

HP:n WLAN-kontrollerin konfigurointi

Dokumentissa esitetään HP:n WLAN-kontrollerin konfigurointia. Kuvat on otettu Procurve MSM760-kontrollerista joten eri mallin komentoikkunat saattavat näyttää erilaisilta.

Sisältö

Yleistä.....	2
RADIUS-palvelimen määrittäminen.....	2
VSC:n (Virtual Service Community) määrittäminen	3
Tukiasemien liittäminen verkkoon ja konfigurointi.....	7
Viitteet	10

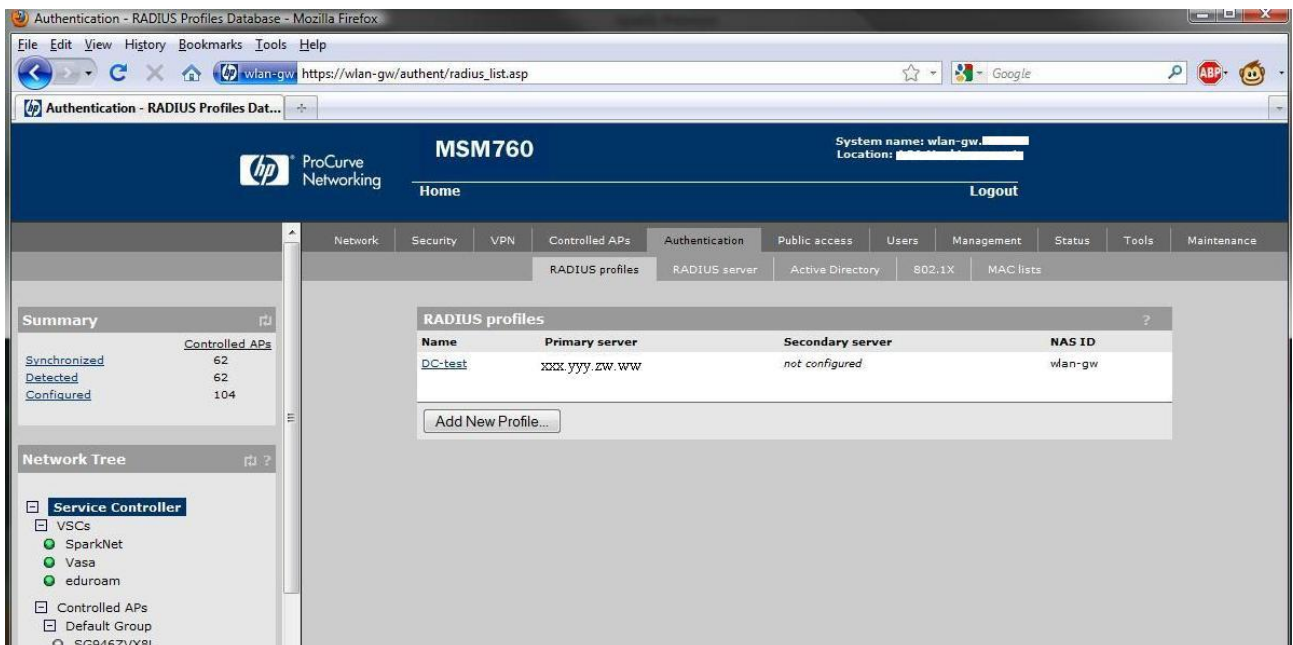
Yleistä

Kun kontrollerille on annettu IP-osoite ja käyttäjätunnus on määritelty, voidaan siirtyä konfiguroimaan kontrolleria selaimen avulla.

HP:n WLAN-kontrollerissa WLAN-verkon konfiguroinnin vaiheet ovat seuraavat: Ensin luodaan VSC (virtual service community), jolle määritellään mm. SSID, autentikointitapa ja kryptaus. Seuraavaksi järjestetään kontrolleriin liittyneet tukiasemat ryhmiin ja toivottu verkko saadaan aikaan määrittelemällä tietyille ryhmälle tietty VSC. On kuitenkin järkevää aloittaa määrittelemällä WLAN-verkon autentikointia hoitava RADIUS-palvelin.

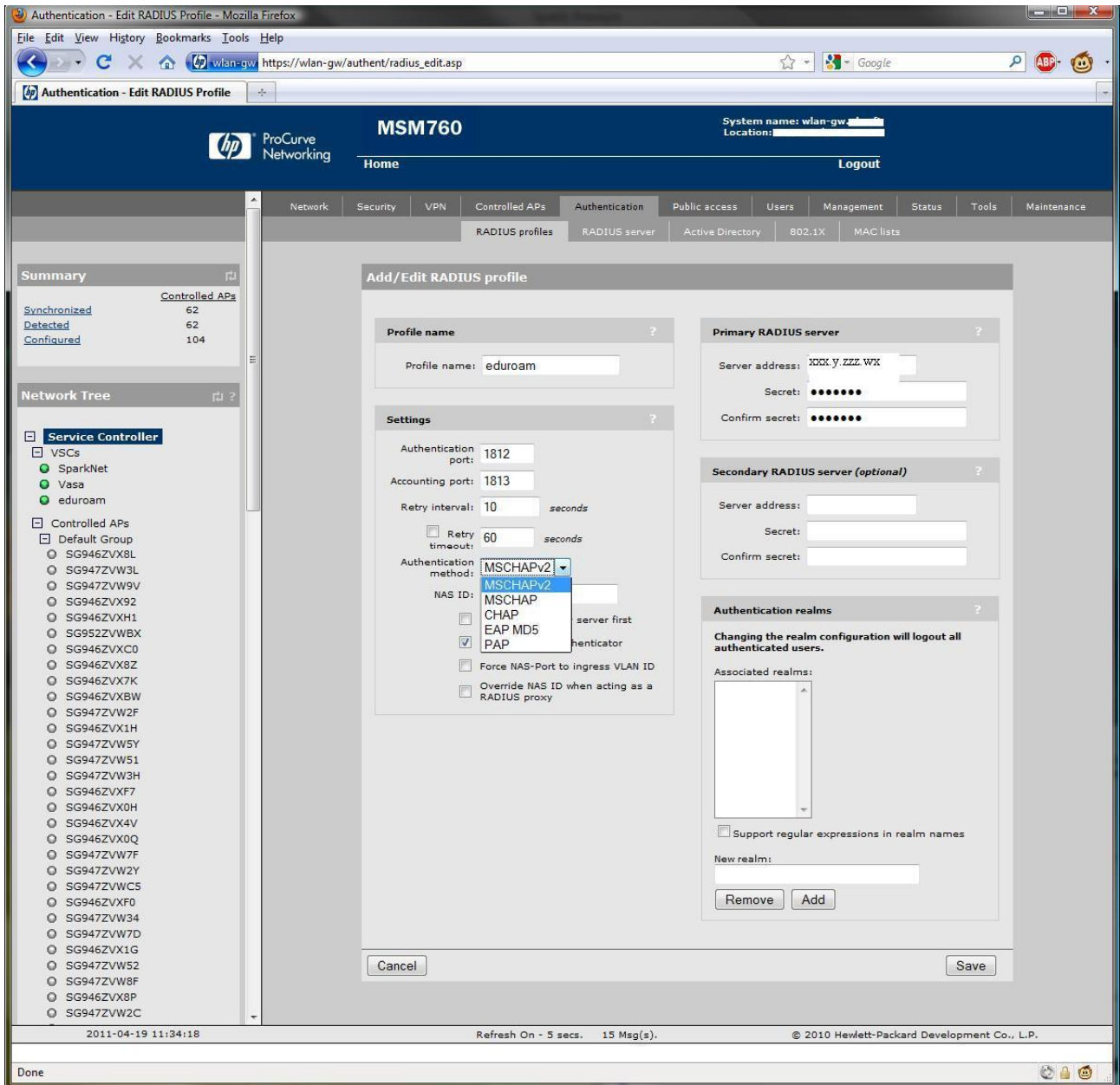
RADIUS-palvelimen määrittäminen

HP Procurve sisältää integroidun RADIUS-palvelimen, mutta se on suunniteltu pienille verkoille eikä sitä kannata käyttää kampusverkoissa. Siirry määrittelemään ulkoista RADIUS-palvelinta valitsemalla Service Controller >> Authentication > RADIUS profiles, jolloin sinulle aukeaa kuvassa 1 näkyvä ikkuna.



Kuva 1. RADIUS-profiilien/palvelimien yhteenvetoikkuna.

Paina Add New Profile...-painiketta ja määrittele RADIUS-palvelin kuvassa 2 näkyvällä tavalla. Authentication method-alasvetovalikon vaihtoehdot ei huomioida jos WLAN-verkossa käytetään 802.1x-autentikointia, kuten esim. eduroamissa. Authentication realms-kohta voidaan jättää tyhjäksi, ellei halua käyttää eri palvelimia eri realmien autentikointiin.



Kuva 2. RADIUS-profiilin, eli RADIUS-palvelimen määrittäminen.

VSC:n (Virtual Service Community) määrittäminen

Siirry määrittämään VSC valitsemalla Service Controller >> Overview > VCS profiles, jolloin sinulle aukeaa kuvassa 3 näkyvä ikkuna.

The screenshot shows the HP ProCurve MSM760 VSC profiles configuration page. The browser address bar shows the URL: https://wlan-gw/centcfg/vsc_list.asp?entity=allvsc&selector=All. The page title is "VSC profiles" and the system name is "wlan-gw".

The page is divided into several sections:

- Summary:** Shows the number of Controlled APs: Synchronized (62), Detected (62), and Configured (104).
- Network Tree:** Shows a tree view of the network configuration, including Service Controller, VSCs (SparkNet, Vasa), Controlled APs (Default Group, Datacentralen), and <None Configured>.
- VSC profiles table:** A table showing the configuration for VSC profiles. The table has columns for Name, Ingress, Egress, Encryption, and Authentication. The rows are SparkNet (Default) and Vasa.

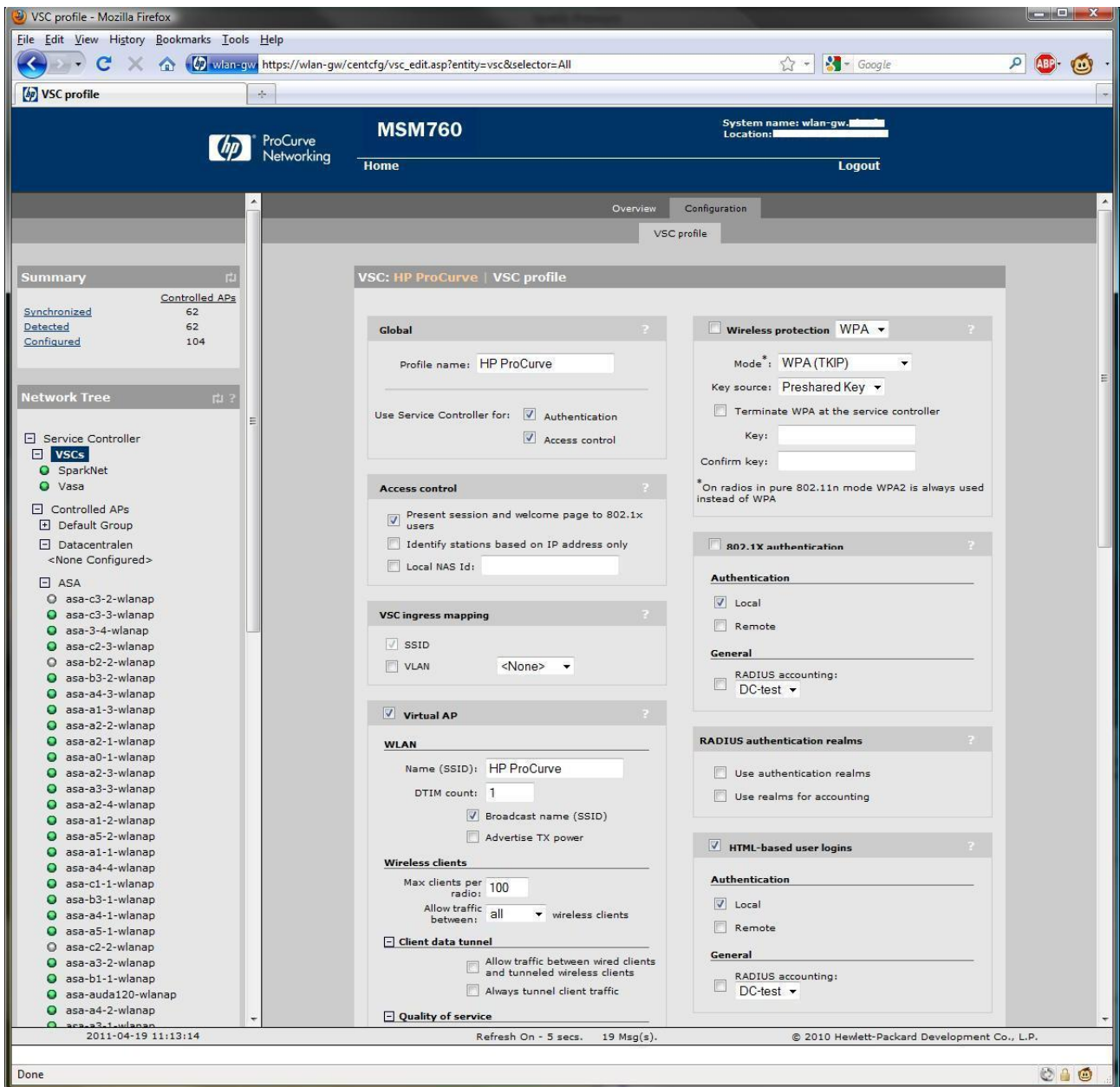
Name	Ingress		Egress			Encryption			Authentication		
	SSID	VLAN	GRE	VLAN	TKIP	AES	WEP	802.1x	MAC	HTML	
SparkNet (Default)	Spark	-	-	-	-	-	-	-	-	-	
Vasa	Abo Akademi	-	-	-	-	-	-	-	-	-	

Below the table, there is a legend for the status icons:

- = Access controlled
- = SSID Off
- = SSID On
- = SSID On and configured for broadcast

Kuva 3. VSC profiilien yhteenveto.

Paina kuvassa näkyvää Add New VSC Profile... -painiketta. Sinulle aukeaa kuvassa 4 näkyvä ikkuna.

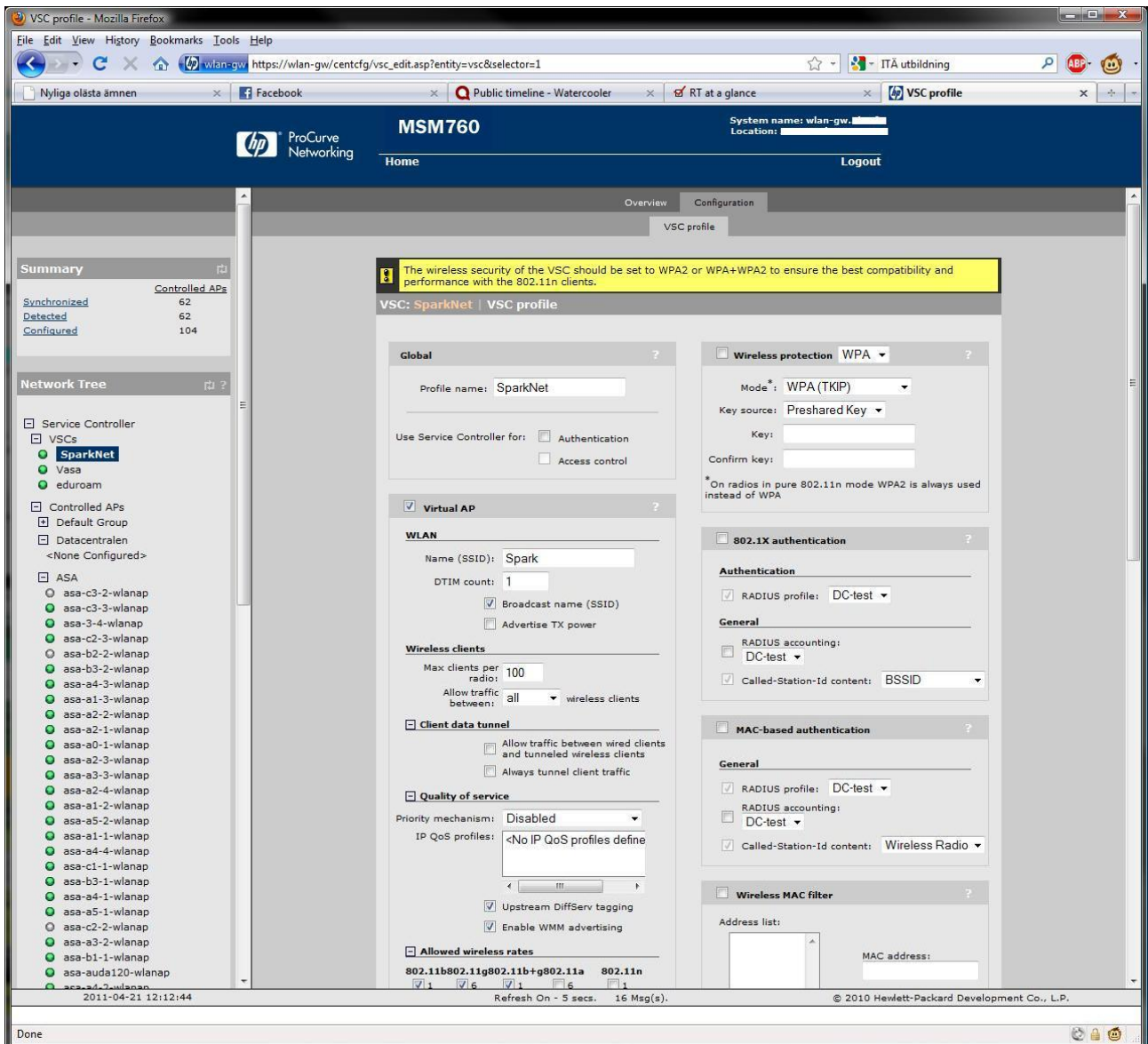


Kuva 4. VSC-profiilin määrittely.

Jos haluat määrittellä verkon, missä käytetään web-autentikointia, on esitetty esimerkki kuvassa 5. Määrittele vasemmassa kolumnissa ensin profiilille sopiva nimi ja poista ruksit kohdista Authentication ja Access control. Valitse seuraavaksi verkolle sopiva SSID. Kuvan alareunassa näkyy osan nopeuksien määrittelyä. 802.11b-standardin tukeminen alentaa verkon kokonaiskapasiteettia, joten olisi suotavaa tukea ainoastaan 802.11a/g/n-standardit. Lisätietoja kokonaiskapasiteetin alentamisesta löytyy Parhaat käytännöt-dokumentista "WLAN-verkon suunnittelu ja rakentaminen" [2]. Vasemman kolumnin alalaidassa voidaan määrittellä liikenteelle suodattimia. Suodattimen säännöt ovat lähtökohtaisesti liian tiukasti määriteltyjä ja liikenteen sujuvan kulkemisen edistämiseksi on syytä keventää sääntöjä tai poistaa suodatin poistamalla ruksi Wireless security filters-kohdasta.

Kuvassa 5 näkyy oikeassa kolumnissa ensimmäisenä kohtana Wireless protection. Koska web-autentikoidussa verkossa ei käytetä salausta, Wireless protection-kohta jätetään ruksaamatta. Seuraava kohta, eli 802.1x authentication, jätetään myös ruksaamatta. Kohta HTML-based user logins ruksataan web-

autentikoinnin tapauksessa ja RADIUS-palvelimeksi valitaan aikaisemmin määritelty RADIUS-profiili, ruksaamalla ensin Remote-kohta. Oikean kolumnin jäljellä olevat kohdat voidaan jättää ruksaamatta.

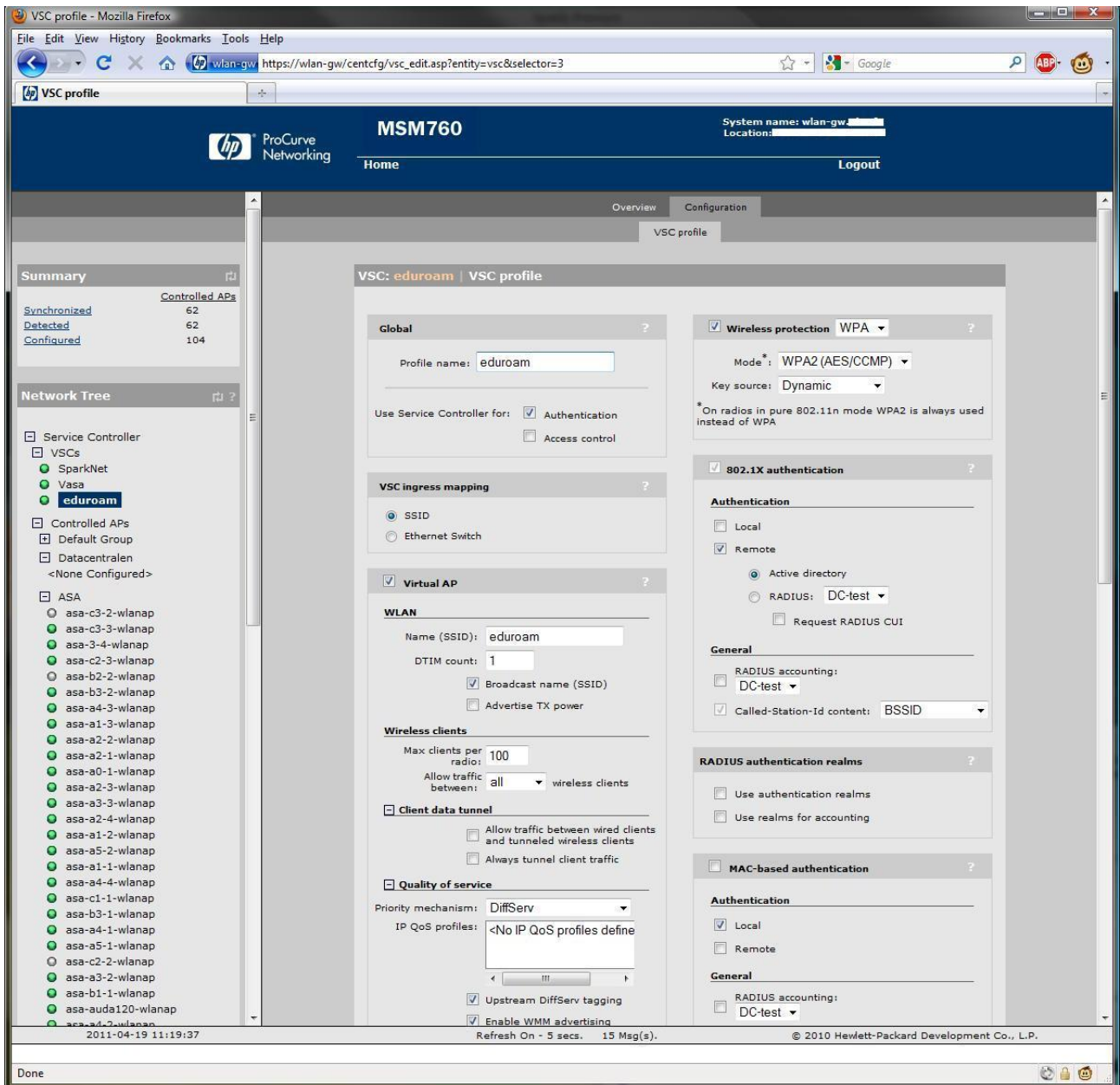


Kuva 5. VSC-profiili web-autentikointia varten. Keltaisella näkyvä varoitus johtuu siitä, että 802.11n-standardin korkeiden siirtonopeuksien täydellinen hyödyntäminen vaatii WPA2-salauksen tukeminen verkossa.

Jos haluat määritellä verkon, missä käytetään autentikointimenetelmänä 802.1x, on esitetty esimerkki kuvassa 6. Profiilin nimeksi on valittu eduroam, koska eduroam-verkoissa käytetään aina 802.1x-autentikointia. VSC ingress mapping saa olla SSID, ellei haluta liittää liikennettä tukiasemien tiettyyn porttiin. Eduroam-verkossa myös SSID on aina eduroam. Vasemman kolumnin muut asetukset voivat olla samanlaiset kuin web-autentikoidun verkon asetukset.

Oikeassa kolumnissa ruksataan Wireless protection-kohta ja Mode-kohdassa valitaan WPA2 (AES/CCMP). Näin verkossa tuetaan vain WPA2-salausta, eikä WPA-salausta, "WLAN-verkon tietoturva"-Parhaat käytännöt -dokumenttia, [1], seuraten. Key source-kohdassa valitaan Dynamic. Seuraavaksi ruksataan 802.1x authentication-kohta sekä Remote-kohta. Määrittele kuvasta poiketen Active directory:n sijasta

RADIUS ja valitse alavetovalikosta aikaisemmin määritelty RADIUS-profiili. Oikean kolumnin jäljellä olevat kohdat voidaan jättää ruksaamatta.

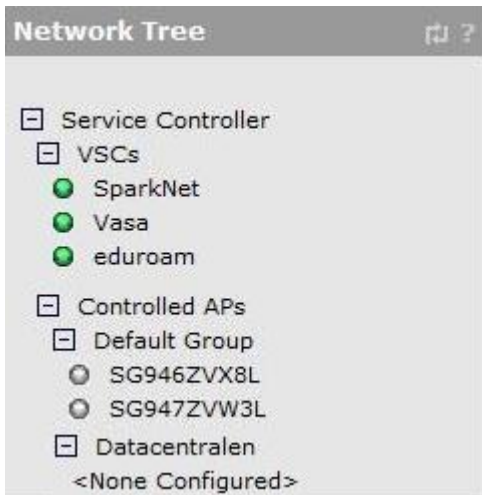


Kuva 6. VSC-profiili 802.1x-autentikointia varten.

Tukiasemien liittäminen verkkoon ja konfigurointi

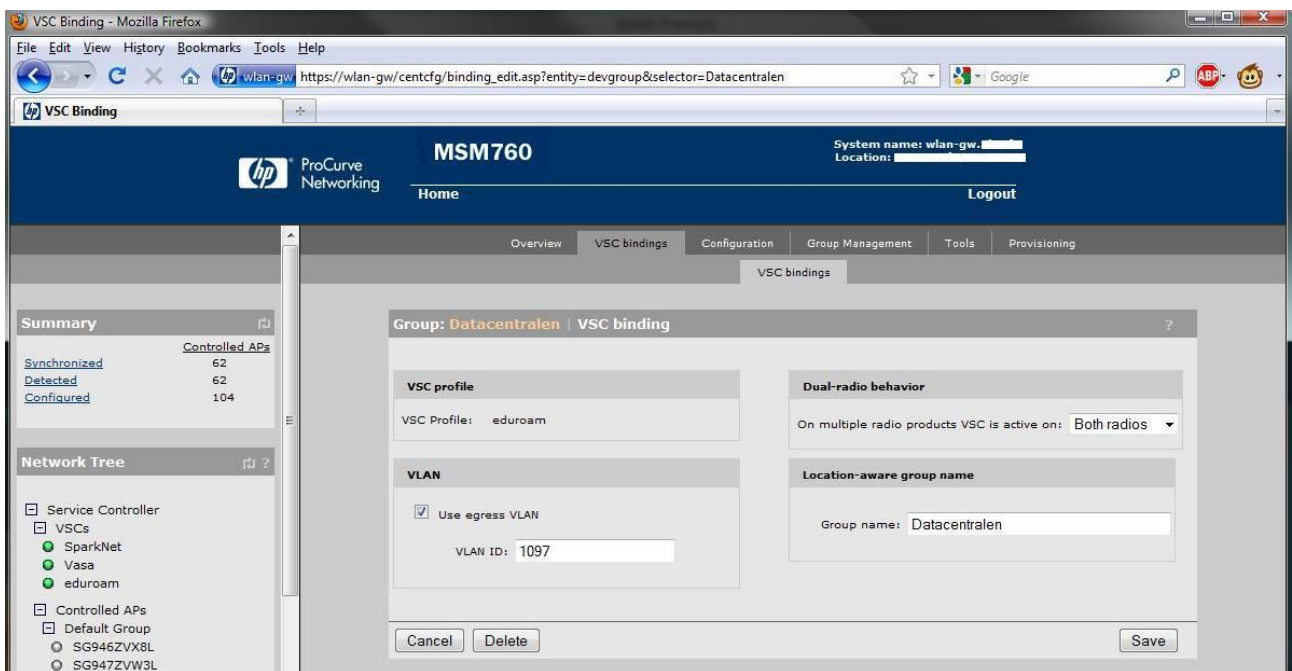
Helpoin tapa saada tukiasemat liittymään kontrolleriin on kytkeä ne samaan aliverkkoon kuin kontrolleri. Muissa tapauksissa on käytettävä DHCP option 43 tai DNS palvelimeen on lisättävä kontrollerin IP-osoite nimelle cnsrv1.mydomain.com, cnsrv2.mydomain.com tai cnsrv3.mydomain.com.

Kun tukiasema on liittynyt kontrolleriin, se kuuluu automaattisesti ryhmään Default group, katso kuva 7. Määritä tuotannossa oleville verkon tukiasemille oma ryhmä valitsemalla Controlled APs >> Group management, painamalla Add New Group... -painiketta, valitse ryhmälle nimi, esim Datacentralen ja paina Save-painiketta. Nimi ilmestyy Controlled APs-valikkoon, kuten kuvassa 7.



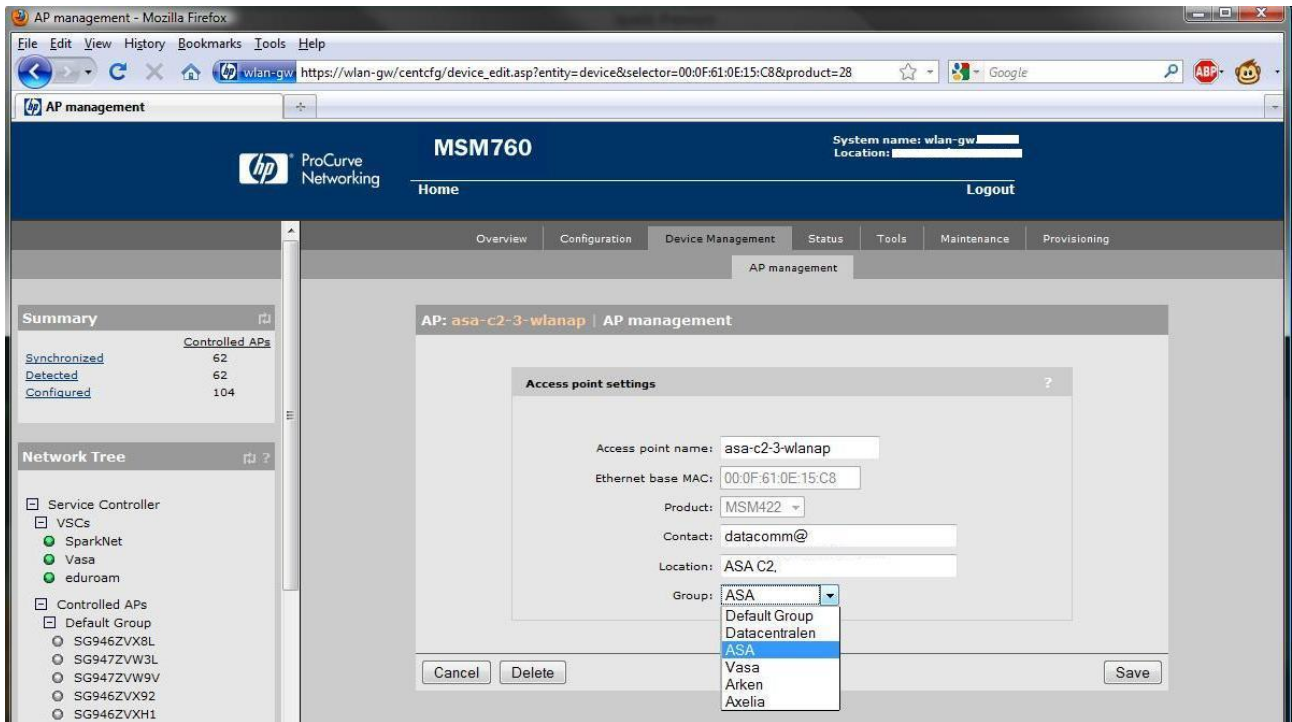
Kuva 7. Verkon rakenne.

Ennen kuin tukiasemat siirretään Default group:ista juuri määritettyyn ryhmään, ryhmän verkkoasetukset voidaan määrittää. Ryhmän verkkoasetukset määrätään liittämällä ryhmälle sopiva VSC. Valitse ryhmä Controlled APs-valikon alta ja valitse oikealla VSC bindings ja Add New Binding. Liitä ryhmä sopivaan VSC:hen kuvan 8 näyttämällä tavalla. Tässä yhteydessä voidaan myös määrittellä käytettävä VLAN.



Kuva 8. VSC:n asettaminen ryhmälle.

Seuraavaksi siirretään tukiasemat Default groupista määritettyyn ryhmään. Valitse tukiasema ja aseta sille toivottu ryhmä kuvan 9 näyttämällä tavalla.



Kuva 9. Tukiaseman siirtäminen tiettyyn ryhmään.

Kuvassa 10 näytetään vielä esimerkki tukiaseman tiedoista. Tukiasema on liitetty ASA-ryhmään.

AP details - Mozilla Firefox

System name: wlan-gw
Location: _____

MSM760

Home Logout

Overview Configuration Device Management Status Tools Maintenance Provisioning

AP details Wireless clients Wireless rates Neighborhood Mobility neighbors Local mesh neighborhood Local mesh links RTLS Licen

Summary

Controlled APs

Synchronized 62
Detected 62
Configured 104

Network Tree

Service Controller

VSCs

- SparkNet
- Vasa
- eduroam

Controlled APs

- Default Group
 - SG946ZVX8L
 - SG947ZVW3L
 - SG947ZVW9V
 - SG946ZVX92
 - SG946ZVXH1
 - SG952ZVWBX
 - SG946ZVXC0
 - SG946ZVX8Z
 - SG946ZVX7K
 - SG946ZVXBW
 - SG947ZVW2F
 - SG946ZVX1H
 - SG947ZVW5Y
 - SG947ZVW51
 - SG947ZVW3H
 - SG946ZVXF7
 - SG946ZVX0H
 - SG946ZVX4V
 - SG946ZVX0Q
 - SG947ZVW7F
 - SG947ZVW2Y
 - SG947ZVWC5
 - SG946ZVXF0
 - SG947ZVW34
 - SG947ZVW7D
 - SG946ZVX1G
 - SG947ZVW52
 - SG947ZVW8F
 - SG946ZVX8P
 - SG947ZVW2C

AP: asa-c2-3-wlanap | Overview

Number of displayed access points: 1

Select the action to apply to all listed APs: -- Select an Action -- Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	asa-c2-3-wlanap	SG947ZVW47	📶	0	Synchronized	

📶 = AP Mode 📶 = Local Mesh Mode 📶 = AP/Local Mesh Mode 🔍 = Monitor Mode 📶 = Sensor Mode ✖ = Disabled

AP: asa-c2-3-wlanap | Details

Diagnostic information

The AP is up and running, offers wireless services and had its firmware and configuration settings successfully updated by the service controller.

Configured information

Access point name: asa-c2-3-wlanap
Access point location: ASA C2
Access point contact: datacomm@
Group name: ASA

Maintenance information

Serial number: SG947ZVW47
Ethernet base MAC: 00:0f:61:0e:15:c8
Platform: MSM422
Boot revision: Boot 9.24 (Oct 23 2009 - 19:15:09)
Hardware revision: 50-00-1034-00
Firmware revision: 5.3.6.18-01-9124

Networking information - AP

Control channel: Port 1
VLAN identifier: Untagged
MAC address: 00:0f:61:0e:15:c8
IP address: 130.
IP netmask: 255.255.252.0
IP gateway: 130.
Connectivity: L3

Networking information - Service controller

Discovered on interface: Internet port
VLAN ID: Untagged

Licensing information

Integrated license(s): None

Wireless information

Radio	Operating mode	Wireless mode	Channel selection	Current channel
Radio 1	AP only	802.11n (5 GHz)	Automatic	Channel 44, 5.220GHz
Radio 2	AP only	802.11b/g	Automatic	Channel 8, 2.447GHz

Security information

Authorization status: Authorized
Authorization method: Discovered

2011-04-19 11:31:05 Refresh On - 5 secs. 15 Msg(s). © 2010 Hewlett-Packard Development Co., L.P.

Kuva 10. Tukiaseman tiedot.

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>