verkon nimen ja muuttaa suojausasetuksia haluamakseen, kuten kuvassa 19 on havannollistettu. Langattomia verkkoja voidaan luoda useampia, esimerkiksi: vieras-verkko ja käyttäjä-verkko, vaikka käytössä olisikin vain yksi tukiasema.

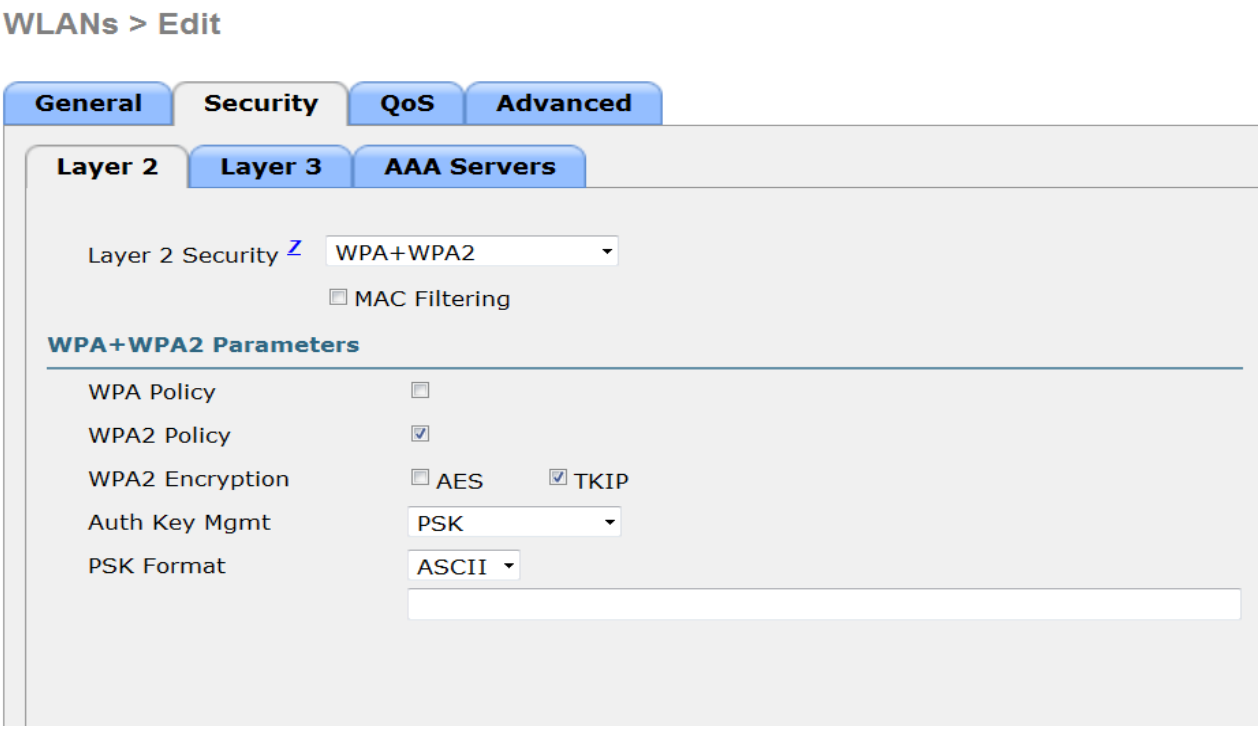


KUVA 19. Langattomien verkkojen luonti

Verkon suojauksen osalta kontrollerista löytyy paljon erilaisia vaihtohehtoja. Autentikointi vaihtoehtoja on RADIUS ja TACAS+. Näistä RADIUS tarvitsee serverille asennettavan RADIUS-palvelimen toimiakseen. TACAS+ voidaan myös käyttää palvelimelta, mutta TACAS+:sta löytyy myös vaihtoehtona paikallinen kirjautuminen, joka sisältää käyttäjä profiilit. Paikalliseen kirjautumiseen voidaan käyttää TACAS+ alta löytyvää local net users:a kuvassa 20, jos autentikointi-palvelinta ei ole olemassa tai se on pois käytöstä. Local net users tallentaa luodut käyttäjä profiilit itse kontrolleriin.

KUVA 20. Local net users

Tavanomaiseen langattoman verkon suojaukseen kontrollerista löytyy samat menetelmät, kuin yleisimmistä langattomista tukiasemista mm. WPA-PSK ja WEP salaukset. Kuvassa 21 näkyy WPA-PSK suojauksen asetus.

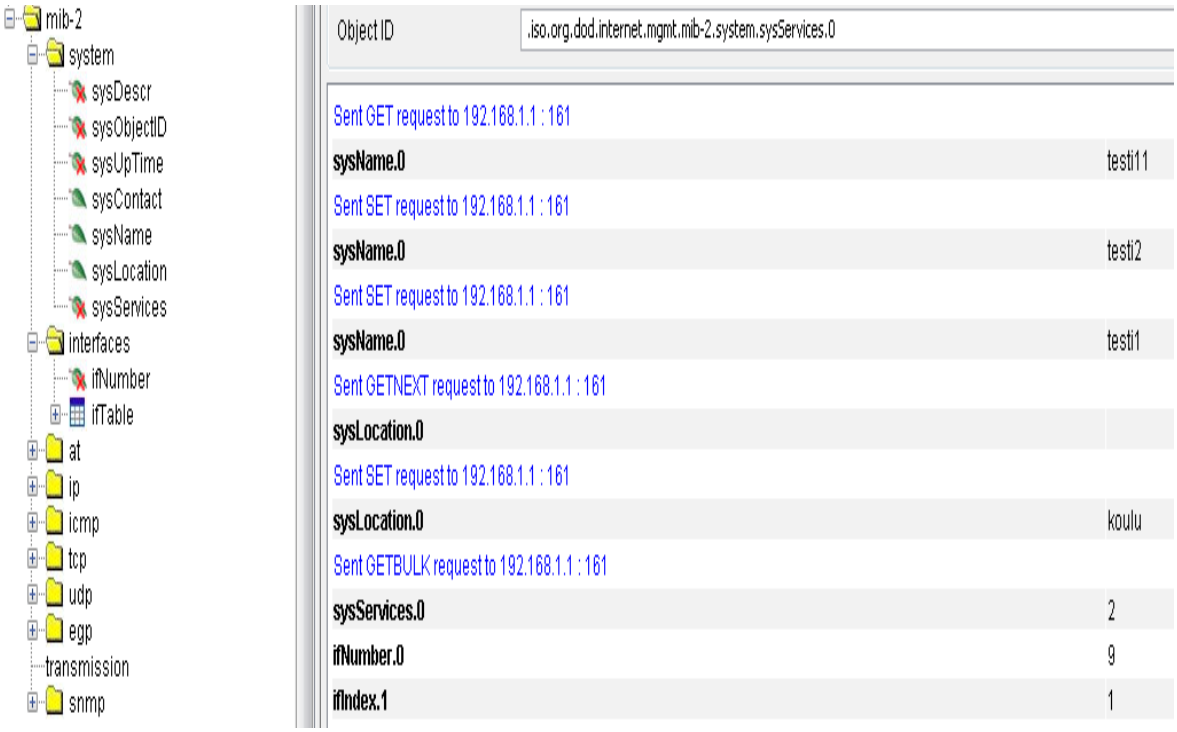


KUVA 21. Langattoman verkon suojaaminen WPA-PSK avaimella

5.4 SNMP ja sen käyttöönotto kontrollerissa

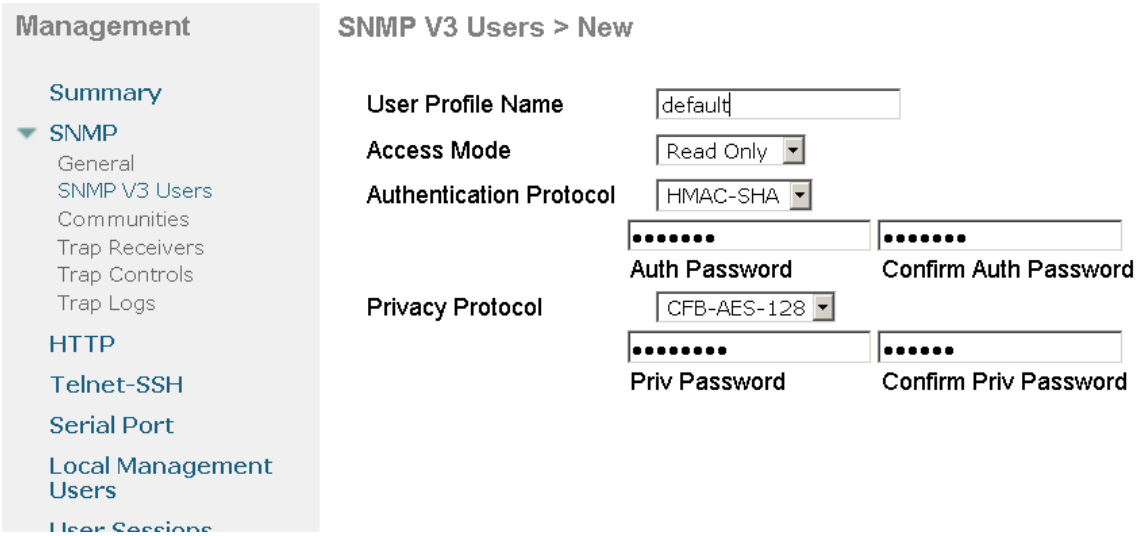
Itse kontrolleria voidaan hallita SNMP-protokollalla, joko käyttäen palvelimelle asennettavaa WCS-ohjelmistoa tai jotain muuta verkonhallintaohjelmaa, joka tukee SNMP:tä. Näin saavutetaan keskitetty hallinta, jossa WCS:llä tai jollain muulla hallintaohjelmalla ohjataan kontrolleria ja sen kautta myös tukiasemia.

Käytettäessä jotakin muuta ohjelmaa, voidaan siihen ladata kontrollerin oma MIB-taulukko Cisco Systemsin sivuilta. Yleisiä MIB-taulukoita voidaan myös käyttää, mutta ne eivät välttämättä tunnista kaikkia laitteen lähettämiä OID:tä. SNMP:n peruskomentoja ovat Get, Getnext, Getbulk ja Set. Kuvassa 22 on havainnollistettu nämä komennot MIB viewerillä käyttäen RFC1213-MIB taulukkoa kontrollerissa.



KUVA 22. SNMP:n peruskäskyt

SNMP saadaan päälle kontrollerissa management välilehden alta, josta löytyy vaihtoehdot SNMP:n eri versioiden käyttöönottoon. Kontrolleri tukee kaikkia kolmea versiota. Tässä työssä käytetään versiota kolme, joka mahdollistaa autentikoinnin ja salauksen protokollalle. Kuvassa 23 on SNMPv3:n käyttöönotto.

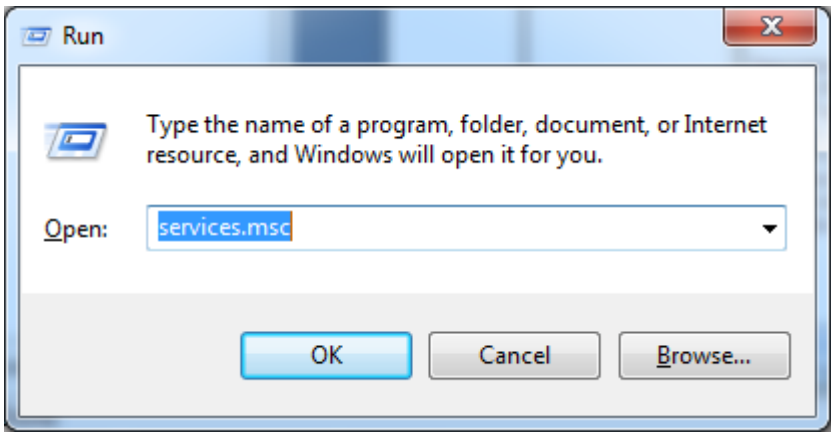


KUVA 23. SNMPv3:n käyttöönotto kontrollerin hallintaa varten

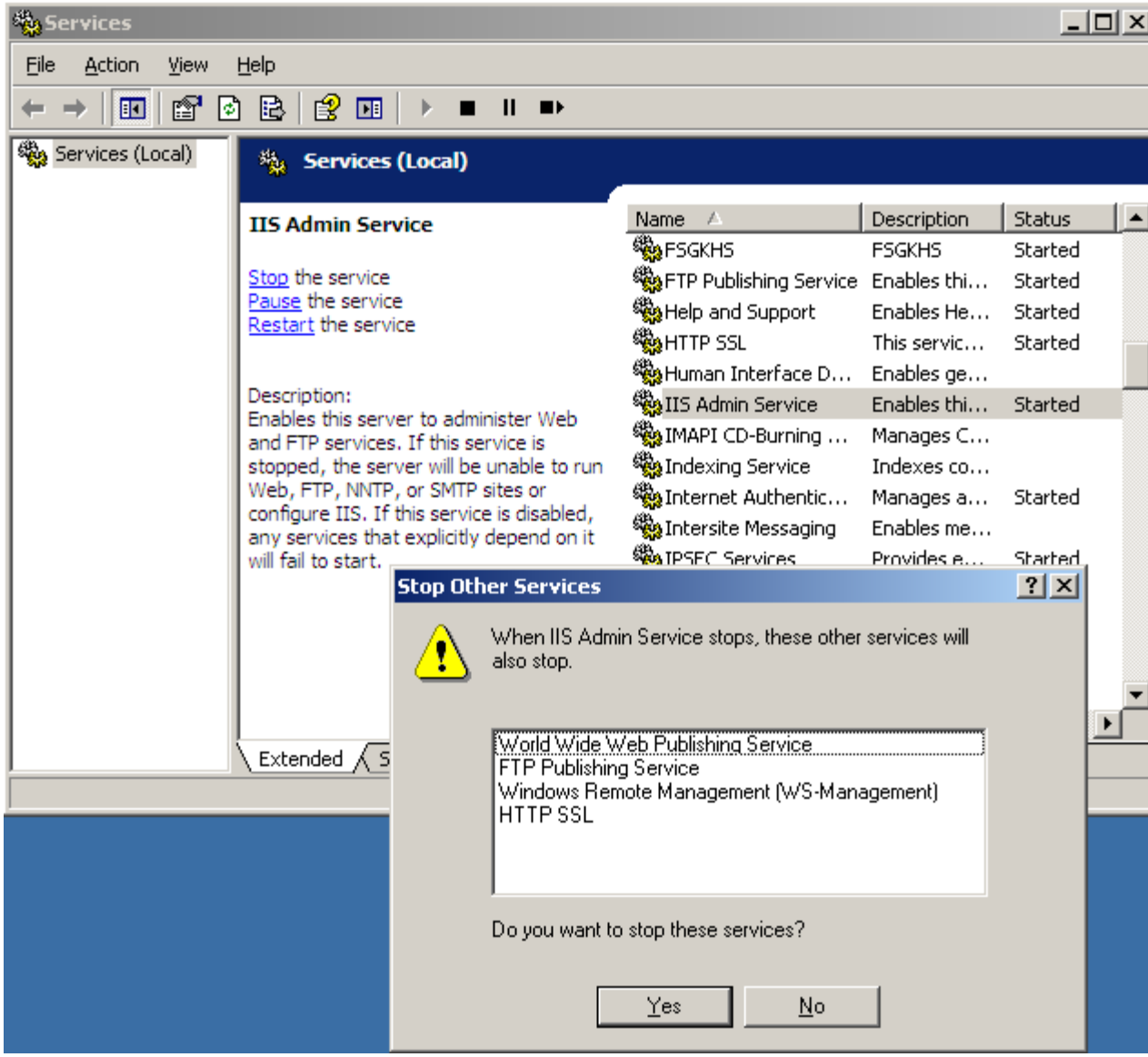
5.5 WCS

Cisco Systemsin WCS (Wireless Control System) on tarkoitettu erittäin laajoihin langattomiin ratkaisuihin, joissa on useita kymmeniä tukiasemia ja useampia kontrollereita ohjaamassa niitä. Ohjelmiston tarkoitus on siis hallita kontrollereita ja näin ollen myös tukiasemia. WCS:llä voidaan myös hallita muita verkon laitteita SNMP:n avulla, kuten: kytkimiä, jos niistä löytyy SNMP-tuki. Tässä työssä on keskitytty vain kontrollerin ja tukiasemien hallintaan. Ohjelmalla pystytään tekemään samat asiat, kuin kontrollerillakin pystytään, mutta ohjelmassa on paljon laajemmin eri ominaisuuksia ja ohjelma on visuaalisempi. WCS:n käyttö tapahtuu selaimella HTTP-protokollalla, yhteys luodaan käyttämällä palvelimen IP-osoitetta.

WCS voidaan ainoastaan asentaa Windows 2003-palvelimelle. Tässä työssä käytetään tietokoneelle asennettua virtuaalista Windows 2003-palvelinta. Ennen ohjelmiston asennusta serverillä pitää pysäyttää IIS admin services palvelu, jolla saadaan vapautettua WCS:lle portteja, kuten: HTTP ja HTTPS:n portit 80 ja 443, sekä muutamia muita portteja. IIS admin services löytyy ajamalla RUN-komento: services.msc, kuten kuvassa 24 on laitettu. Kuvassa 25 on havainnollistettu IIS:n pysäytys.

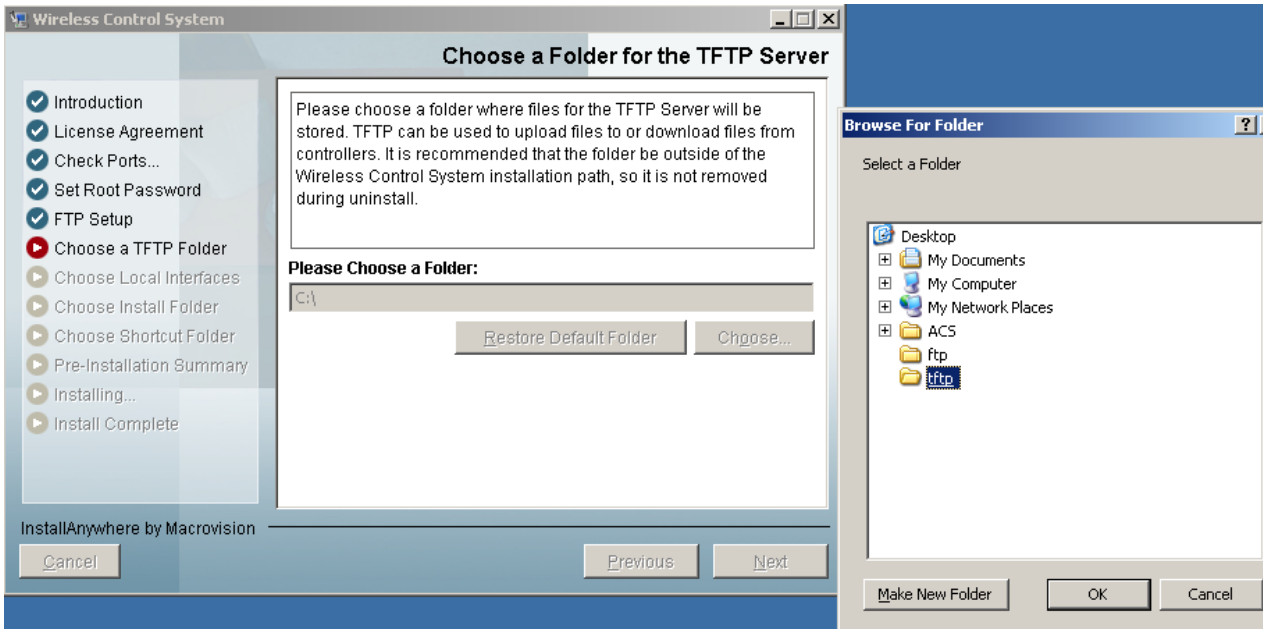


KUVA 24. Palveluiden hakeminen



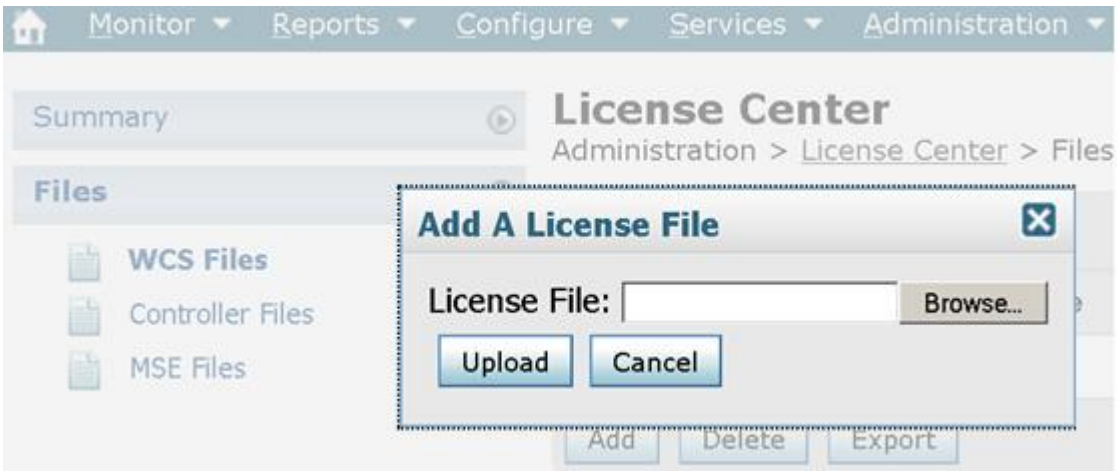
KUVA 25. IIS admin services pysäytys

Asennuksen yhteydessä pitää ohjelmistolle luoda FTP- ja TFTP-palvelimet. Näitä voidaan käyttää esimerkiksi uusien IOS:n lataamiseen tukiasemiin tai kontrolleriin. TFTP-palvelimella voidaan myös siirtää konfiguraatio-tiedosto kontrollerin asetuksista palvelimelle säilöön. FTP- ja TFTP-palvelimia varten WCS kysyy asennusvaiheessa niiden tallennuskansiot kuvan 26 mukaisesti.



KUVA 26. TFTP-palvelimelle luotava kansio

WCS:n asennuksen jälkeen ensimmäisenä ohjelmisto pitää lisensoida, jotta siihen voidaan kytkeä laitteita. Lisenssejä löytyy useita erilaisia, riippuen tukiasemine ja kontrollereiden määristä ja niistä käyttäjä voi valita itselleen sopivan. Lisenssit saadaan hankittua Cisco Systemsin sivuilta, josta lisenssiavain lähetetään sähköpostiin tiedostona ja voidaan lisätä ohjelmaa, kuten kuvassa 27 näkyy.



KUVA 27. WCS:n lisensointi

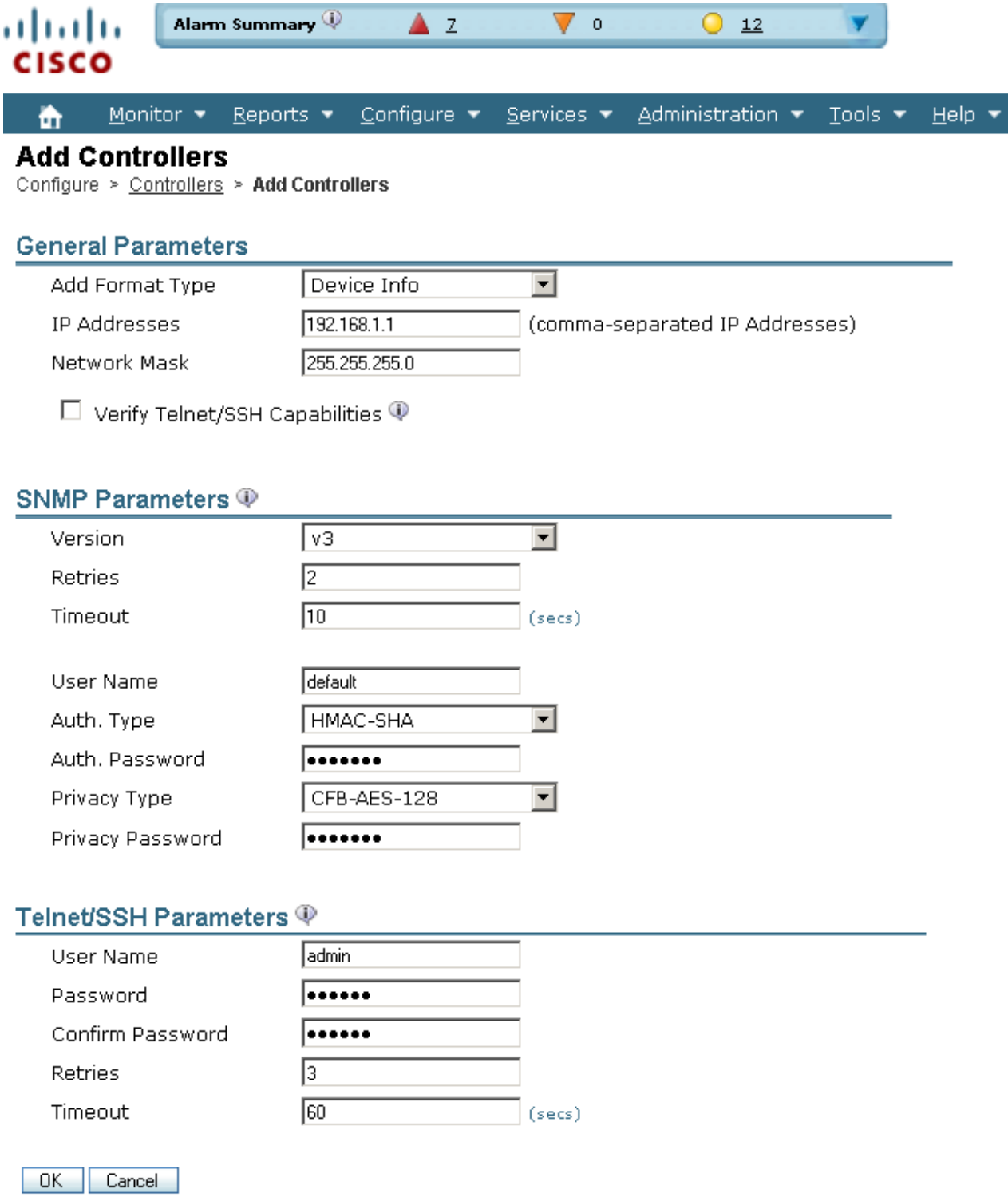
Tässä työssä käytetään 30 päivän kokeilulisenssiä, joka mahdollistaa kontrollerin ja 10 tukiaseman lisäämisen ohjelmaan. Taulukossa 2 on kuvaukset osasta saatavilla olevista lisensseitä.

TAULUKKO 2. WCS:n linsenssit

Lisenssi	**Kuvaus**
Cisco WCS Demonstration License	Ilmainen 30 päivän kokeilu versio 10:lle tukiasemalle
Cisco WCS Base	3 erilaista lisenssiä 50, 100 ja 500 tukiasemaa. Asennus vain yhdelle palvelimelle
Cisco WCS Plus	3 erilaista lisenssiä 50, 100 ja 500 tukiasemaa ja mobiili paikannus. Asennus vain yhdelle palvelimelle
Cisco Enterprise Plus Licenses	4 erilaista lisenssiä 100, 2500, 10000 ja 50000 tukiaemaa. Asennus useammalle palvelimelle. Sisältää myös Cisco WCS Navigator-ohjelman.

5.6 WCS:llä hallinta

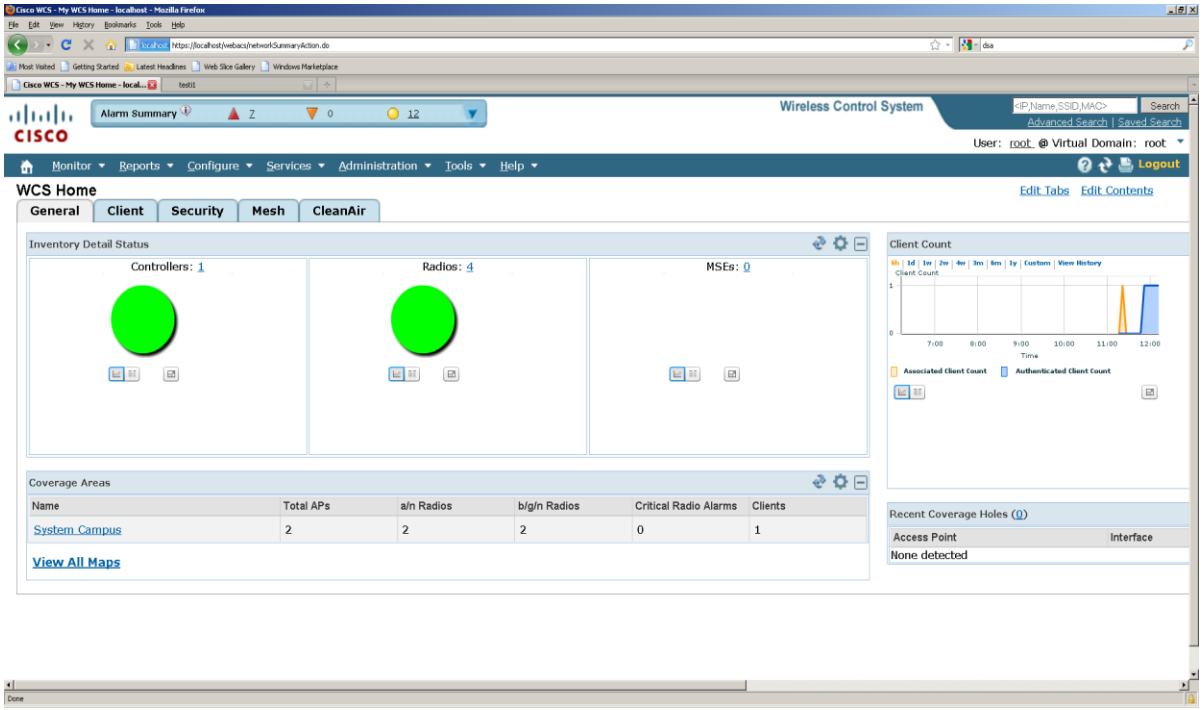
Kontrollerin lisääminen ohjelmaan tapahtuu configure-välilehdeltä kuvassa 28. Lisäämistä varten tarvitaan kontrollein ip-osoite, SNMPv3:n käyttäjätunnus ja autentikointi, sekä privacy salasanat, jotka määriteltiin aiemmin kontrolleriin kuvan 23 mukaisesti. Lisäksi tarvitaan kontrollerin oma käyttäjätunnus ja salasana telnet/ssh kohtaan. Kontrollerin hallinnassa olevat tukiasemat lisätään automaattisesti ohjelmaan.



KUVA 28. Kontrollerin lisääminen WCS-ohjelmaan

Kontrollerin lisäämisen jälkeen se ilmestyy WCS:n home-sivulle, jossa näkyvät myös käytössä olevat tukiasemat. Etusivulta voi tarkastella verkon kokonaisuutta. Kuvassa 29 on WCS:n etusivu, jossa näkyy kontrolleri, tukiasemat ja asiakkaat. Näitä klikkaa-

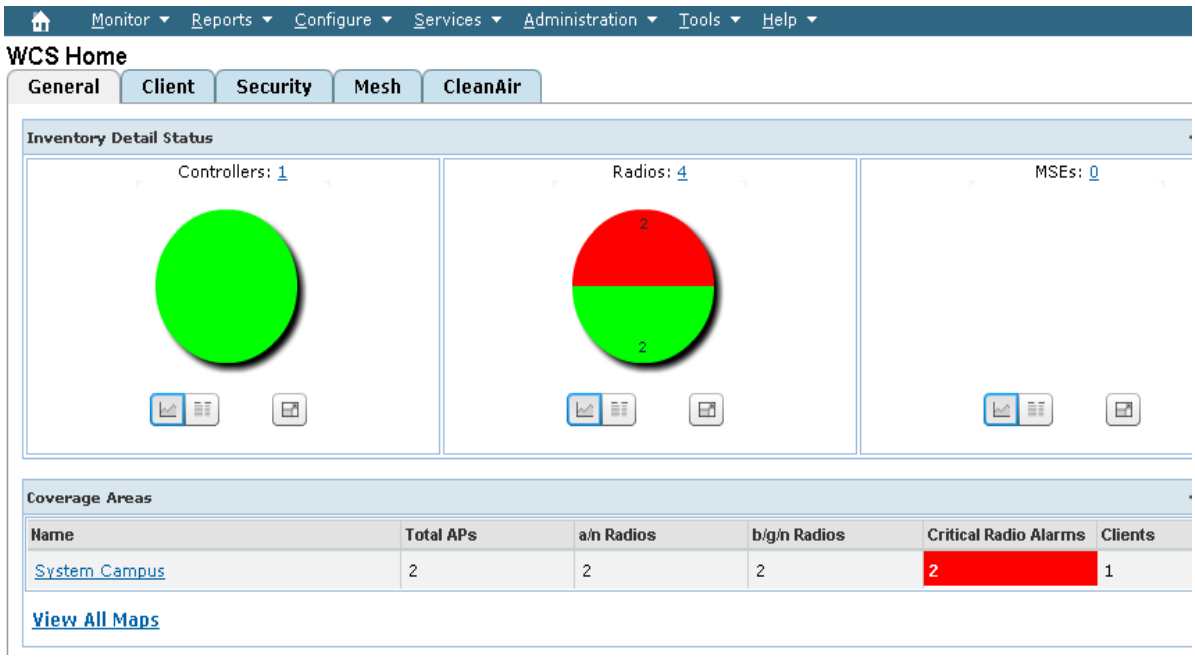
malla päästää tarkastelemaan laitteen tarkempia tietoja ja myös muuttamaan niitä haluttaessa.



KUVA 29. WCS:n etusivu

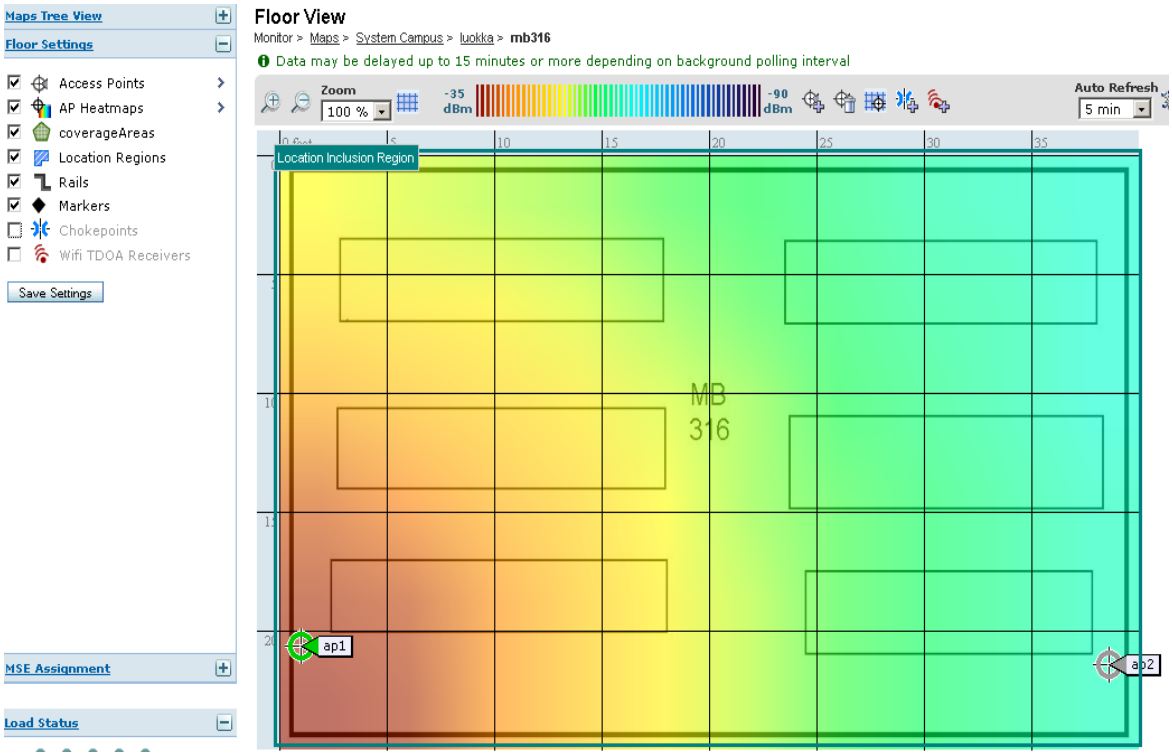
WCS:n tärkeimpiin ominaisuuksiin kuuluu laitteiden asetusten muuttamisen lisäksi erinäisten ongelmatilanteiden ja hälytysten seuranta ja niistä ilmoittaminen hallinnoijalle. Ohjelmaa voidaan muokata ilmoittamaan vain tietyistä halutuista hälytyksistä tai muutoksista käyttäjälle. Ilmoitukset ja hälytykset voidaan varastoida lokitiedostoihin ja tarvittaessa lähettää vaikkapa hallinnoijan sähköpostiin.

Kuvassa 30 etusivulla näkyy hälytys irronneesta RJ-45 kaapelista yhdessä tukiasemista. Vika ilmoitetaan tässä tapauksessa käyttäen SNMP:n trap-sanomaa.



KUVA 30. Hälytys irronneesta kaapelista

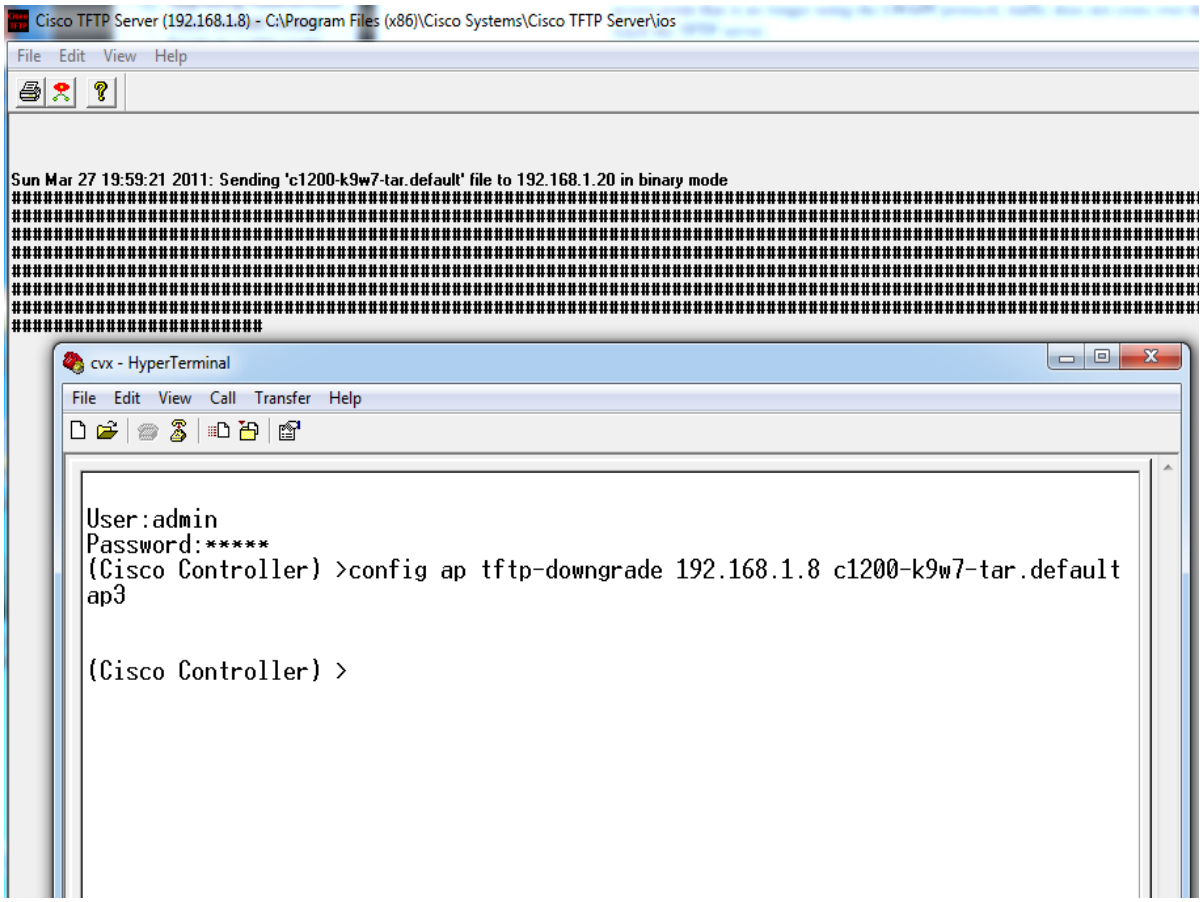
Vika voidaan myös paikantaa käyttämällä karttoja ja pohjapiirustuksia. Hälytykset näkyvät ohjelman kartta-osiossa, jossa hälytystä klikkaamalla ohjelma näyttää käyttäjälle kartalta vikaantuneen tukiaseman. Kuvassa 31 näkyy harmaalla tukiasema ap2, jonka kaapeli on irronnut. Karttoja voidaan myös käyttää tukiasemien yhteyden kantavuuden määrittämiseen.



KUVA 31. Kartalla tukiasema ap2, josta kaapeli on irrotettu

5.7 Tukiaseman IOS:n palautus

Tukiaseman voi palauttaa lightweigt ap:sta takaisin normaaliin autonomous ap muotoon useammalla eri tavalla. Palautus voidaan hoitaa WCS-ohjelmalla tai pelkällä TFTP-palvelimella ja reset-nappulalla. Tässä tapauksessa palautus toteutettiin käyttämällä Ciscon TFTP-palvelinta ja kontrollerin console-yhteyttä. TFTP-palvelimen kansioon pitää lisätä haluttu IOS nimettynä seuraavasti: *c1130-k9w7-tar.default* 1130-sarjan tukiasemia varten ja *c1200-k9w7-tar.default* 1200-sarjan tukiasemiin.
TFTP-palvelin käyttää ip-osoitteenaan samaa osoitetta, joka on koneessa, johon se on asennettu. palautus komento näkyy kuvassa 32, jossa ip-osoite tarkoittaa siis TFTP-palvelinta ja haluttu tukiasema ilmoitetaan sen nimellä esim: ap3.



KUVA 32. IOS:n palautus lightweight-ap muodosta takaisin autonomous-ap muotoon

6 PÄÄTÄNTÖ

Työn tarkoituksena oli rakentaa testiverkko Mikkelin ammattikorkeakoulun laboratorioon ja tutkia verkon keskitettyä hallintaa, käyttäen Cisco Systemsin Wlan-kontrolleria, johon tukiaseman yhdistetään, sekä WCS-ohjelmistoa, jolla voidaan ohjata kontrolleria ja tätä kautta koko verkkoa.

Työn teoriaosuudessa käytiin läpi verkonhallinnan oleellisimmat osa-alueet, erilaiset tavat hallinnoida verkkoja, käytettävissä olevat työkalut sekä hallinta protokollat, joista SNMP oli oleellisensa osana testiverkon hallintaa. Käytännön osuudessa havainnollistettiin miten WLAN-kontrollerin ja WCS-ohjemiston käyttöönotto tapahtuu ja millaisia ominaisuuksia niistä löytyy hallintaa varten.

Työn alkuvaiheessa teoriaosuutta kirjottaessa tarkoituksena oli tutkia myös verkon langallisten laitteiden, kuten reitittimien ja kytkinten hallintaa, mutta työ kasvoi yllättävän suureksi jo pelkästään langattomien laitteiden tutkiskelun osalta testiverkossa. WLAN-kontrolleri, sekä WCS-ohjelmisto sisältävät hyvin paljon erilaisia toiminnallisuuksia, myös kontrollerin ja WCS:n käyttöönotto on aikaa vievää.

WLAN-kontrollerilla ja WCS-ojelmalla mahdollistettiin asetusten muuttaminen niin yksittäisissä tukiasemissa, kuin kokoverkkoa koskevissa asioissa, kuten langattomien verkkojen luomisessa. WCS-ohjelmalla pystyttiin havainnollistamaan ja paikantamaan mahdollisia vikatilanteita verkossa hälytysten muodossa. Nämä asiat ovat hyvin olennaisia verkon keskitetyssä hallinnassa.

WLAN-kontrolleri soveltuu suurempiin yrityksiin, oppilaitoksiin tai organisaatioihin, joissa on käytössä useampia tukiasemia. Kotikäytössä tästä ei juuri ole hyötyä, ohjattaessa vain yhtä tai muutamaa tukiasemaa. WCS-ohjelma taas soveltuu useamman kontrollerin hallintaan ja tätä kautta kymmenien tai satojen tukiasemien ohjaamiseen. Tukiasemien yhdistäminen kontrolleriin ja WCS-ohjelmaan ja näin ollen niiden hallinta vaatii tiettyjä alustustoimien ja työkalujen käyttöä.

Työn tarkoituksena oli demonstroida kuinka yksittäisiä tukiasemia voidaan myös tarvittaessa hallinnoida keskitetysti, sekä miten tämä mahdollistetaan ja tässä tavoitteessa onnistuttiinkin. Keskitetty hallinta voi olla hyvinkin tärkeää monessa yrityksessä, jois-

sa ylläpidetään tietoverkkoja ja tästä työstä voi olla hyötyä etenkin niille, joilla tukiasemien määrä on kasvamassa ja verkonhallinnalle voisi olla tarvetta. Tästä työstä voi olla myös hyötyä itselleni ylläpitotehtäviin suuntautuneissa työtehtävissä tulevaisuudessa.

LÄHTEET

1. Jaakohuhta Hannu. Lähiverkot. Helsinki: Edita Prima Oy. 3 Painos. 2002.

2. Hotti, Mikko. Verkonhallinta. Opinnäytetyö. Lahden ammattikorkeakoulu. PDF-dokumentti. https://publications.theseus.fi/bitstream/handle/10024/11888/2006-11-20-11.pdf?sequence=1. Päivitetty 24.3.2010. Luettu 7.2-15.3.2011.

3. Salokanne, Salla. Verkonhallinta ja verkonhallintajärjestelmä Nagios. Tutkintotyöraportti. Tampereen ammattikorkeakoulu. PDF-dokumentti. https://publications.theseus.fi/bitstream/handle/10024/10100/TMP.objres.68.pdf?sequence=2. Päivitetty 8.3.2010. Luettu 7.2-15.3.2011.

4. Telnet. WWW-dokumentti. http://en.wikipedia.org/wiki/Telnet. Päivitetty. 2.2.2011. Luettu 10.2.2011.

5. Secure shell. WWW-dokumentti. http://en.wikipedia.org/wiki/Secure_Shell. Päivitetty 5.2.2011. Luettu 10.2.2011.

6. Cisco router and security device manager. WWW-dokumentti. http://www.cisco.com/en/US/prod/collateral/routers/ps5318/product_data_sheet0900aecd800fd118.html. Luettu 12.2.2011.

7. Cisco Systems, Inc. Fundamentals of Network Security. Indianapolis, USA: Cisco Press. 2 Painos. 2005.

8. Turunen, Jukka ja Leppälahti, Jarkko. Verkonhallinta. WWW-dokumentti. http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/35/protokollat.shtml. Päivitetty 8.12.2000. Luettu 27.2.2011.

9. Lummevaara, Vesa. SNMP v3 Verkonhallinta & Ciscoworks. Opinnäytetyö. Satakunnan ammattikorkeakoulu. PDF-dokumentti. https://publications.theseus.fi/bitstream/handle/10024/740/Lummevaara%20Vesa.pdf?sequence=1. Päivitetty 1.10.2008. Luettu 15.2-15.3.2011.

10. Kuva MIB:stä. WWW-dokumentti. http://www.oreilly.de/catalog/9780596008406/figs/I_2_tt57-web.png.

11. Stallings William. Data & computer communications. New Jersey, USA: Prentice-Hall Inc. 6 Painos. 2000.

12. Fry Chris ja Nystrom Martin. Security monitoring. O`Reilly Media Inc. 2009.

13. Cisco Systems. Configuring Intrusion detection and prevention. Luento materiaalia. WWW-dokumentti. http://www.scribd.com/doc/26548816/Lecture-11-Configuring-Intrusion-Detection-and-Prevention. Luettu 15.3.2011.

14. Cisco IOS IPS Q&A. WWW-dokumentti. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_qas0900aecd806fc530.html. Luettu 17.3.2011.

15. Sipilä, Matti. Keskitetysti hallittavat WLAN-verkot. Opinnäytetyö. Lahden amattikorkeakoulu. PDF-dokumentti. https://publications.theseus.fi/bitstream/handle/10024/6798/Sipila_Matti.pdf?sequence=1. Päivitetty 26.2.2010. Luettu 15.3.2011.

16. Vehkamaa, Jukka. Yrityksen vierailijaverkon hankinta. Insinöörityö. Metropolian ammattikorkeakoulu Helsinki. PDF-dokumentti. https://publications.theseus.fi/bitstream/handle/10024/2941/Insinoorityo_Jukka_Vehkamaa.pdf?sequence=1. Päivitetty 15.5.2009. Luettu 16.3-25.3.2011.

17. Mäkinen, Iiro. Konserninlaajuisen WLAN-verkon suunnittelu. Insinöörityö. Helsingin ammattikorkeakoulu. PDF-dokumentti. http://www.doria.fi/bitstream/handle/10024/5557/stadia_1159999789_0.pdf?sequence=1. Päivitetty 20.2.2011. Luettu 20.3-25.3.2011.

18. Cisco Systems. Upgrading autonomous Cisco aironet access points to lightweight mode. WWW-dokumentti. http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html. Luettu 15.3-1.4.2011

19. Cisco Systems. LWAPP upgrade tool troubleshoot tips. WWW-dokumentti. http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072d9a1.shtml. Päivitetty 12.8.2009. Luettu 25.3-1.4.2011.

20. Cisco Systems. End-of-Sale and End-of-Life Announcement for the Cisco Router and Security Device Manager. WWW-dokumentti. http://www.cisco.com/en/US/prod/collateral/routers/ps5318/eol_c51-620445.html. Luettu 26.4.2011.