Ciscon WLAN-kontrollerin konfigurointi

Dokumentissa esitetään Ciscon WLAN-kontrollerin konfigurointia. Kuvat on otettu 4402-sarjan kontrollerista joten eri mallin komentoikkunat saattavat näyttää erilaisilta.

Sisältö

Perusasetukset ja IP-osoitteen määrittäminen

Ensimmäisessä vaiheessa kontrollerilla ei ole IP-osoitetta ja konfigurointi on tehtävä komentorivistä Command Line Interface:n (CLI:n) kautta. Kun kontrollerille on asennettu IP-osoite, muut konfiguroinnit voidaan tehdä selaimen avulla web-rajapintaa käyttäen.

Avaa ensin yhteys kontrolleriin joko suoraan sarjakonsolilla tai kytke kontrolleri sarjakonsolipalvelimeen ja käytä sitä. Suorita konfigurointi seuraavasti:

```
Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

System Name [Cisco_b2:e2:83]: <your_system_name>

Enter Administrative User Name (24 characters max): <your_username>

Enter Administrative Password (24 characters max): <your_password>

Re-enter Administrative Password                  : <your_password>


Service Interface IP Address Configuration [none][DHCP]: DHCP


Enable Link Aggregation (LAG) [yes][NO]: NO


Management Interface IP Address: esim. xxx.yyy.zzz.1

Management Interface Netmask: <your_network_mask>

Management Interface Default Router: <your_router's_IP_address>

Management Interface VLAN Identifier (0 = untagged): <0 tai 1>

Management Interface Port Num [1 to 2]: 1

Management Interface DHCP Server IP Address: esim. xxx.yyy.zzz.2


AP Transport Mode [layer2][LAYER3]: <layer2 jos kontrolleri ja tukiasemat
sijaitsevat samassa verkossa, layer3 jos välissä on reititetty verkko>

AP Manager Interface IP Address: esim. xxx.yyy.zzz.3


AP-Manager is on Management subnet, using same values

AP Manager Interface DHCP Server (xxx.yyy.zzz.2):
```

Virtual Gateway IP Address: xxx.yyy.zzz.www

#HUOM: Jos halutaan määritellä web-autentikoitu verkko, tämä IP on oltava #eri alueelta kun kontrollerin muiden rajapintojen IP-osoitteet. Muussa #tapauksessa sisäänkirjautumisessa käytettyä varmennetta ei tule #toimimaan toivotulla tavalla.

Mobility/RF Group Name: <määrittele nimi jos haluat liittää useampia kontrollereita yhteen>

Enable Symmetric Mobility Tunneling [yes][NO]: NO

Network Name (SSID): <test_SSID tai vastaavaa olisi hyvä määritellä tässä vaiheessa>

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no #Suoritetaan myöhemmin

Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: FI

Enable 802.11b Network [YES][no]: no

Enable 802.11a Network [YES][no]: YES

Enable Auto-RF [YES][no]: YES

Configure a NTP server now? [YES][no]: no

Configure the system time now? [YES][no]: no

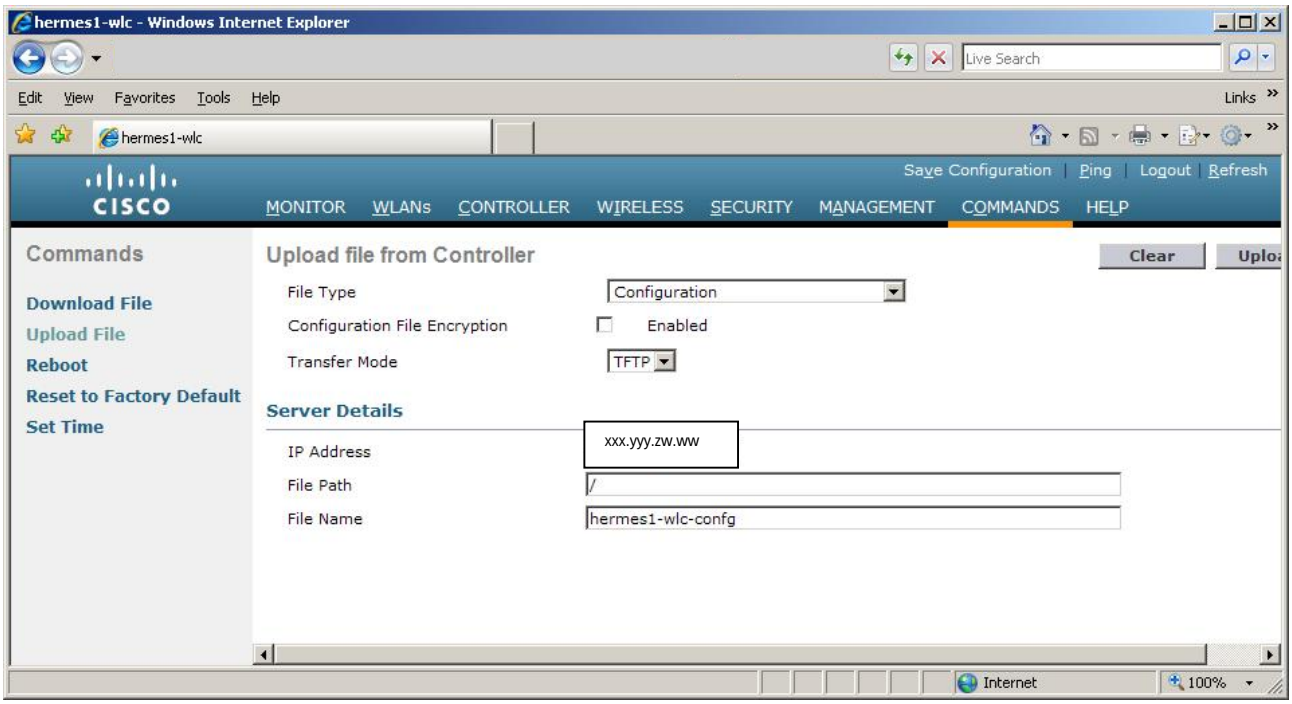
Warning! No AP will come up unless the time is set.

Please see documentation for more details.

```
Configuration correct? If yes, system will save it and reset. [yes][NO]:
yes

#Kun uudelleenkäynnistys on suoritettu määritellään NTP-palvelimet:

(Cisco Controller) >config time ntp server 1 xxx.yyy.z.www

(Cisco Controller) >config time ntp server 2 xxx.yyy.z.wwz
```

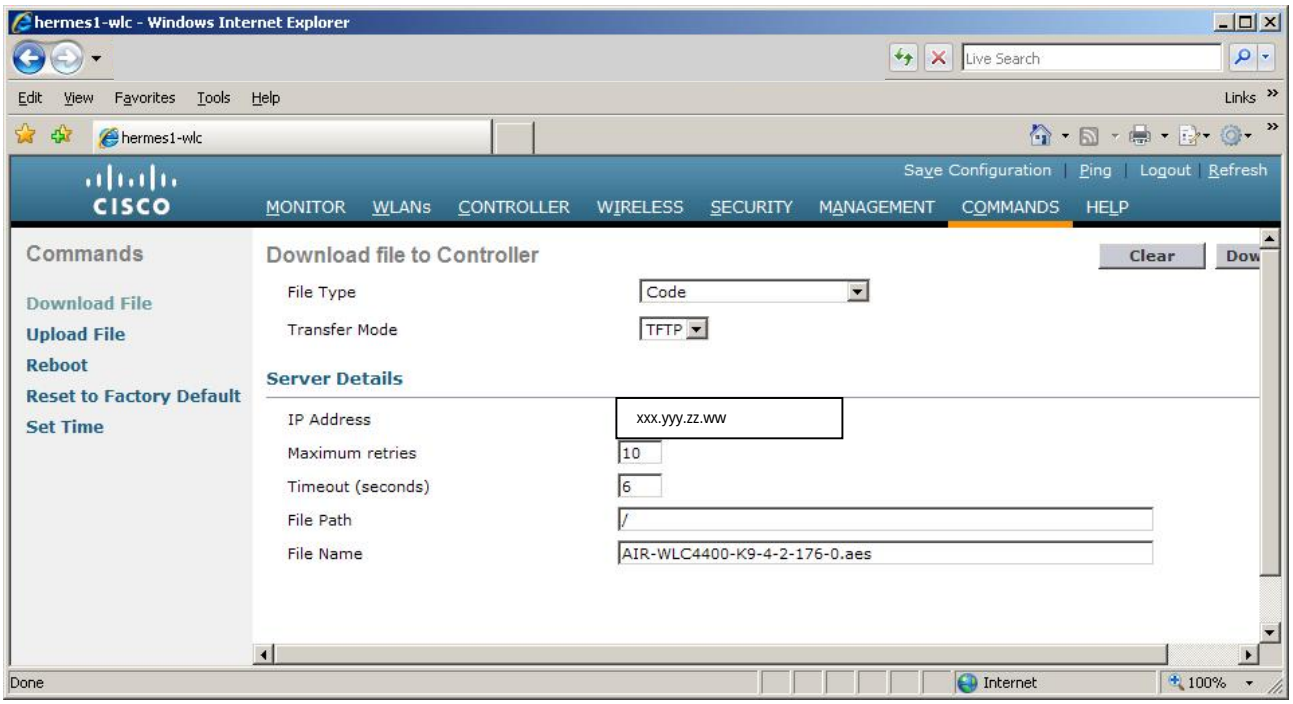
Ohjelmistopäivitys

Seuraavassa vaiheessa on hyvä suorittaa ohjelmistopäivitys. Viimeisin versio ohjelmistosta haetaan Ciscon sivuilta mutta tätä varten tarvitaan siihen oikeuttava käyttäjätunnus. Käytössä oleva ohjelmistoversio on kuitenkin ensin hyvä siirtää talteen TFTP-palvelimelle. Toiminto suoritetaan kuvan 1 mukaisesti.



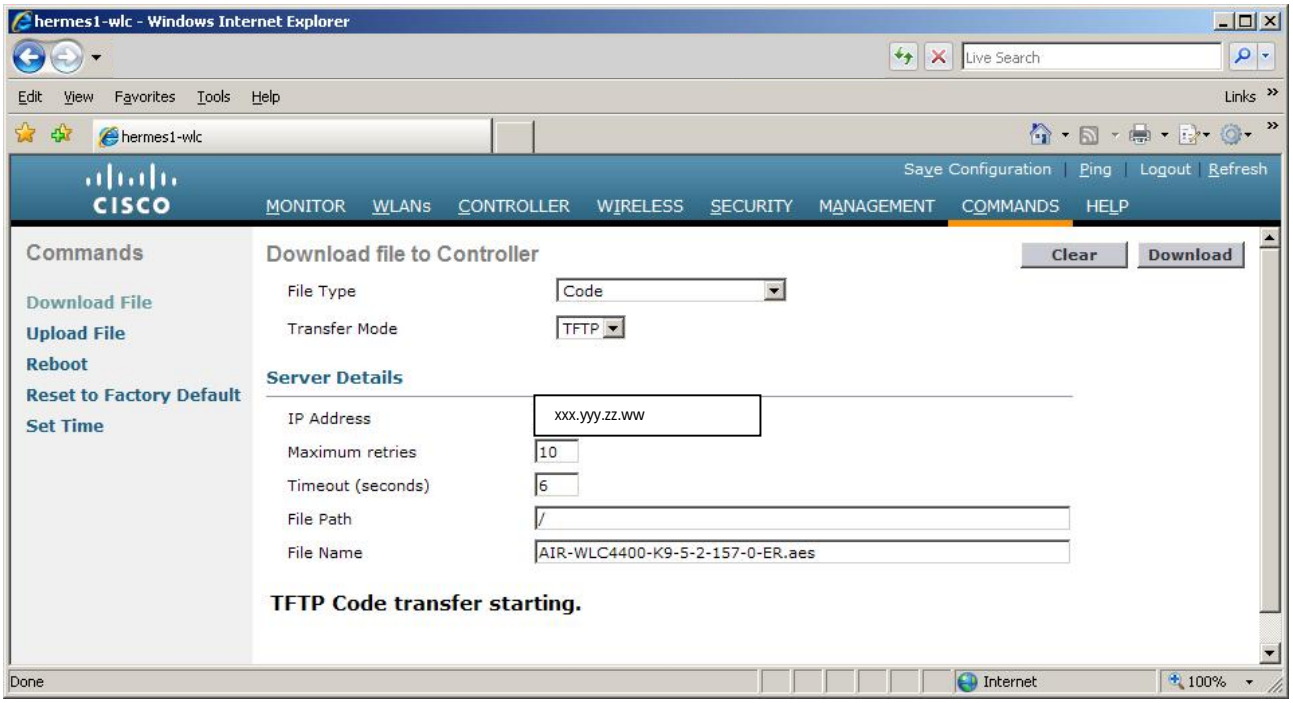
Kuva 1. Käytössä olevan ohjelmistoversion siirtäminen talteen.

Seuraavaksi ladataan uusi ohjelmistoversio TFTP-palvelimelta kontrollerille kuvan 2 mukaisesti.



Kuva 2. Uuden ohjelmistoversion siirtäminen kontrollerille.

Tässä vaiheessa olisi hyvä päivittää myös uusi bootloader kuvan 3 mukaisesti.



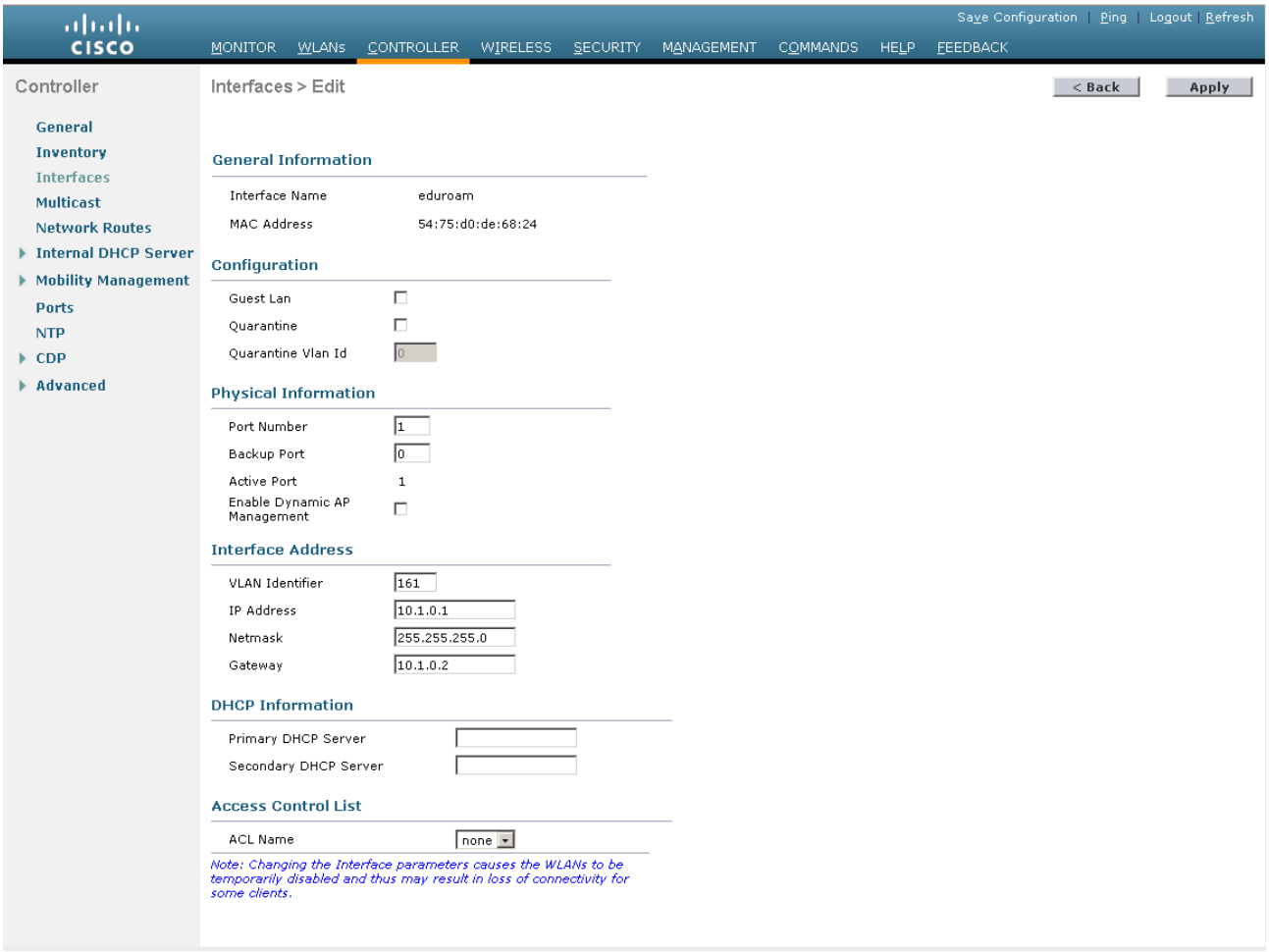
Kuva 3. Uuden bootloader-version siirtäminen kontrollerille.

Bootloader-päivityksen jälkeen varsinainen ohjelmisto olisi hyvä päivittää uudelleen, kuvan 2 mukaisesti.

Virtual LAN:ien (VLAN) huomioonottaminen

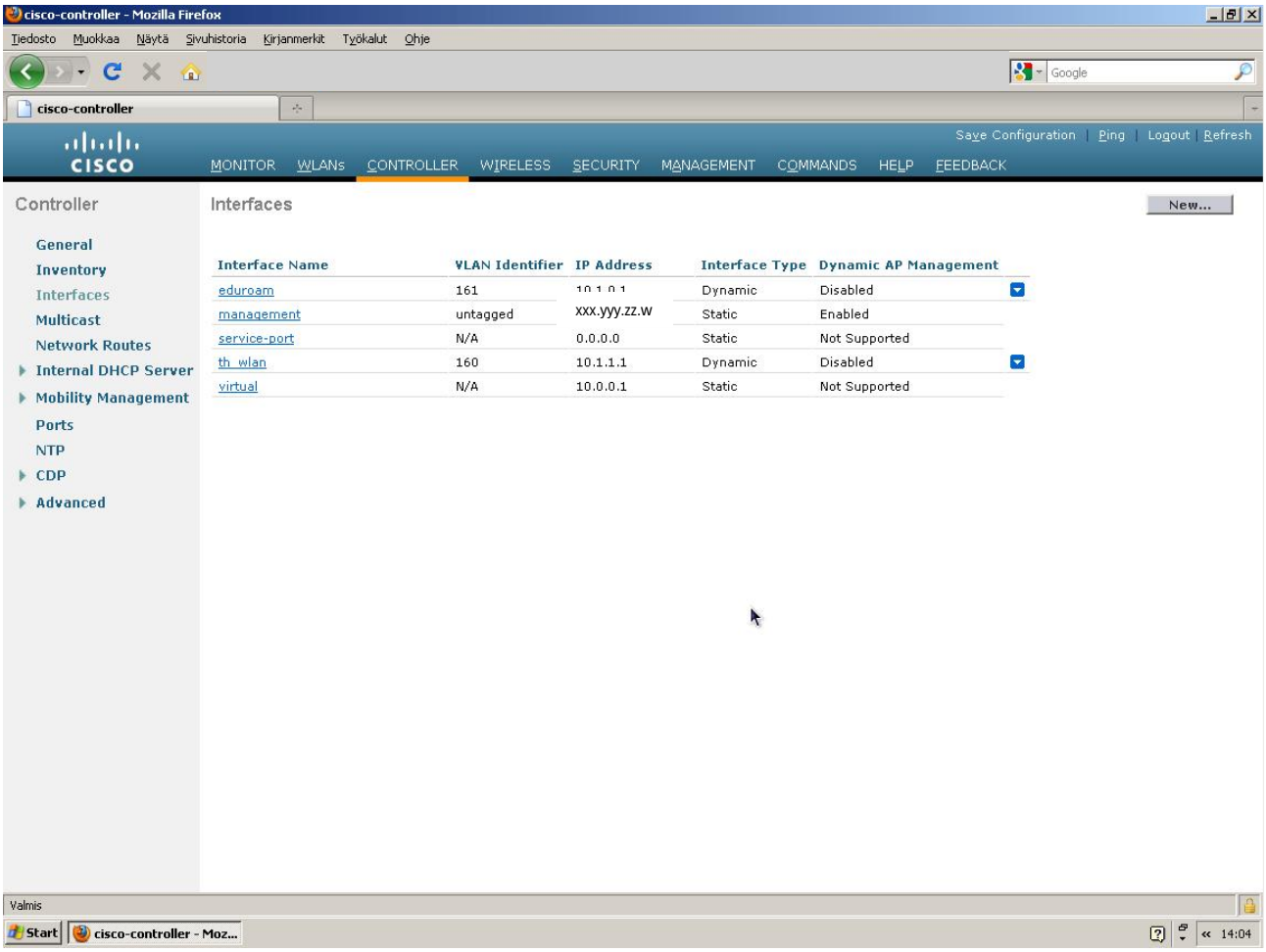
Jos kontrolleri liitetään lähiverkkoon, jossa on käytössä virtual LAN:eja, nämä määritellään myös kontrolleriin. VLANit määritellään lisäämällä kontrolleriin dynaamisia rajapintoja, joihin on määritelty oikeat

tunnisteet. Lisää VLAN-tunniste valitsemalla ensin yläpalkista CONTROLLER ja sivupalkista Interfaces. Paina New...-painiketta, ja määrittele aukeavalle sivulle VLANin tiedot, esim. kuvan 4 näyttämällä tavalla.



Kuva 4. VLAN-tunnisteen määritteleminen.

Paina Apply-painiketta, jolloin tulos on kuvan 5 näköinen.

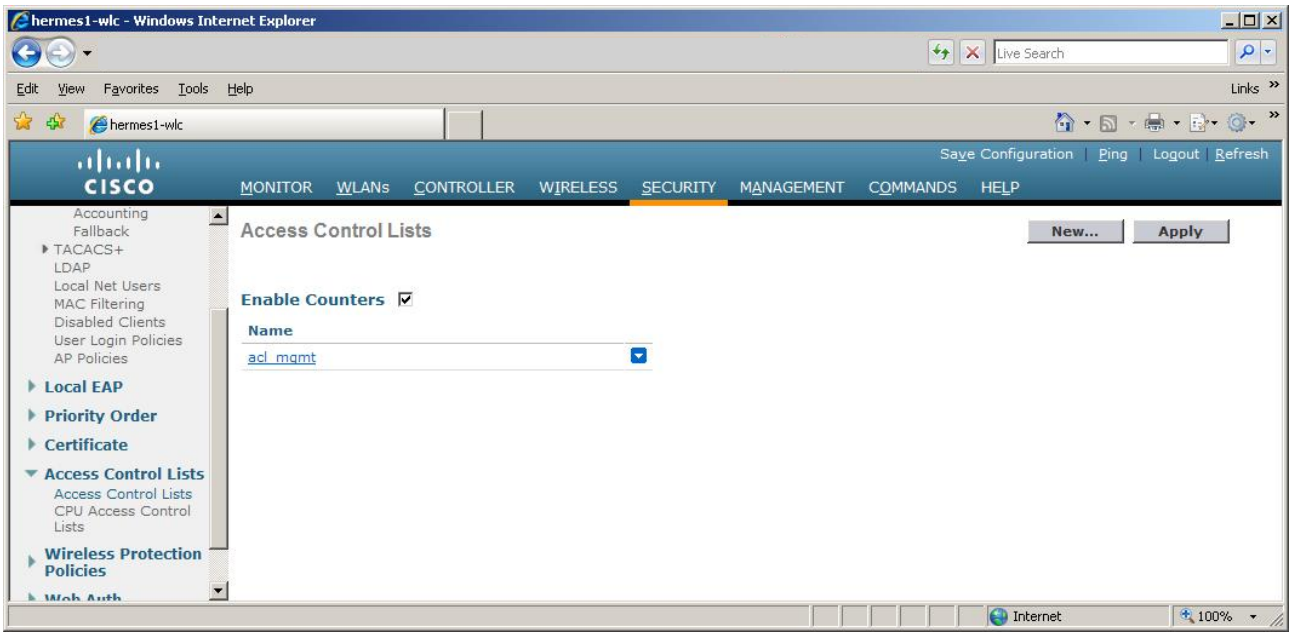


Kuva 5. VLANit 161 (eduroam) ja 160 (th_wlan) lisätty dynaamisina rajapintoina kontrolleriin.

Kun lähiverkossa olevat VLANit on määritelty kontrolleriin, käyttäjä voidaan ohjata oikealle VLANille päivittämällä Access-Accept-pakettiin oikean VLANin tunnisteen. Tämä tehdään kuitenkin vain käyttäjän ollessa kotiorganisaationsa verkossa, eli VLAN-tunnisteita ei lähetetä kampuksen ulkopuolelle. Lisää ohjeita käyttäjien ohjaamisesta oikealle VLANille löytyy FreeRADIUS:en konfigurointiohjeista [3].

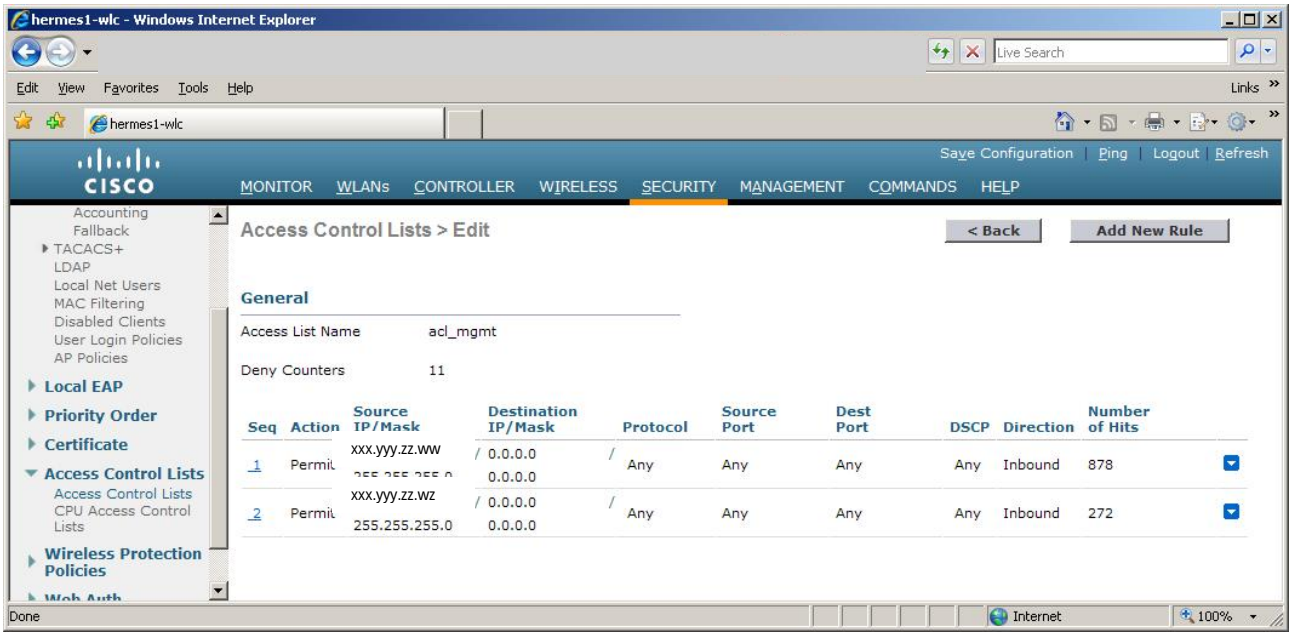
Läpipääsylistan määritteleminen

Access Control List (ACL) on väline jolla estetään luvaton pääsy kontrollerille. Läpipääsylistan määritteleminen aloitetaan valitsemalla yläpalkista SECURITY ja sivupalkista Access Control Lists | Access Control Lists. Luo uusi lista New...-painikkeen avulla, katso kuva 6.



Kuva 6. Läpipääsylistan luomisikkuna.

Avaa seuraavaksi juuri luotu läpipääsylista ja lisää tarvittavat säännöt käyttäen Add New Rule... -painiketta. Esimerkki on esitetty kuvassa 7.

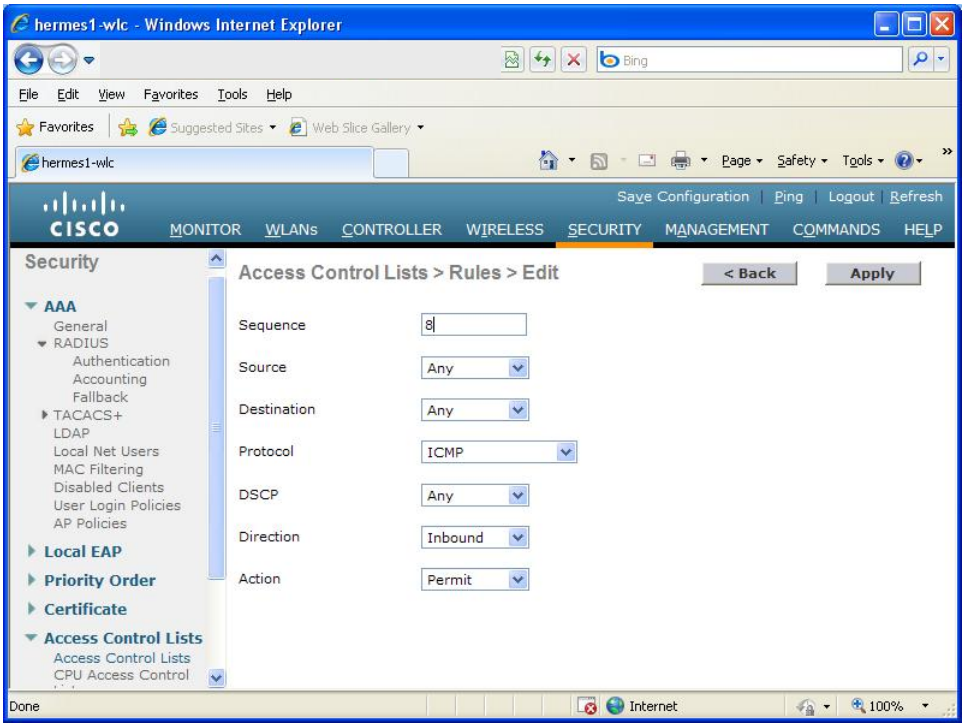


Kuva 7. Läpipääsylistan sääntöjen luomisikkuna.

Läpipääsylistalle tulisi laittaa seuraavat säännöt:

- Verkko/verkot, jo(i)sta ylläpito hoidetaan
- Mahdollisten valvontapalvelinten osoitteet
- Verkko/verkot, jo(i)sta WLAN-klienteille ja tukiasemille annetaan osoitteita
- RADIUS-palvelimen osoite, jonka avulla käyttäjiä autentikoidaan
- Pingiin vastataan aina, katso kuva 8.

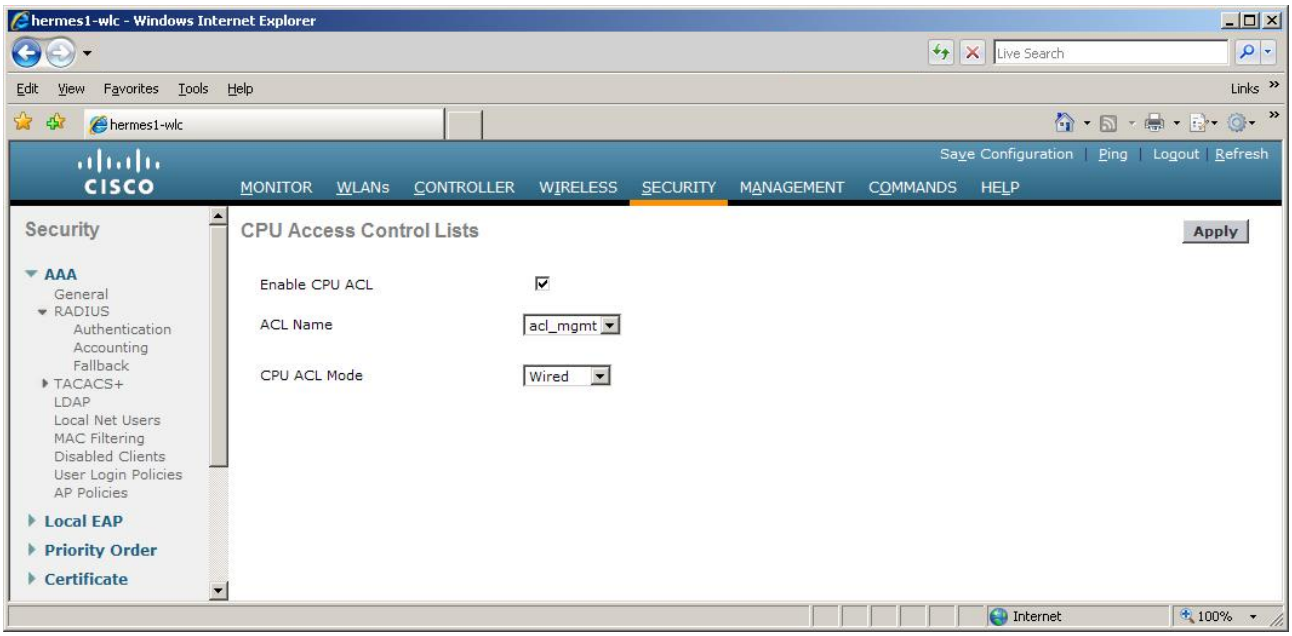
Sääntöjen määrittelemisen yhteydessä Direction-kohdassa on muistettava että Inbound tarkoittaa kontrolleriin suuntaan tulevat paketit ja Outbound tarkoittaa päätelaitteiden suuntaan lähtevät paketit. Ylhäällä esitetyt säännöt tullaan määrittelemään CPU:lle, minkä takia suunta on aina Inbound. CPU:n lähettämille paketeille ei pysty asettamaan rajoituksia.



Kuva 8. Ping-komennolle vastaaminen

HUOM: Parhaat käytännöt –dokumentin ”WLAN-verkon Tietoturva:n”, [1], mukaisesti SMTP-yhteydet on rajoitettava späm-lähetyksien estämiseksi. SMTP-yhteydenotot Internetistä WLAN-verkon käyttäjiin on estettävä ja SMTP-yhteydenotot WLAN-verkon käyttäjistä on rajoitettava niin, että ainoastaan pääsy organisaation omiin SMTP-palvelimiin on sallittu. Nämä rajoitukset voidaan implementoida läpipääsylistojen avulla mutta seuraus on, että WLAN-verkon klienttien yhteyksien nopeudet tippuvat noin 1 Mbps:iin. Tästä syystä suositellaan, että SMTP-yhteydet rajoitetaan muualla, esim. palomuurissa.

Seuraava vaihe on ottaa lista käyttöön CPU:lle ja se tehdään valitsemalla sivupalkista CPU Access Control Lists ja täyttämällä valikot kuvan 9 esittämällä tavalla.

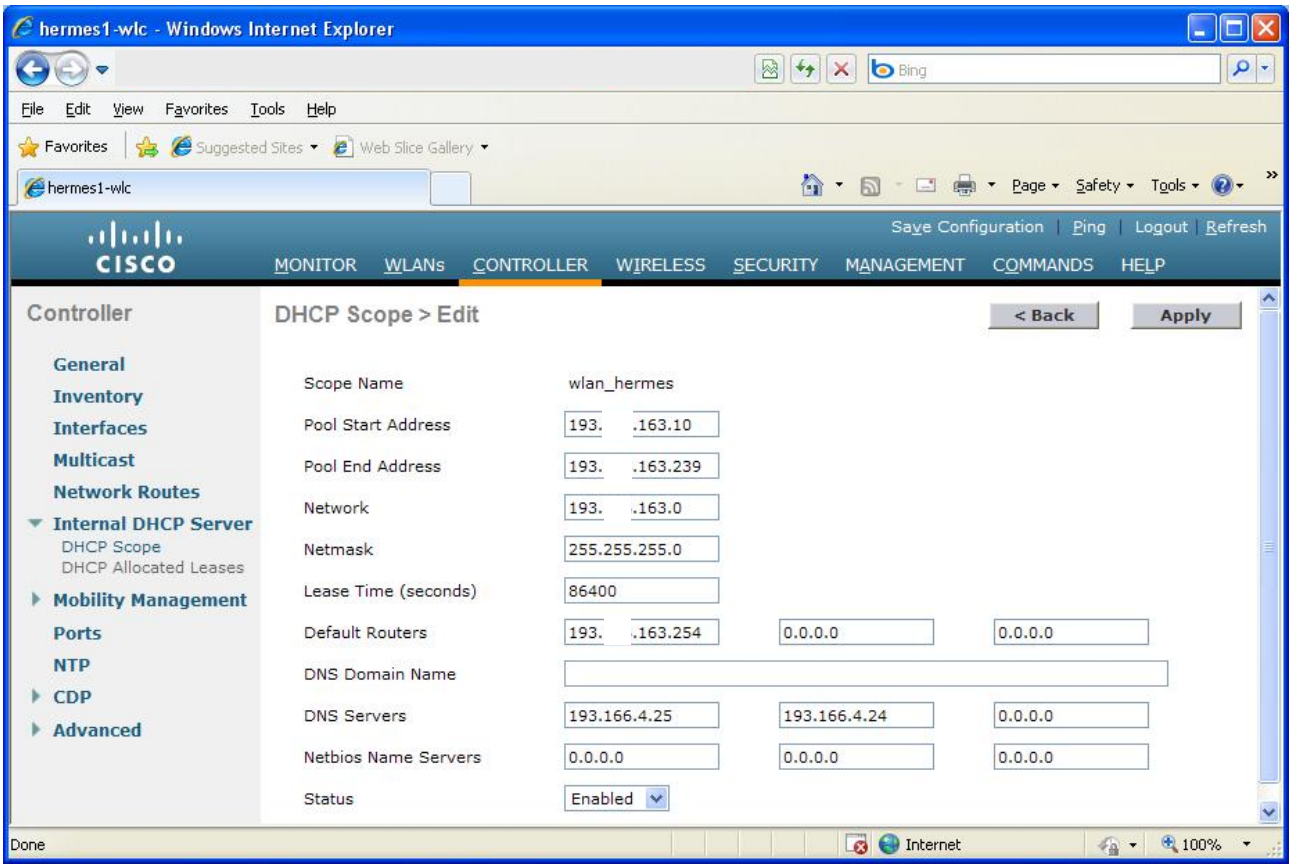


Kuva 9. Läpipääsylistan ottaminen käyttöön.

Sisäisen DHCP-palvelimen konfigurointi (valinnainen)

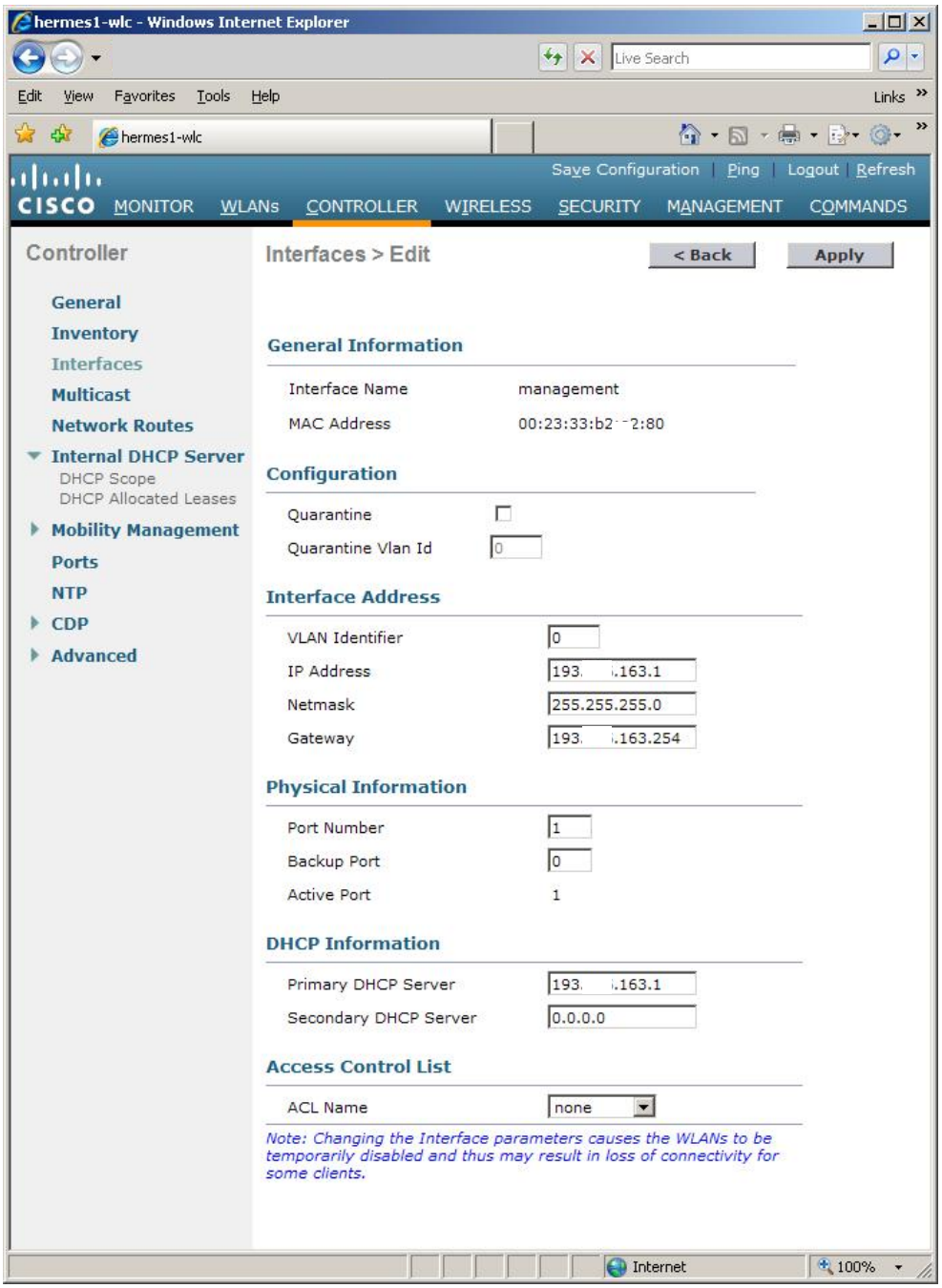
Ciscon kontrolleri pystyy toimimaan DHCP-palvelimena ja tässä tapauksessa palvelemaan tukiasemat ja verkossa olevia WLAN-päätelaitteita. Muita päätelaitteita sisäinen DHCP-palvelin ei pysty palvelemaan. Jos verkossa ei ole DHCP-palvelinta ennestään, sisäistä DHCP-palvelinta voidaan käyttää hyväksi. Toiminto ei kuitenkaan ole kovin kehittynyt ja IP-osoitteen jakaminen voi olla hidasta. Mikäli mahdollista, WLAN-verkolle kannattaa järjestää erillinen DHCP-palvelin.

Sisäistä DHCP-palvelinta pystytään muokkaamaan valitsemalla yläpalkista CONTROLLER ja sivupalkista Internal DHCP Server | DHCP Scope. Esimerkki konfiguroinnista on esitetty kuvassa 10. Verkon IP-osoitteiden alku- ja loppupäästä on hyvä jättää muutama osoite pois, jotta nämä voidaan jakaa kontrollerin eri rajapinnoille sekä mahdollisesti kytkimille ja muille verkkolaitteille.



Kuva 10. Sisäisen DHCP-palvelimen konfigurointi.

Seuraavaksi hallintarajapinnalle määritellään DHCP-palvelin valitsemalla sivupalkista Interfaces -> management ja määrittelemällä Primary DHCP Serverin osoitteeksi sama kun hallintarajapinnan osoite, katso 11.



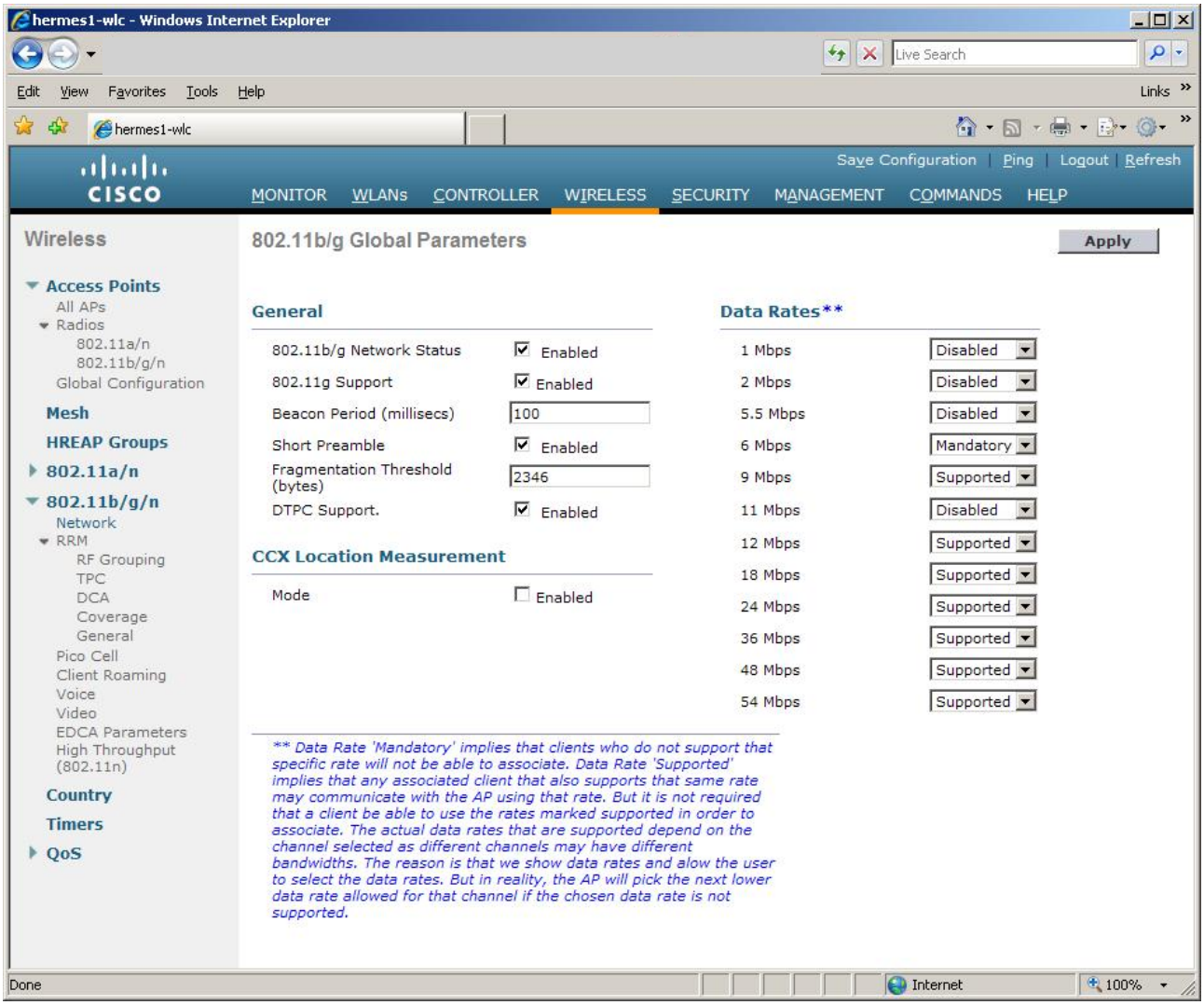
Kuva 11. Sisäisen DHCP-palvelimen ottaminen käyttöön.

IPv6-osoitteita voidaan jakaa reitittimen kautta autoconfiguration-protokollaa käyttäen.

Tukiasemien liittäminen verkkoon ja konfigurointi

Jos tukiasemat liitetään samaan verkkoon kun kontrolleri, ne löytävät automaattisesti kontrollerin ja liittyvät siihen. Muissa tapauksissa kontrollerin IP on löydettävä nimipalvelusta nimellä CISCO-LWAPP-CONTROLLER. Kun tukiasema on kerran löytänyt kontrollerin, sillä on kontrollerin osoite tallessa ja se pystyy liittymään mistä tahansa verkosta, kunhan pääsy verkosta on avattu kontrollerin CPU:lle, katso Läpipääsylistan määritteleminen.

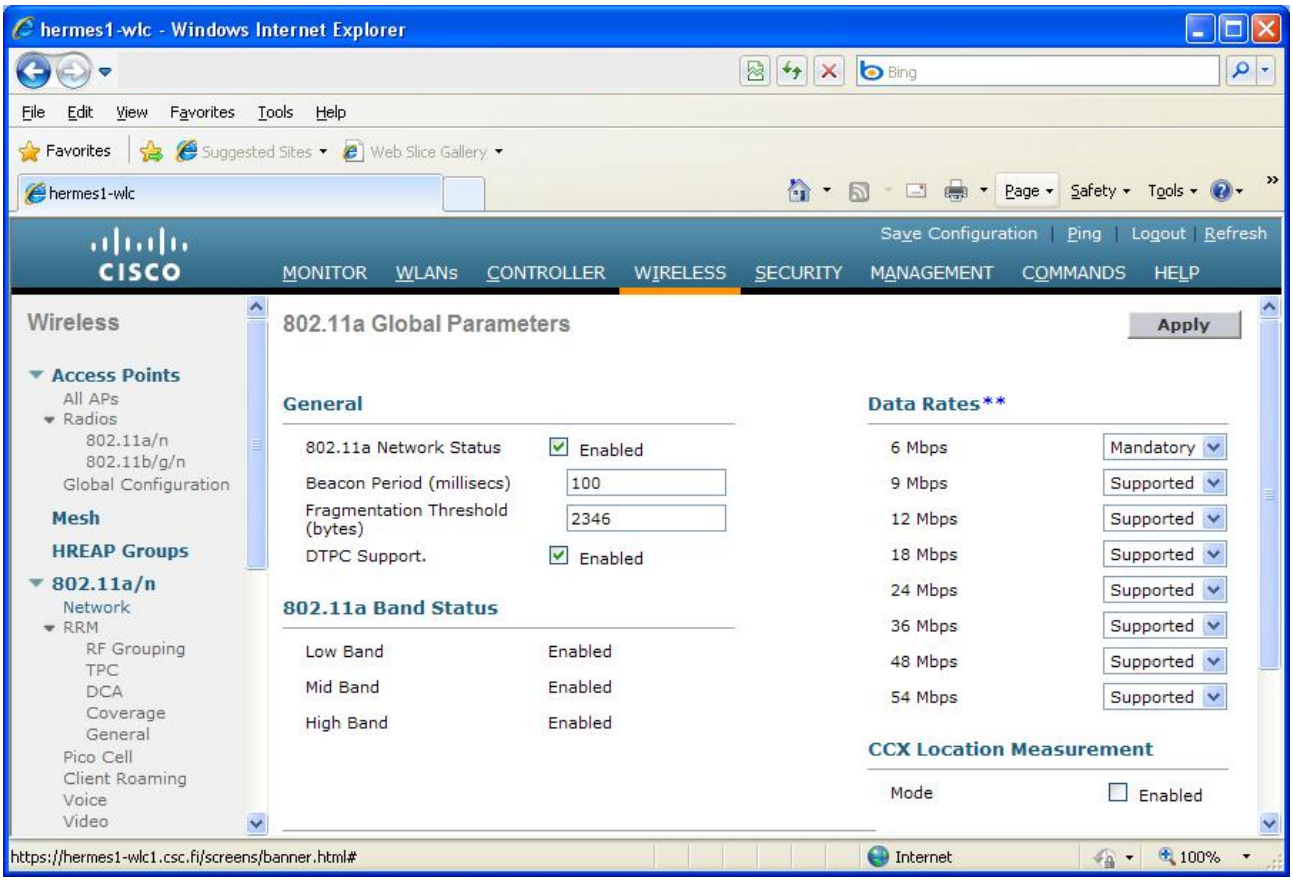
Ciscon tukiasemien oletuskonfigurointi on ainakin muutamissa malleissa sellainen, että 5 GHz:n radiot on oletusarvoisesti päällä. Kun tukiasemat ovat liittyneet verkkoon, muu ilmarajapintaan liittyvä konfigurointi voidaan suorittaa. Siirry ensin määrittelemään 2,4 GHz:n taajuudella toimiva verkko valitsemalla yläpalkista WIRELESS ja sivupalkista 802.11b/g/n | Network. 802.11b-standardin tukeminen alentaa verkon kokonaiskapasiteettia, joten olisi suotavaa tukea 2,4 GHz:n taajuudella ainoastaan 802.11g/n-standardit. Lisätietoja kokonaiskapasiteetin alentamisesta löytyy Parhaat käytännöt-dokumentista ”WLAN-verkon suunnittelu ja rakentamien” [2]. Verkkoon määritellään tukea 802.11g-standardeille kuvassa 12 esitetyllä tavalla.



Kuva 12. Tuen standardille 802.11g määritteleminen verkkoon.

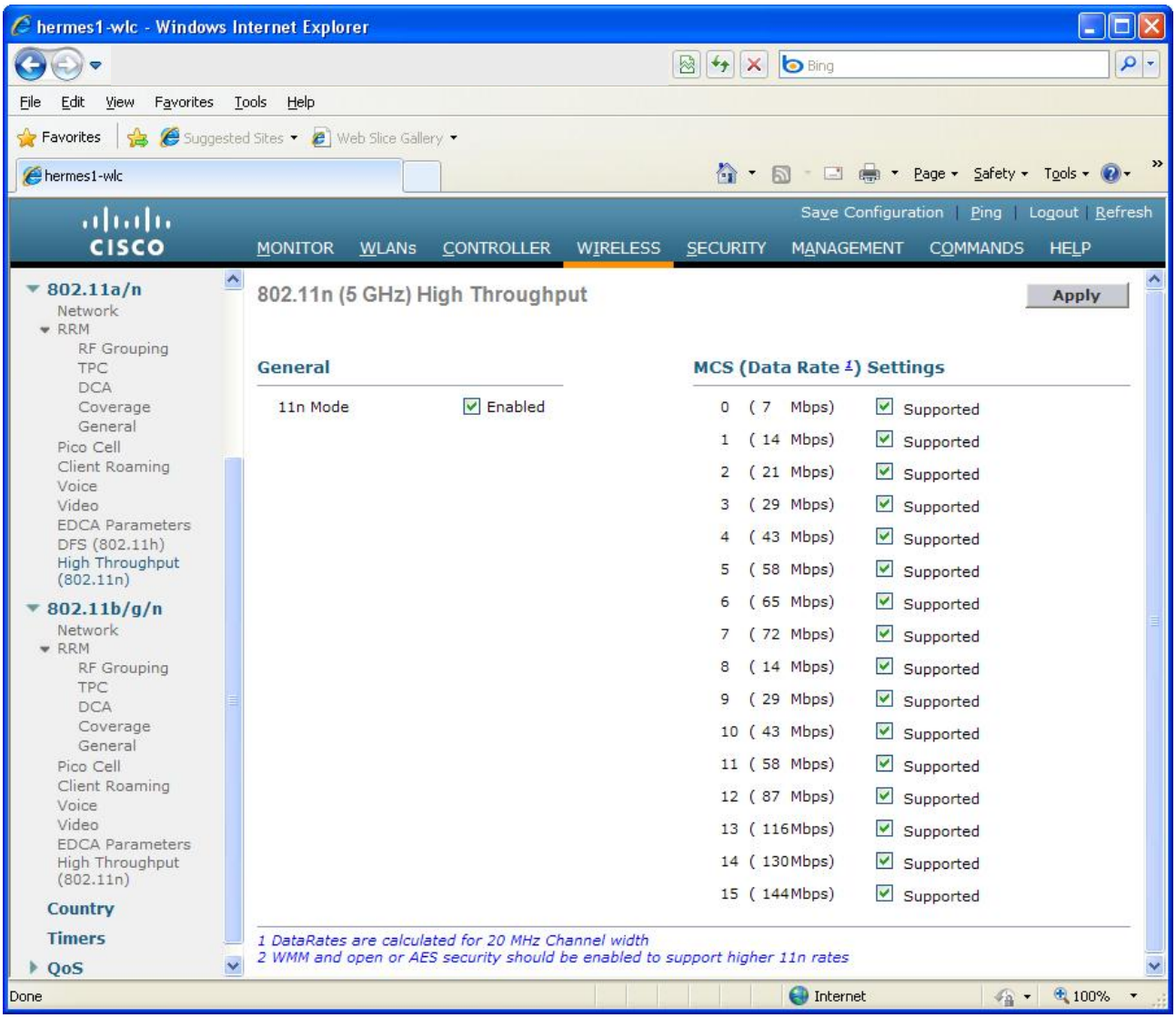
Jos halutaan tukea myös 802.11b-standardia, muutetaan tuetut siirtonopeudet niin että 1 Mbps:n kohdalla lukee *Mandatory* ja muualla *Supported*.

Määrittele seuraavaksi 5 GHz:n taajuudella toimiva 802.11a-standardi kuvan 13 mukaisella tavalla. Siirry määrittelysivulle valitsemalla sivupalkista 802.11a/n | Network.



Kuva 13. Tuen standardille 802.11a määritteleminen verkkoon.

Seuraavaksi määritellään 802.11n-standardille tukea verkossa. Tämä on suoritettava erikseen 2,4 GHz:n taajuudelle ja 5 GHz:n taajuudelle. Voi olla järkevää määritellä tukea 802.11n-standardille vain 5 GHz:lla, katso BPD ”WLAN-verkon suunnittelu ja rakentaminen” [2]. Avaa määrittelysivut sivupalkista valitsemalla ensin 802.11a/n | High throughput (802.11n) ja valinnaisesti sen jälkeen 802.11b/g/n | High throughput (802.11n) ja täytä kuvan 14 esittämällä tavalla.

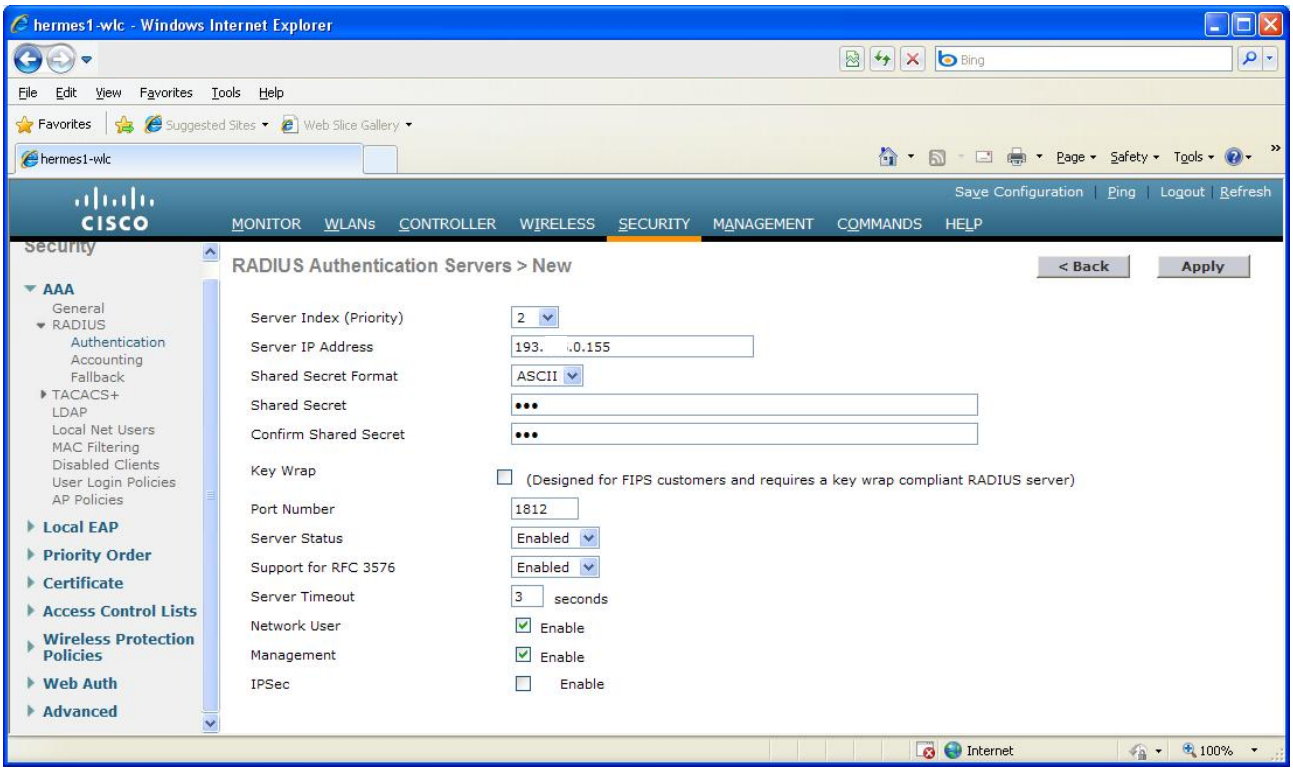


Kuva 14. Tuen standardille 802.11n määritteleminen verkkoon.

HUOM: Myös langattoman verkon ominaisuudet on määrittävä ennen kuin verkkoon voidaan liittyä. Tästä enemmän luvussa Langattoman verkon määrittäminen.

RADIUS-palvelimen määrittäminen

Ulkoinen RADIUS-palvelin siirrytään määrittelemään valitsemalla yläpalkista SECURITY ja sivupalkista AAA | RADIUS | Authentication. Määrittele palvelin kuvassa 15 esittämällä tavalla. Kuvasta poiketen Server Index (Priority) on ensimmäiselle palvelimelle 1.

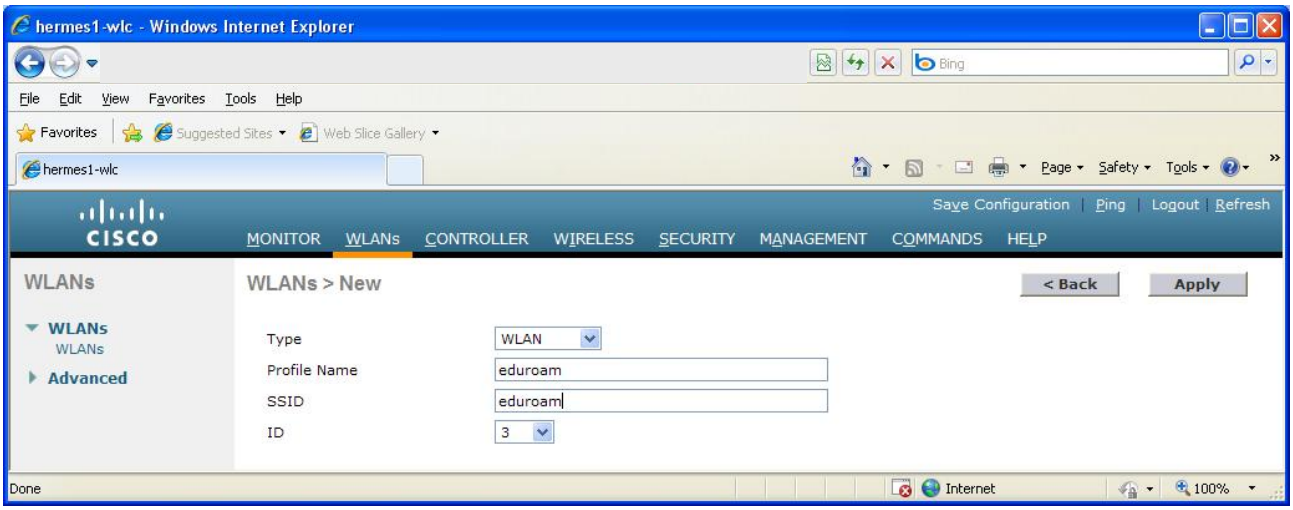


Kuva 15. Radius-palvelimen määritteleminen.

Määrittele tarvittaessa myös accounting-palvelin (sivupalkista Accounting) ja/tai muita RADIUS-palvelimia.

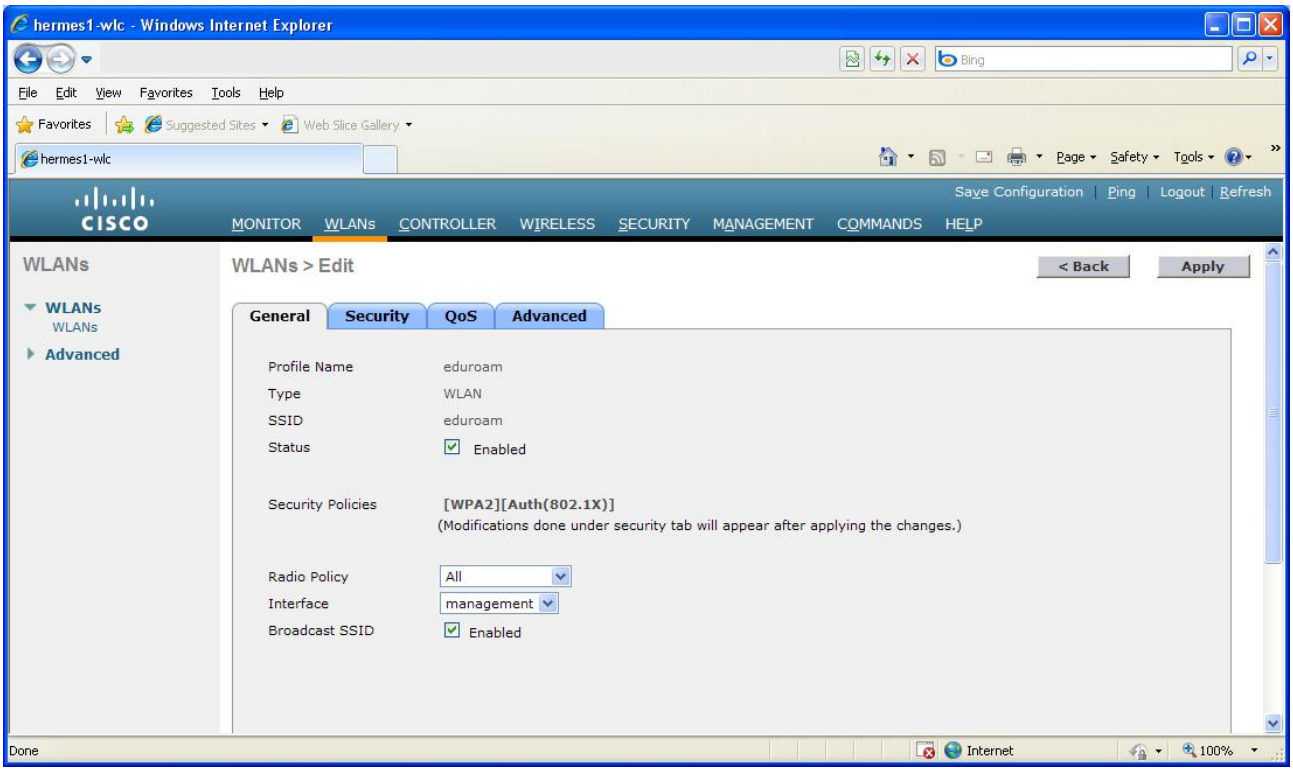
Langattoman verkon määrittäminen

Avaa yläpalkista WLANs ja sivupalkista WLANs | WLANs. Valitse Create New... ja määrittele verkko. Kuvassa 16 on esitetty eduroam-verkon määrittely. Paina lopuksi Apply-painiketta.



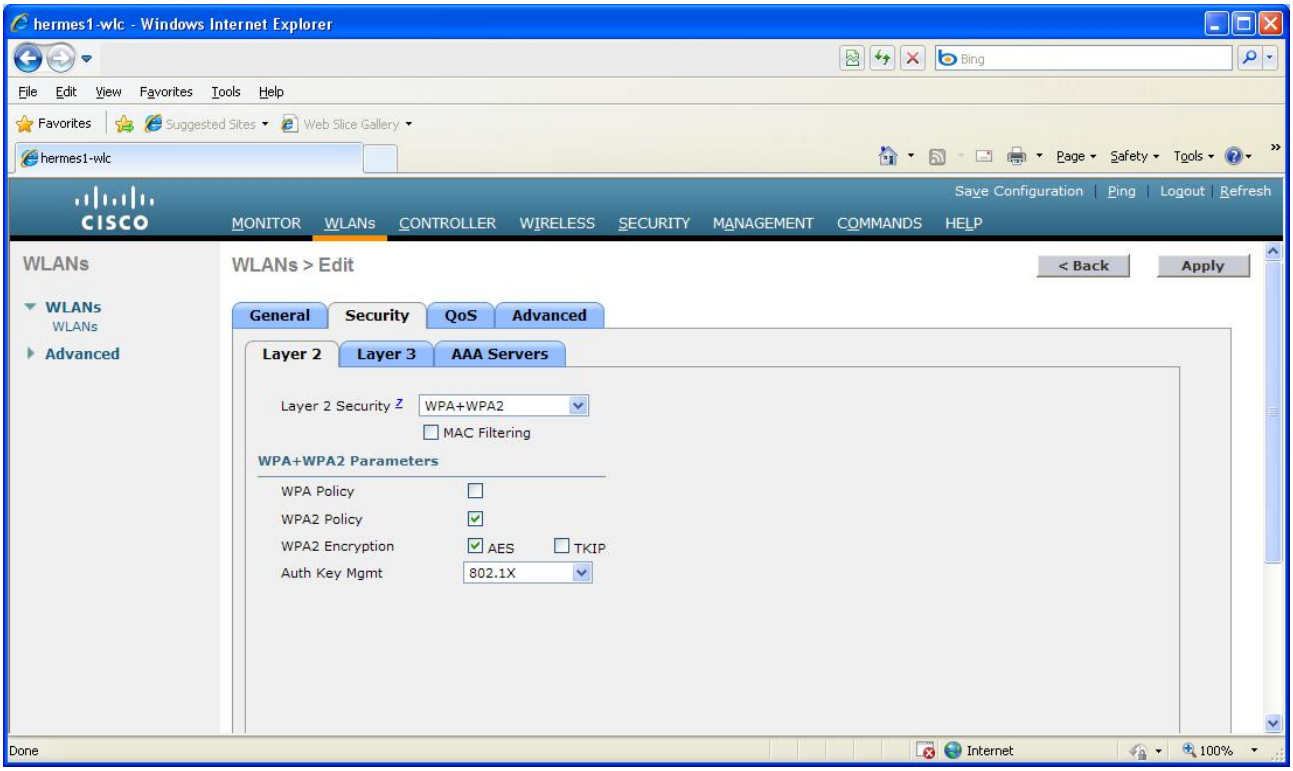
Kuva 16. eduroam-verkon määritteleminen.

Seuraavaksi määritellään verkon yleiset asetukset ja eduroam on esitetty esimerkkinä kuvassa 17. Jos halutaan välittää määritetyn verkon liikennettä tietyllä VLAN:illa kiinteässä lähiverkossa, valitaan Interface-kohdasta oikea dynaaminen liitäntä. Tämä edellyttää, että dynaaminen liitäntä on ensin määritetty CONTROLLER - Interfaces kohdassa.



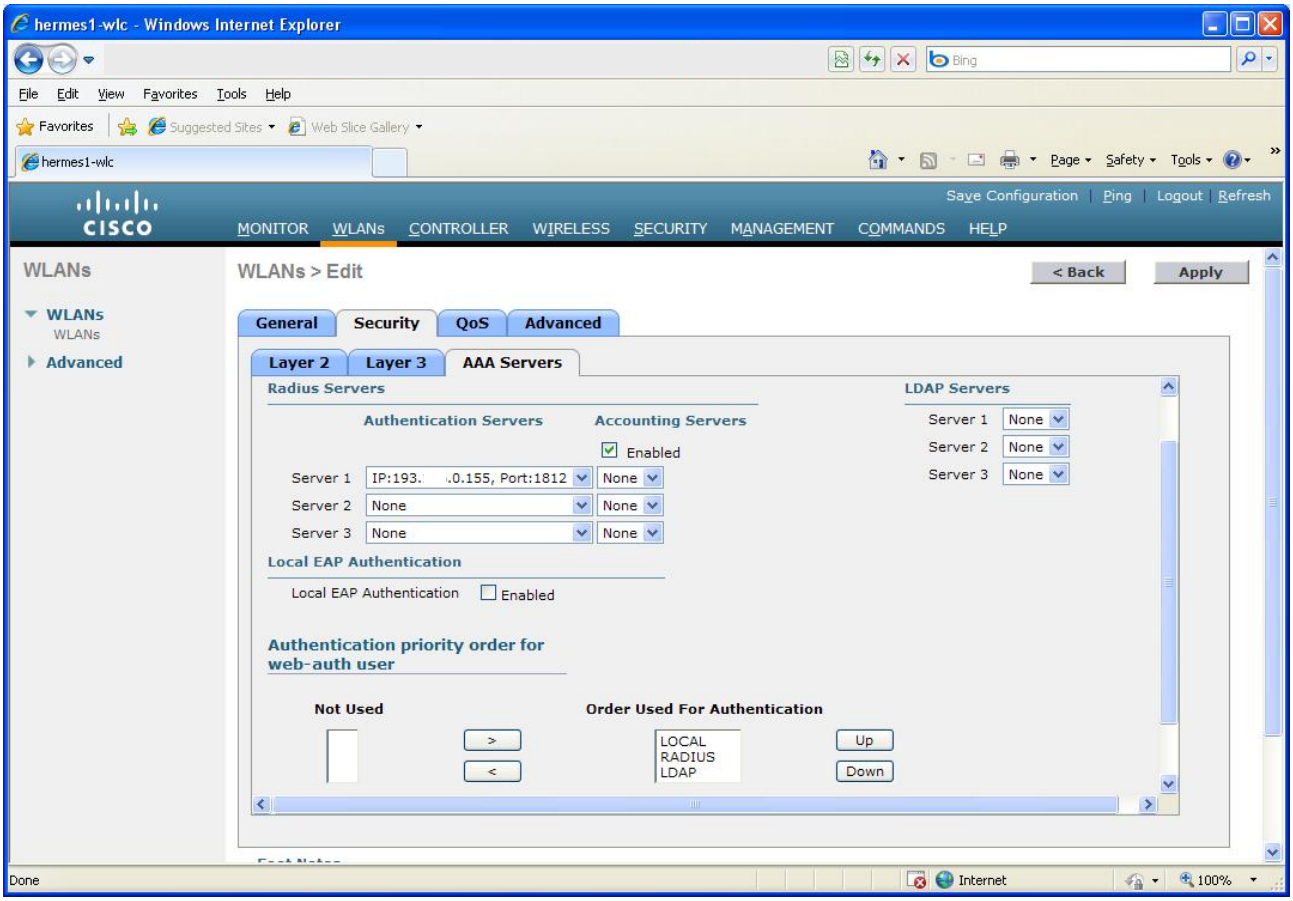
Kuva 17. eduroam-verkon yleiset asetukset.

Määrittele seuraavaksi turva-asetukset valitsemalla Security-välilehteä. eduroam-verkko, missä on käytössä ainoastaan WPA2-AES, on esitetty esimerkkinä kuvassa 18.



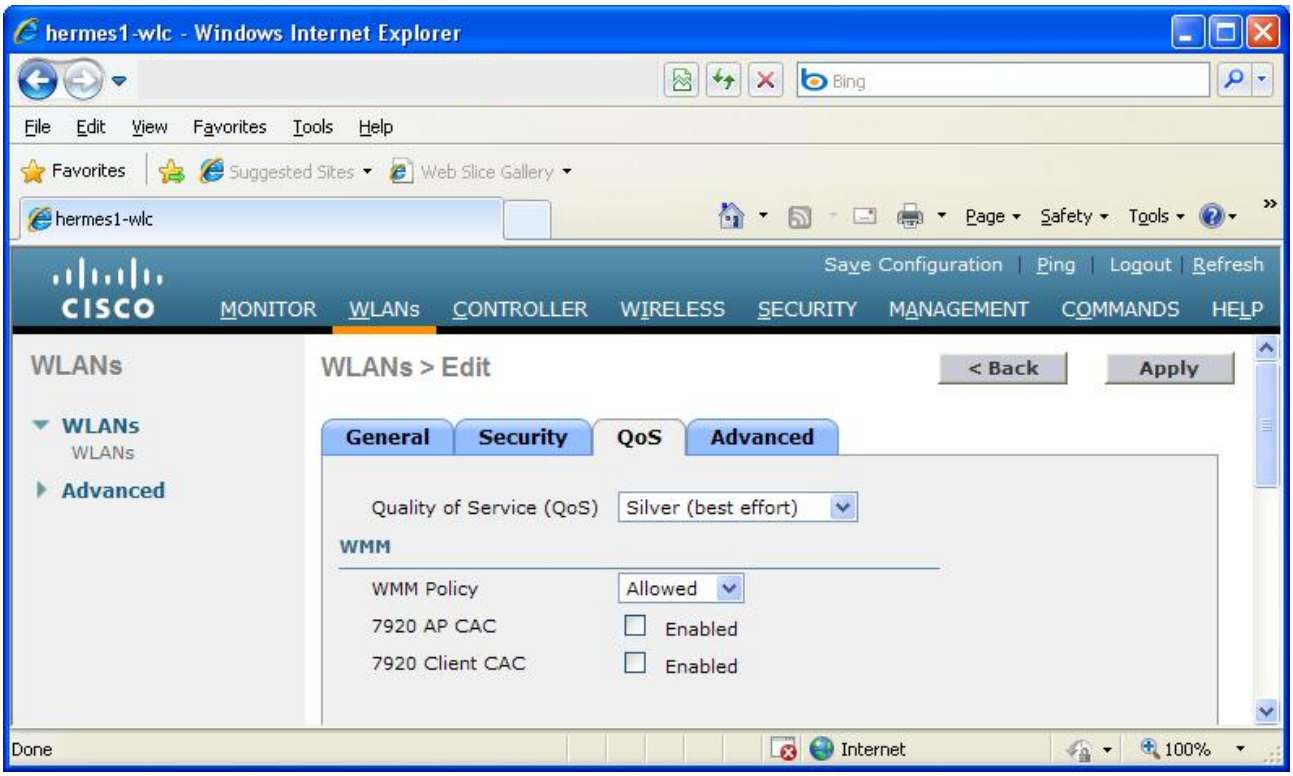
Kuva 18. eduroam-verkon turva-asetukset.

Siirry seuraavaksi AAA Servers –välilehteen ja valitse määritelty/määritellyt RADIUS-palvelin/palvelimet. Kuvassa 19 on esitetty esimerkki.



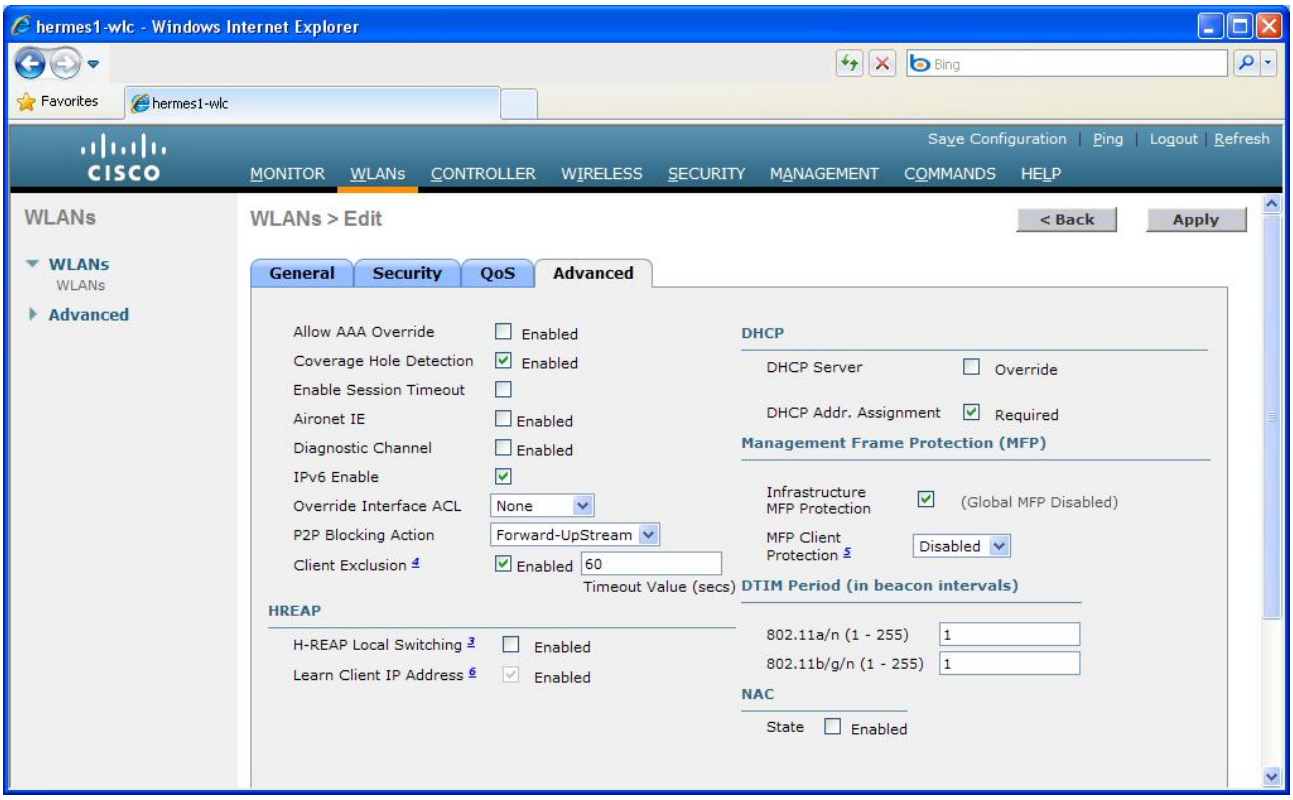
Kuva 19. RADIUS-palvelimen liittäminen tietyn verkon pääsyhallintaan.

Valitse seuraavaksi QoS välilehteä ja varmista että WMM Policy:lle on valittu joko Allowed tai Required. Muissa tapauksissa 802.11n-standardin nopeudet eivät ole tuettu verkossa. Kuvassa 20 on esitetty esimerkki.



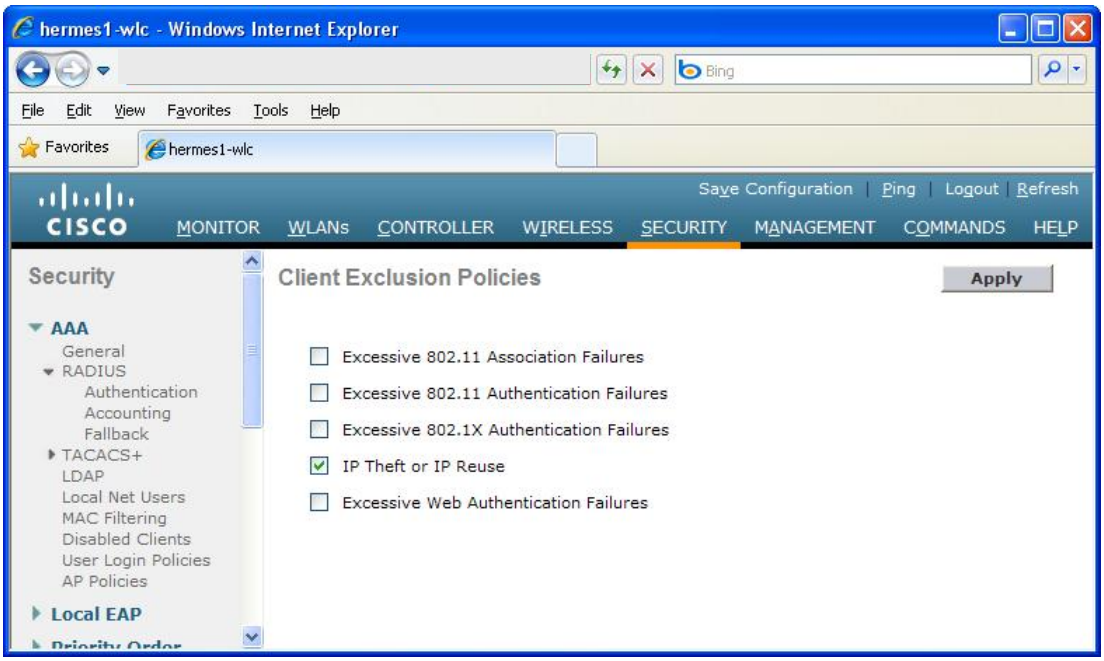
Kuva 20. Verkon QoS-asetukset.

Paina seuraavaksi Advanced-välilehteä ja muokkaa asetukset kuvan 21 mukaisiksi. Muuttamalla P2P Blocking Action-parametrin arvoksi Forward-UpStream:ksi estetään suoraa liikennöintiä verkossa olevien WLAN-klienttien välillä, BPD:n ”WLAN-verkon tietoturva”, [1], mukaisesti. MFP Client Protection on aiheuttanut ongelmia ja kytketään pois. Paina lopuksi Apply-painiketta verkon asetusten tallentamiseksi. HUOM! Jos verkossa on käytössä VLAN:eja, aseta myös ”Allow AAA Override” päälle.



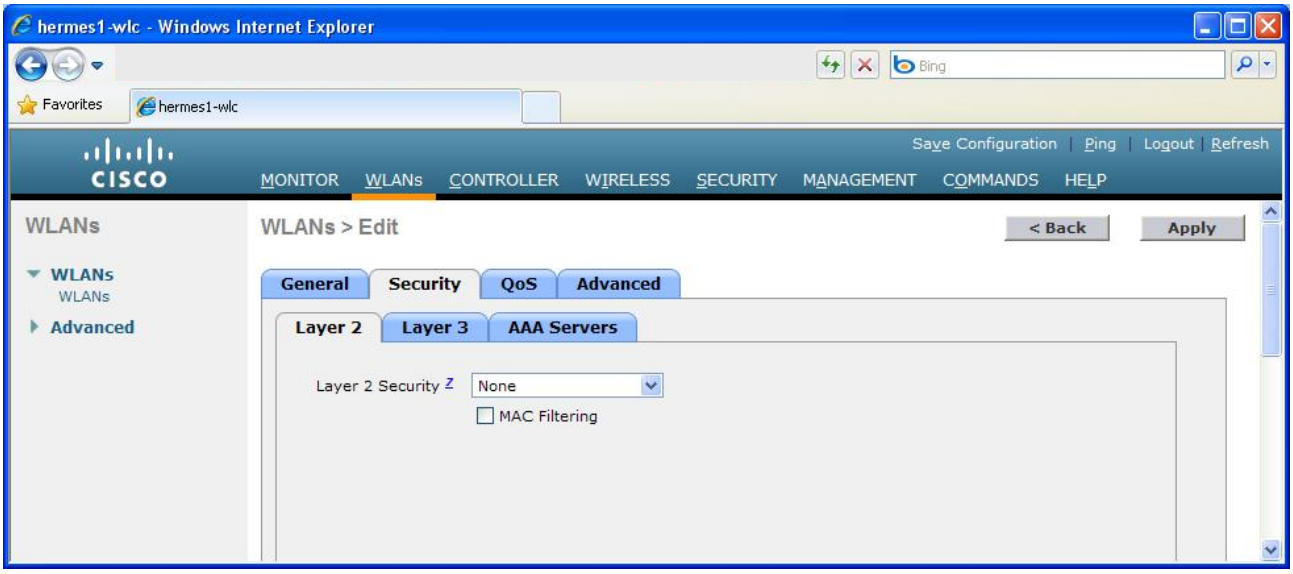
Kuva 21. Verkon muut asetukset.

Kuvan 21 kohdassa Client Exclusion-arvoksi on määritelty 60s. Client Exclusion on oletusarvoisesti määritelty hieman liian tiukasti, joten siirrytään tässä välissä muokaamaan asetukset valitsemalla yläpalkista SECURITY ja sivupalkista Wireless Protection Policies | Client Exclusion Policies. Poistetaan ruksit muista kohdista kuin ”IP Theft or IP Reuse” kuvan 22 mukaisesti. Painetaan tämän jälkeen Apply-painiketta.

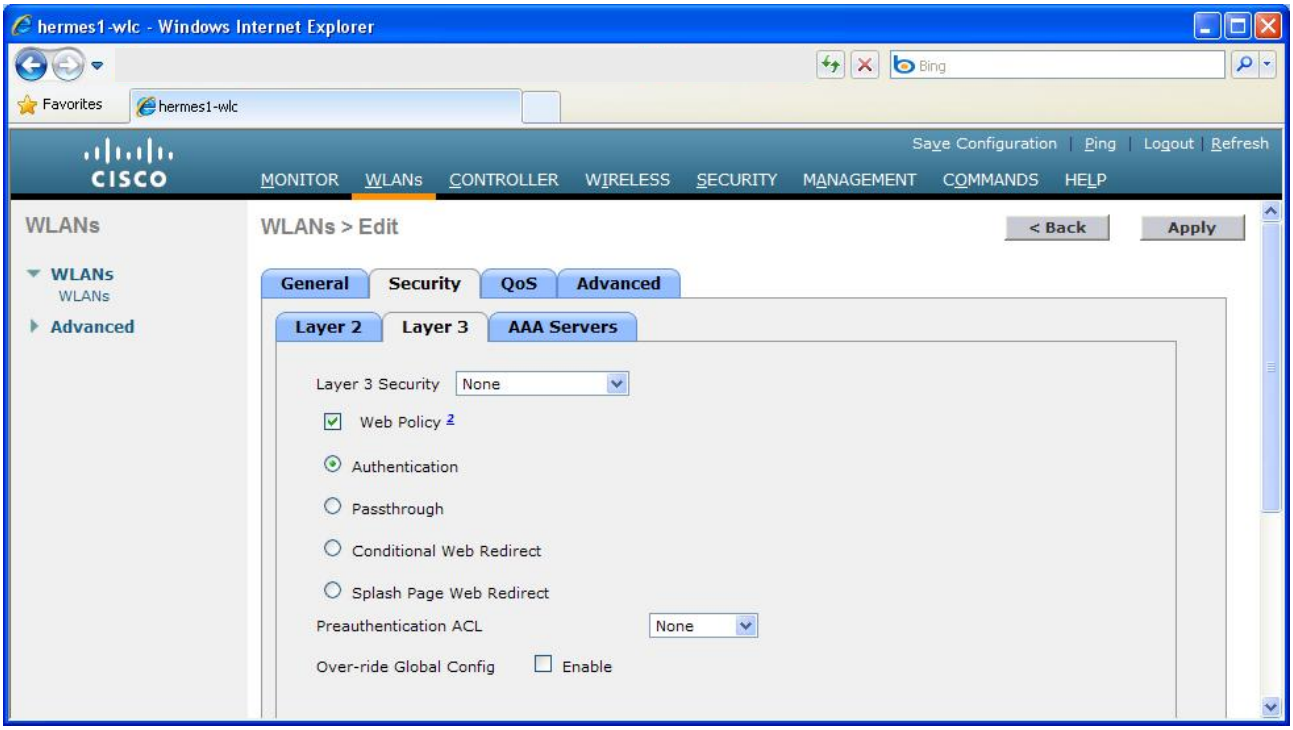


Kuva 22. Client Exclusion Policies-asetusten määritteleminen.

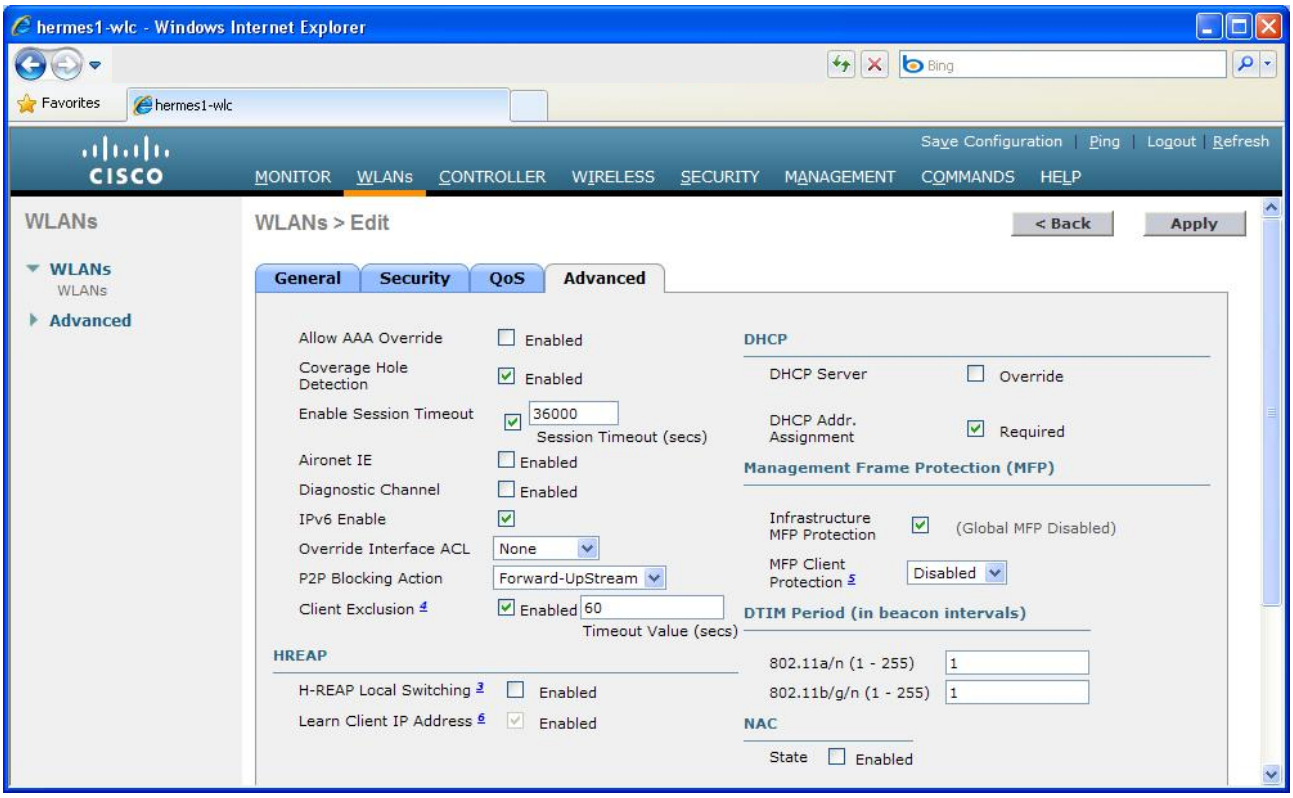
Jos määritellään toinen verkko kun eduroam-verkko ja tälle langattomalle verkolle halutaan web-autentikointia 802.1x-autentikoinnin sijaan, määritellään verkon turva-asetukset eri tavalla. Security välilehden Layer 2-asetukset määritellään kuvassa 23 esitetyllä tavalla ja Layer 3-asetukset kuvassa 24 esitetyllä tavalla. Lisäksi Advanced -välilehdellä määritellään istunnon maksimiaika Enable Session Timeout-kohdassa kuvan 25 mukaisesti. Istunnon maksimiaika ei saa olla liian lyhyt, koska ajan umpeutuessa käyttäjä joutuu autentikoimaan uudelleen, mikä johtaa avointen sessioiden katkeamiseen. HUOM! Jos verkossa on käytössä VLAN:eja, aseta myös ”Allow AAA Override” päälle Advaced-välilehden kohdalla.



Kuva 23. Web-autentikoidun verkon Security Layer2 -asetukset

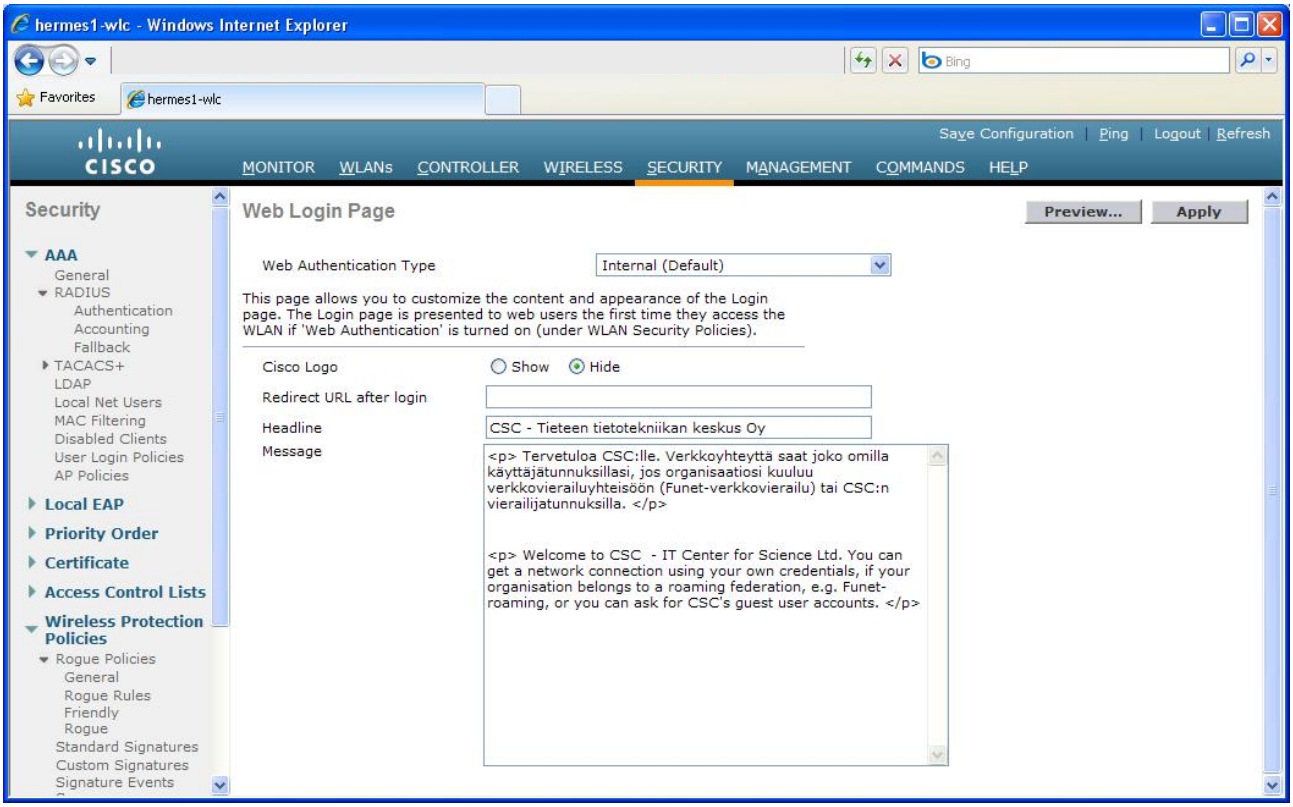


Kuva 24. Web-autentikoidun verkon Security Layer3 -asetukset.



Kuva 25. Web-autentikoidun verkon muut asetukset, joista tärkein on Enable Session Timeout.

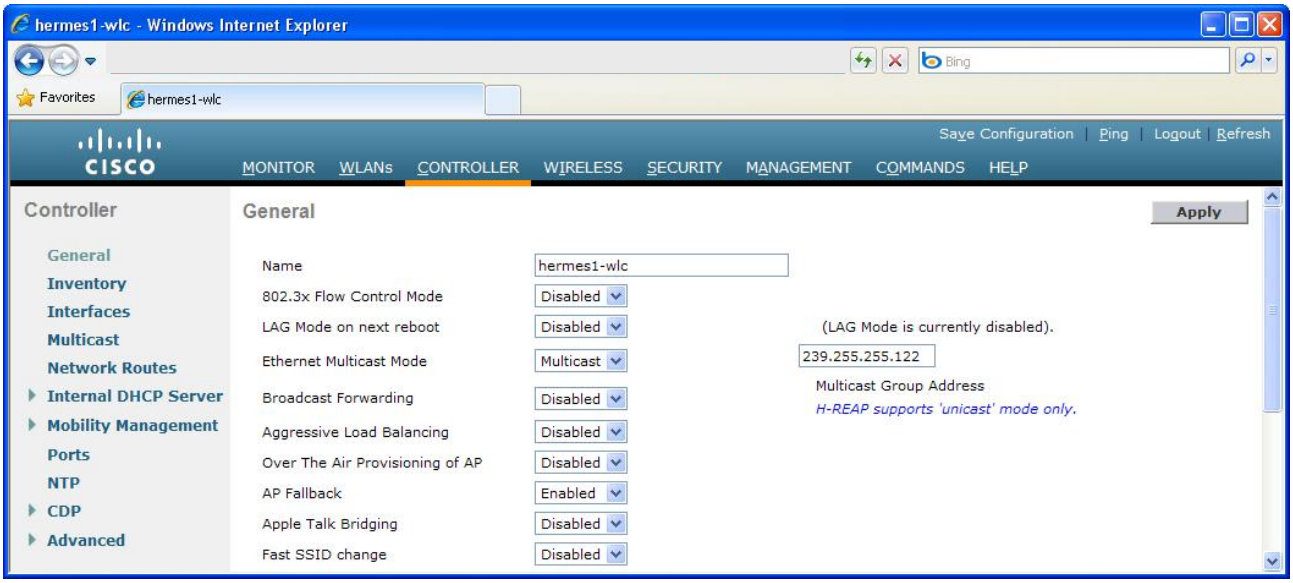
Määrittele lopuksi web-autentikointa hyödyntävälle verkolle sisäänkirjautumissivu. Kuvassa 32 on esitetty esimerkkinä vakiosivun muokkaaminen.



Kuva 26. Web-autentikoidun verkon sisäänkirjautumissivun määritteleminen.

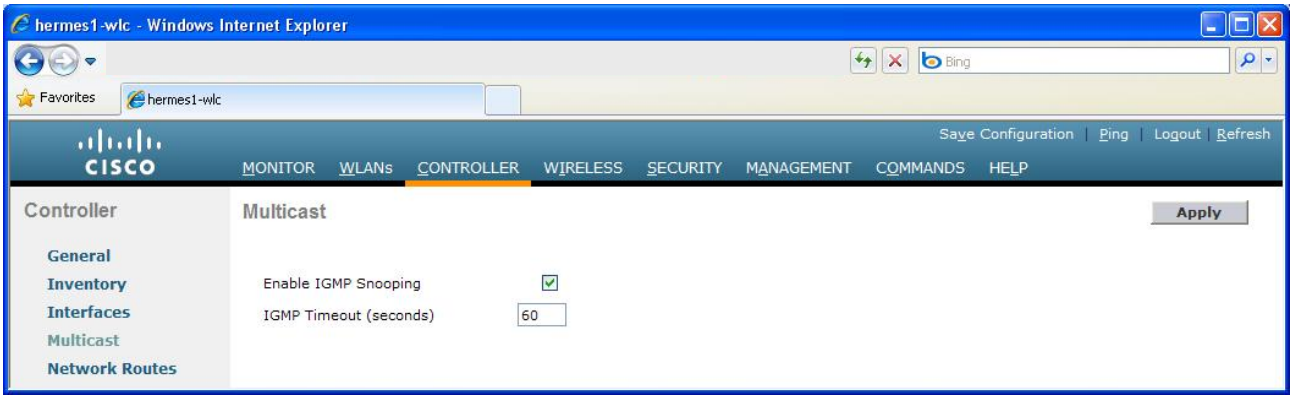
Multicast-toiminnon asettaminen päälle

Lähiverkon resurssien säästämiseksi voidaan hoitaa osan viestinvälityksestä kontrollerin ja tukiasemien välillä multicastilla. Multicast-toiminto on määriteltävä kontrollerin asetuksissa ja se tehdään valitsemalla ensin yläpalkista CONTROLLER ja sivupalkista General. Aukeavaan ikkunaan määritellään Ethernet Multicast Mode:ksi Multicast ja multicastin ryhmäosoite asetetaan, katso kuva 27. Multicastin ryhmäosoite on valitseva niin, että Funet-verkon suunnasta ei tule pyyntöjä liittyä tähän osoitteeseen. Pyydä tarvittaessa Funetilta apua. Toinen vaihtoehto suojata kontrollerin ja tukiasemien väliset multicast-lähetykset olisi ollut määritellä Time-To-Live (TTL)-arvoksi 1, mutta tätä parametria ei voida määritellä kontrollerissa.



Kuva 27. Mulicast toiminnon asettaminen kontrollerin ja tukiasemien väliselle liikenteelle.

Seuraavaksi siirrytään kontrollerin Multicast-kohtaan valitsemalla samasta sivupalkista Multicast. Aukeavassa ikkunassa laitetaan multicastille IGMP snooping päälle ja asetetaan timeout-arvoksi jotain 30s ja 300s väliltä, esim. 60 s. Esimerkki on esitetty kuvassa 28.



Kuva 28. Multicastin IGMP-asetukset.

Varmenteen asentaminen

Kontrollerille on asettava varmenne, jotta web-autentikointi toimisi loogisesti ja turvallisesti. Ilman varmennetta käyttäjälle näkyy selaimessa varoitus sisäänkirjautumissivun sijasta, kun hän yrittää päästä verkkoon. Jotta käyttäjälle aukeaisi heti sisäänkirjautumissivu, on asettava varmenne.

HUOM: Varmenteen hakuvaiheessa on muistettava että varmenteen CN-kentässä oleva nimi on oltava sama kun kontrollerin virtuaalirajapinnan (Virtual Interface) IP-osoitetta vastaava nimi DNS-palvelimessa.

Kun varmenne on hankittu, on huomattava että sitä ei voida siirtää kontrollerille ilman salasanasuojausta. Jos varmennetiedosto ei ole salasanasuojattu, se voidaan suojata openssl-ohjelman avulla esim. seuraavalla komennolla:

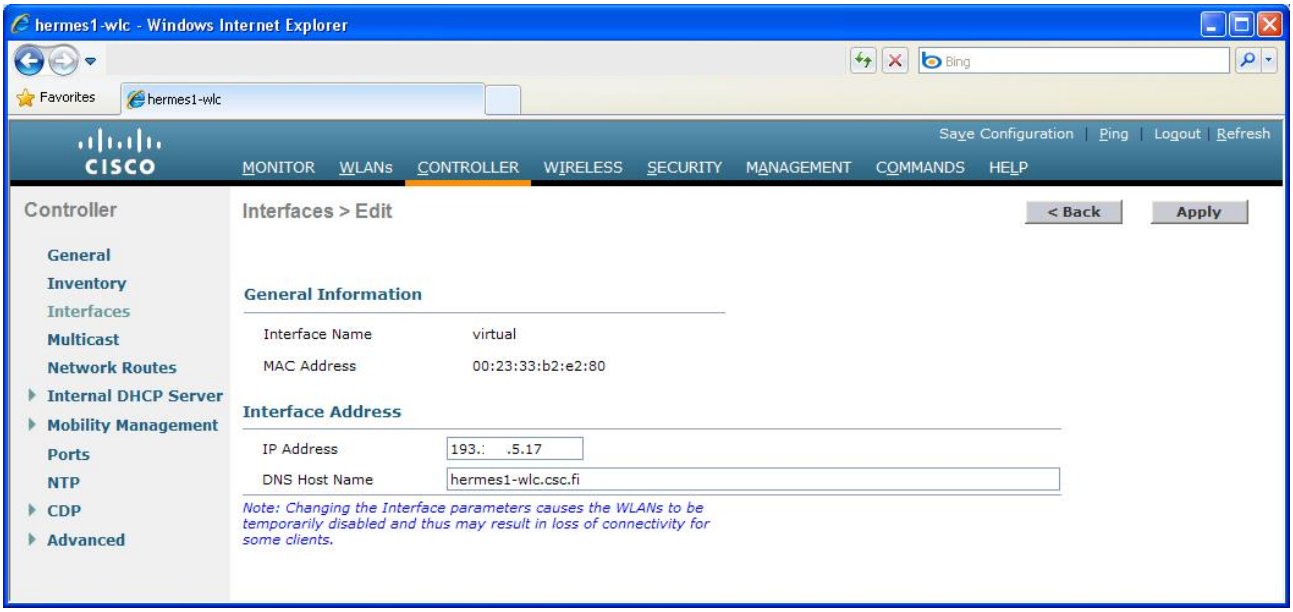
```
OpenSSL> pkcs12 -export -in myname.pem -inkey mykey.pem -out CA.p12 -
clcerts -passin pass:mypasswd -passout pass:mypasswd
```

Seuraavaksi asennetaan varmenteen salasana CLI:in kautta ja varmenne ladataan CLI:stä:

```
(Cisco Controller) >transfer download certpassword check123

Setting password to <check123>

(Cisco Controller) >transfer download start

Mode..................................................... TFTP

Data Type................................................ Site Cert

TFTP Server IP........................................... <TFTP server IP>

TFTP Packet Timeout...................................... 6

TFTP Max Retries......................................... 10

TFTP Path................................................ /

TFTP Filename............................................ myname.pem


This may take some time.

Are you sure you want to start? (y/N) y


TFTP Webauth cert transfer starting.


TFTP receive complete... Installing Certificate.


Certificate installed.

  Reboot the switch to use new certificate.
```

Käynnistä kontrolleri uudelleen ja siirry tämän jälkeen konfiguroimaan virtuaalirajapintaa valitsemalla yläpalkista CONTROLLER, sivupalkista Interfaces ja klikkaamalla *virtual* -rajapintaa. Varmista aukeavasta

ikkunasta että rajapinnan IP-osoite on oikein ja määrittele DNS host name-kohtaan varmenteen CN-kentässä oleva nimi, katso kuva 29.



Kuva 29. Virtuaalirajapinnan parametrien määrittely.

Useamman kontrollerin liittäminen yhteen (Mobility group)

Jos organisaatiolla on käytössä useampaa kontrolleria, on syytä liittää ne yhteen. Näin käyttäjät voivat siirtyä tukiasemasta toiseen ilman katkoja ja säilyttäen auki olevat sessionsa, eli IP-osoite pysyy samana. Määrittelemällä kontrollerit samaan mobility group:iin voidaan toteuttaa saumatonta siirtymistä tukiasemien välillä.

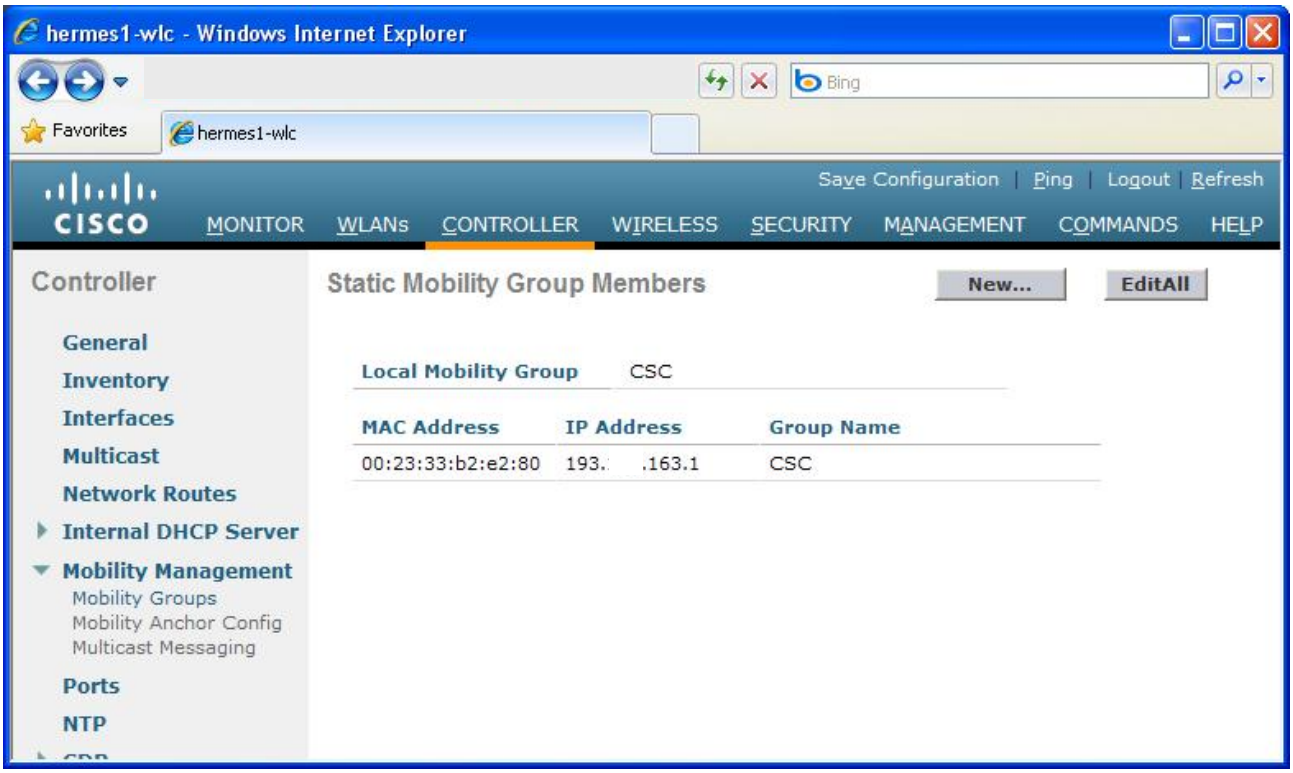
Ennen mobility groupin määrittelemistä, kokeile että pingi kulkee kaikkien kontrollerien välillä valitsemalla oikeasta yläkulmasta ping ja syöttämällä aukeavaan ikkunaan kukin kontrollerin IP-osoite vuorotellen. Kerää myös tässä vaiheessa lista kaikkien kontrollerien management liitännän IP-osotteista ja MAC-osotteista, jotka saadaan selville kun kontrollerista valitaan yläpalkista CONTROLLER ja sivupalkista Mobility Management |Mobility Groups.

On myös huomattavaa, että kontrollereilla, jotka liitetään yhteen mobility group-toiminnon avulla, on oltava sama IP-osoite virtuaalisessa rajapinnassa (CONTROLLER – Interfaces –virtual).

Jos kontrollerien välissä on palomuuri, tarkista asetukset. Portit 16666, 16667, 12222 ja 12223; IP protocol 50 ja 97 sekä UDP portti 500 on oltava auki. Jos käytät IPsec:iä, tarkista asetukset erikseen.

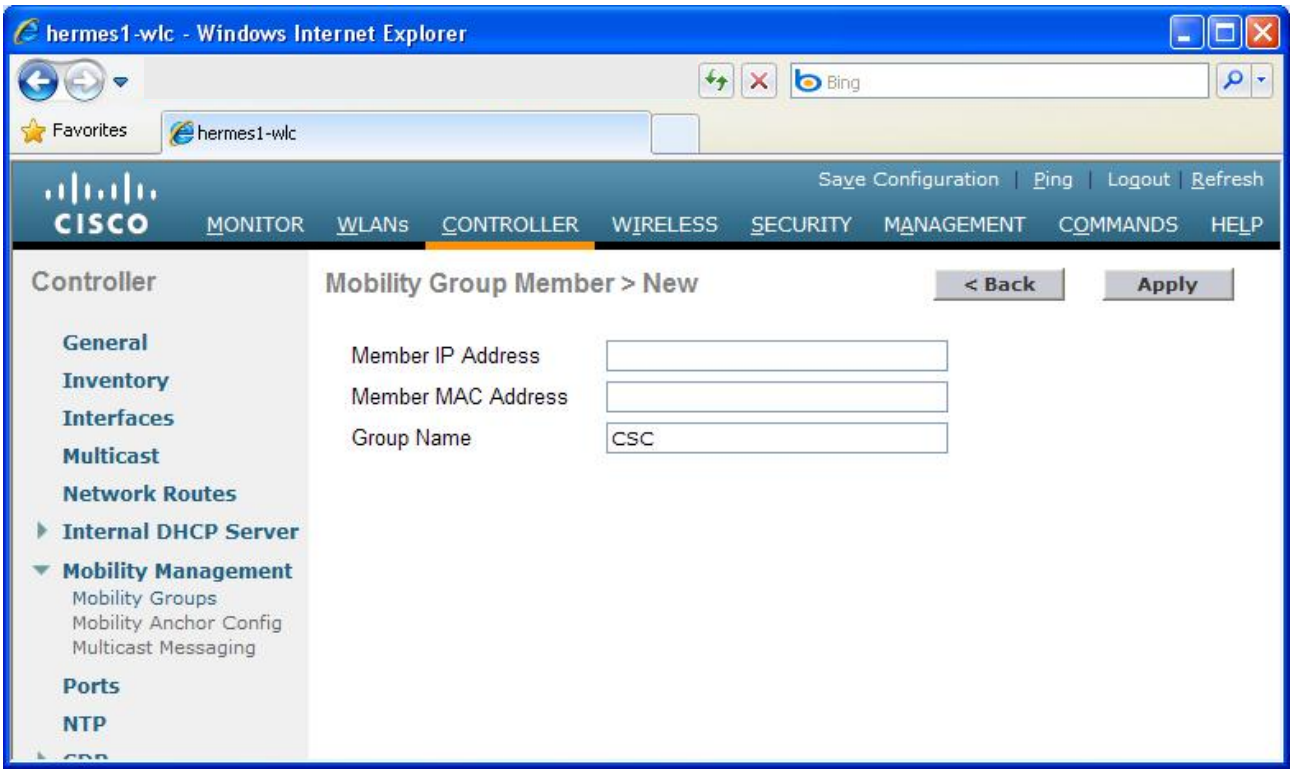
Määrittele seuraavaksi ryhmän nimi valitsemalla yläpalkista CONTROLLER ja sivupalkista General. Syötä valitsemasi nimi kohtaan Default Mobility Domain Name, jos et halua käyttää ensimmäisessä käynnistysvaiheessa valitsemaa nimeä.

Seuraavat muutokset on tehtävä jokaisella ryhmään kuuluvalla kontrollerilla. Siirry määrittelemään muut kontrollerit valitsemalla yläpalkista CONTROLLER ja sivupalkista Mobility Management | Mobility groups. Aukeavassa ikkunassa esitetään tällä hetkellä vain kyseisen kontrollerin tiedot, katso kuva 30.



Kuva 30. Mobility group:iin kuuluvien kontrollerien listaus.

Paina seuraavaksi New… -painiketta ja lisää organisaatiosi toisen kontrollerin tiedot. Määrittele management liitännän IP-osoite sekä MAC-osoite, katso kuva 31. Paina lopuksi Apply-painiketta. Lisää samalla tavalla organisaation muiden kontrollerien tiedot. Määrittele seuraavaksi organisaatioiden muissa kontrollereissa vastaavalla tavalla muiden kontrollereiden tiedot. Jokaisen kontrollerin tulos voidaan tarkistaa listaamalla kontrolleriin määriteltyjen muiden kontrollereiden tiedot painamalla kuvassa 30 esitettyä EditAll-painiketta.



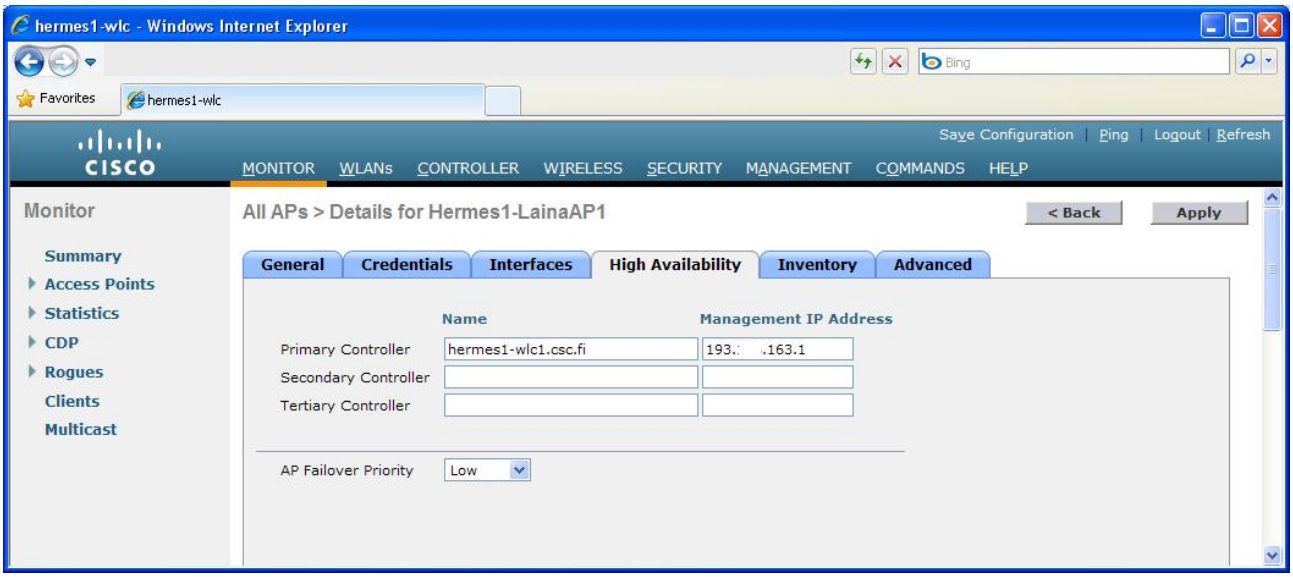
Kuva 31. Kontrollerin liittäminen mobility groupiin.

Seuraavaksi määritellään kontrollereiden väliselle viestinnälle multicast-toimintoa. Valitaan yläpalkista CONTROLLER ja sivupalkista Mobility Management | Multicast messaging. Ruksaa aukeavaan ikkunaan Enable Mulicast Messaging ja määrittele ryhmälle valittu IP-osoite.

Konfigurointi lainatukiasemia varten (valinnainen)

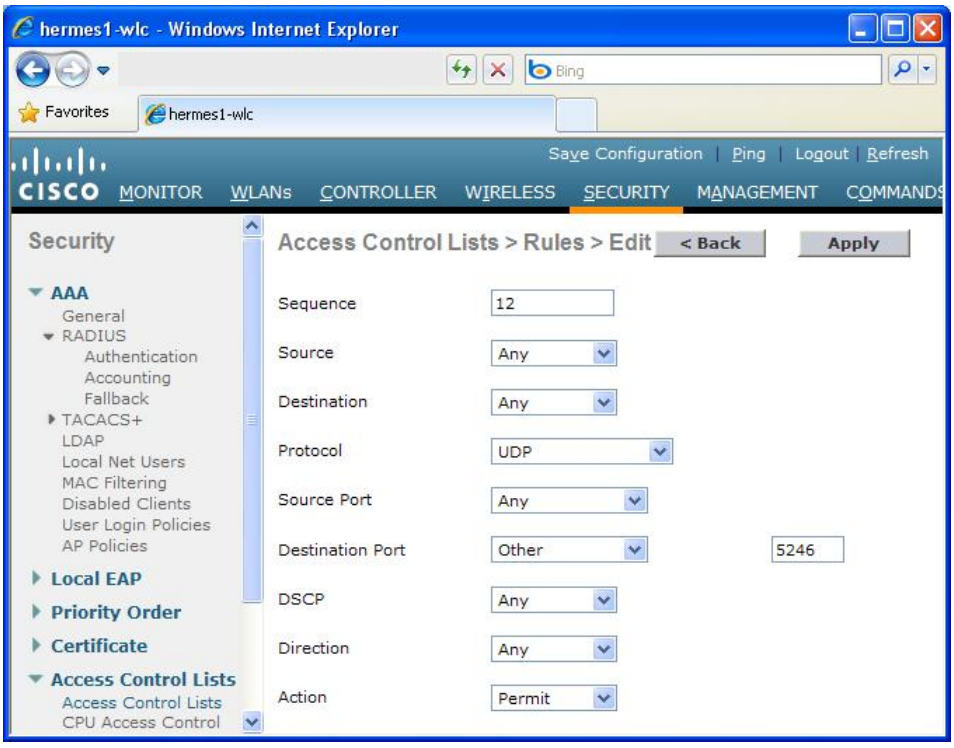
Verkon rakentamisen tai päivittämisen yhteydessä voi olla järkevää hankkia muutama ylimääräinen tukiasema, jotka voidaan käyttää lainatukiasemina. Lainatukiasemien avulla voidaan pysyttää WLAN-verkkoa nopeasti ja kätevästi melkein mistä tahansa lähiverkkorasiasta. Lainatukiasemat voidaan viedä mukaan esim. jos kurssi tai konferenssi järjestetään muualla kuin organisaation omissa tiloissa. Tukiasemat voidaan konfiguroida niin, että ne ottavat automaattisesti yhteyttä organisaation kontrolleriin ja tarjoavat tämän jälkeen samat verkot kuin muut kontrollerissa kiinni olevat tukiasemat. Paikallisen verkon palomuurisäännöt voi periaatteessa estää yhteydenottoa kontrolleriin mutta käytännössä sallitaan yleensä joustavasti liikennettä verkosta Internetiin päin.

Tulevat lainatukiasemat on aina kytkettävä verkkoon kotiorganisaatiossa ennen kun ne voidaan käyttää muualla. Varmistetaan tässä yhteydessä että tukiasemat löytävät kontrolleria Tukiasemien liittäminen verkkoon ja konfigurointi-kappaleen alussa esittämällä tavalla. Lainatukiasemien tarjoamat langattomat verkot sekä niiden ilmarajapinnan asetukset tulevat aina olemaan samanlaiset kuin kontrolleriin liittyneiden muiden tukiasemien verkot ja asetukset. Kun tukiasema on löytänyt kontrolleria sillä on periaatteessa aina kontrollerin osoite tallessa mutta varmuuden vuoksi organisaation kontrollerin/kontrollereiden osoitteet kannattaa määritellä lainatukiasemiin. Se tehdään valitsemalla yläpalkista WIRELESS ja sivupalkista Access Points | All APs. Klikkaa aukeavasta taulukosta juuri liittynyt tukiasema ja määrittele sille kuvaava nimi. Siirry seuraavaksi High Availability-välilehteen ja määrittele organisaatiosi kontrollerit, katso esimerkki kuvasta 32. Paina lopuksi Apply-painiketta.



Kuva 32. Lainatukiasemille on syytä määritellä omat kontrollerit ja niiden IP-osoitteet.

Jotta lainatukiasemat pystyisivät liittymään kontrolleriin mistä verkosta tahansa, on muokattava myös läpipääsylistaa (ACL-listaa). Tukiasemien liittymispyyntöihin käytetään nykyisin CAPWAP-protokollaa ja tälle protokollalle on avattava UDP portit 5246 ja 5247. CAPWAP on standardoitu protokolla ja vanhemman, Ciscon oman LWAPP-protokollan seuraaja. Kuvassa 33 esitetään miten CAPWAP-protokollalle avataan portti 5246 läpipääsylistassa. Portti 5247 avataan vastaavalla tavalla. Enemmän tietoa läpipääsylistoista löytyy kappaleesta Läpipääsylistan määritteleminen.



Kuva 33. CAPWAP-protokollan viestien läpipäästämisen määrittäminen.

HUOM: Kun CAPWAP-protokollalle avataan pääsy läpipääsylistassa ylhäällä esitetyllä tavalla, minkä tahansa tukiaseman liittymistä kontrolleriin ei etukäteen voida estää. Jos tuntematon tukiasema jostain syystä saa tietoa organisaation kontrollerin IP-osoitteesta, tukiasema voi huomaamatta liittyä kontrolleriin ja rupea

tarjoamaan organisaation langattomia verkkoja peittoalueessaan. CAPWAP-protokollan avaaminen sisältää siis pienen tietoturvariskin, mutta monessa Funet-jäsenorganisaatiossa on hyväksytty tämä riski. Muissa tapauksissa tulisi ennen tukiaseman liittymistä kontrolleriin tietää mikä IP-osoite lainatukiasema on saanut paikallisesta verkosta, ja tämä aiheuttaisi IT-tuelle paljon ylimääräistä työtä.

Viitteet

[1] W. Backman et.al. ”WLAN-verkon tietoturva,” Hyväksytty Funet Best Practice Document (BPD), kesäkuu 2010. Saatavilla osoitteesta https://info.funet.fi/wiki/BCP/WLANVerkonTietoturva

[2] W. Backman et. al ”WLAN-verkon suunnittelu ja rakentaminen” Hyväksytty Funet Best Practice Document (BPD), joulukuu 2010.. Saatavilla osoitteesta https://info.funet.fi/wiki/BCP/WLANVerkonSuunnittelu

[3] W. Backman ja M. Räisänen ” FreeRADIUSen konfigurointiohjeita” Saatavilla osoitteesta https://info.funet.fi/wiki/BCP/FreeRADIUSKonfigurointi