

Arch·Red	KÄYTTÖOHJE	JULKINEN
	<i>Langaton Tampere: Cisco WLAN Controller konfigurointi</i>	V1.0 15.10.2008
		1 (18)

LANGATON TAMPERE:

**CISCO WLAN CONTROLLER
KONFIGUROINTI**

Arch • Red	KÄYTTÖOHJE	JULKINEN
	<i>Langaton Tampere: Cisco WLAN Controller konfigurointi</i>	V1.0 15.10.2008
		2 (18)

SISÄLLYSLUETTELO

WLAN-verkkoliityntöjen konfigurointi.....	3
Tunnistautumispalveluiden konfigurointi.....	8
WLAN-radioverkkojen konfigurointi.....	11
WPA-verkon (LANGATON-WPA) konfigurointi.....	12
WWW-verkon (WirelessTampere) konfigurointi.....	16
Lisätietoja.....	18

WLAN-VERKKOLIITYNTÖJEN KONFIGUROINTI

Langattoman Tampereen WLAN-verkkojen konfiguroiminen kannattaa aloittaa niitä varten luotavien verkkoliityntöjen (interfaces) luonnista (kts. Kuva 1). Ciscon kontrollerissa tämä käytännössä tarkoittaa kahden verkkoliityntän luomista – toinen WPA-autentikoidulle verkolle (wpa-vlan) ja toinen WWW-autentikoidulle verkolle (www-vlan). Näitä verkkoja varten kannattaa varata myös kaksi eri VLANia, jotta WPA:n käyttäjien tietoturva ei heikkene kuten yhteistä VLANia käytettäessä muutoin helposti kävisi.

The screenshot shows the Cisco Controller configuration page for 'Interfaces'. The table lists the following configurations:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	42	10.11.12.3	Static	Enabled
management	42	10.11.12.2	Static	Not Supported
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	172.25.72.25	Static	Not Supported
wpa-vlan	145	172.17.148.2	Dynamic	Disabled <input type="checkbox"/>
www-vlan	144	172.17.144.2	Dynamic	Disabled <input type="checkbox"/>

Kuva 1: Ciscon verkkoliityntöjen konfiguraatio

Verkkoliityntöjen konfiguraatiossa ei sinänsä ole mitään erityisen monimutkaista (kts. Kuva 2 ja Kuva 3). Riippuen tilanteesta ja alueesta osoitteita kannattaa varata riittävästi ja mieluummin enemmän kuin vähemmän. DHCP-palvelimena voi käyttää joko Ciscon kontrolleria tai sitten erillistä DHCP-palvelinta kuten tässä konfiguraatioesimerkissä. Ulkoista DHCP- ja DNS-palvelinta käytettäessä on huomattava, että Ciscon kevyet tukiasemat hakevat DHCP:llä ja DNS:llä tietoa mahdollisesta kontrollerista liittyäkseen mukaan verkkoon, joten toiminnan kannalta pääsy konfiguroimaan näitä palveluita on olennaista. Esimerkiksi DNS-palvelimeen kannattaa konfigroida valmiiksi CISCO-LWAPP-CONTROLLER osoittamaan kuvassa 1 näkyvään ap-managerin osoitteeseen.

The screenshot shows the Cisco Controller configuration interface for the 'wpa-vlan' interface. The left sidebar contains a navigation menu with categories like General, Inventory, Interfaces, Network Routes, Internal DHCP Server, Mobility Management, Spanning Tree, Ports, Master Controller Mode, Network Time Protocol, QoS, and CDP. The main content area is titled 'Interfaces > Edit' and includes sections for General Information, Interface Address, Physical Information, Configuration, DHCP Information, and Access Control List. The 'Interface Address' section shows a VLAN Identifier of 145, IP Address of 172.17.148.2, Netmask of 255.255.252.0, and Gateway of 172.17.148.1. The 'Physical Information' section shows Port Number 1, Backup Port 0, and Active Port 1. The 'Configuration' section has a Quarantine checkbox. The 'DHCP Information' section shows a Primary DHCP Server of 172.17.148.1. The 'Access Control List' section has an ACL Name dropdown set to 'none'. A note at the bottom states: 'Note: Changing the Interface parameters causes the WLAs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

Kuva 2: WPA-verkkoliitännän asetukset

The screenshot shows the Cisco Controller configuration interface for the 'www-vlan' interface. The left sidebar contains a navigation menu with categories like General, Inventory, Interfaces, Network Routes, Internal DHCP Server, Mobility Management, Spanning Tree, Ports, Master Controller Mode, Network Time Protocol, QoS, and CDP. The main content area is titled 'Interfaces > Edit' and includes sections for General Information, Interface Address, Physical Information, Configuration, DHCP Information, and Access Control List. The 'Interface Address' section shows a VLAN Identifier of 144, IP Address of 172.17.144.2, Netmask of 255.255.252.0, and Gateway of 172.17.144.1. The 'Physical Information' section shows Port Number 1, Backup Port 0, and Active Port 1. The 'Configuration' section has a Quarantine checkbox. The 'DHCP Information' section shows a Primary DHCP Server of 172.17.144.1. The 'Access Control List' section has an ACL Name dropdown set to 'none'. A note at the bottom states: 'Note: Changing the Interface parameters causes the WLAs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

Kuva 3: WWW-verkkoliitännän asetukset

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		5 (18)

Virtual-verkkoliityntä onkin sitten hieman erikoisempi, sillä tämä on verkkoliityntä, johon WWW-autentikointi (captive portal, web authentication) ohjaa käyttäjän selaimen. Oletusarvoisesti tälle osoitteelle luodaan itseallekirjoitettu varmenne, joka on suositeltavaa korvata tunnetun varmentajan (esim. Thawten varmenteella). Tällaisen tunnetun varmentajan varmenteen käyttö kuitenkin vaatii, että virtual-verkkoliityntän osoitteella on ainakin paikallisessa nimipalvelussa IP-osoitetta vastaava nimi. Tässä esimerkissä kontrollerin ja sitä myötä päätelaitteiden käyttämään nimipalveluun konfiguroitiin nimi 'login.langatonyritys.fi' vastaamaan virtual-verkkoliityntän osoitetta 172.25.72.25 (kuva 4).

The screenshot shows the Cisco Controller web interface. The browser address bar displays 'https://172.16.144.221/screens/frameset.html'. The interface is titled 'Controller' and shows the 'Interfaces > Edit' configuration page. The 'General Information' section includes the interface name 'virtual' and MAC address '00:0b:85:46:5a:c0'. The 'Interface Address' section shows the IP address '172.25.72.25' and DNS host name 'login.langatonyritys.fi'. A note at the bottom of the configuration area reads: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

Kuva 4: virtual-verkkoliityntän konfiguraatio

WWW-autentikoinnin käyttö vaatii virtual-verkkoliityntän konfiguraation lisäksi myös varmenteen ja tätä vastaavan salaisen avaimen siirtämisen yhtenä pakettina kontrollerille. Tämä tehdään Security valikon alta löytyvästä Web Auth -asetuksista (Kuva 5), josta löytyy mahdollisuus siirtää TFTP:llä varmenne joltain toiselta palvelimelta kontrollerille. Varmenne ja salainen avain pitää olla paketoituna yhteen pakettiin ja suojattuna salalauseella ennen kuin kontrolleri hyväksyy ne asennettavaksi.

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		6 (18)

The screenshot shows the Cisco configuration interface for a Web Authentication Certificate. The left sidebar lists various security settings, with 'Web Auth' selected. The main content area displays the details of the 'Current Certificate' and provides options to download or regenerate it. The browser's address bar and status bar are also visible.

Current Certificate	
Name:	bsnSslWebauthCert
Type:	3rd Party
Serial Number:	55425547349853916755558113301879385336
Valid:	From 2008 Jan 27th, 00:00:00 GMT Until 2009 Jan 26th, 23:59:59 GMT
Subject Name:	C=FI, ST=Pirkanmaa, L=Tampere, O=Professia Oy, OU=Professia\, Langaton Tampere, CN=login.langatonyritys.fi
Issuer Name:	C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA, MAILTO=pr...
MD5 Fingerprint:	41:19:a2:7f:9e:ee:bf:3b:d7:18:e2:a0:1f:c1:29:3b
SHA1 Fingerprint:	ef:8c:da:be:49:69:a0:7f:df:00:8d:55:53:c9:05:e3:4b:97:0b:93

Download SSL Certificate *
** Controller must be rebooted for the new certificate to take effect.*

Download SSL Certificate From TFTP Server

Server IP Address	10.11.12.252
Maximum retries	10
Timeout (seconds)	6
Certificate File Path	/
Certificate File Name	

Kuva 5: varmenteen siirto

On tärkeää huomata, että vaikka Web Auth -asetuksista löytyvä Web Login Page sivu antaaakin mahdollisuuden ulkoistaa kirjautumissivu (Web Authentication Type External) vaikka Langattoman Tampereen pääsivuksi, tunnus ja salasana käyttäjän selaimesta syötetään aina takaisin kontrollerille, joka myös tällaisessa ulkoistetussa tapauksessa tarvitsee siis tunnetun varmentajan varmentaman varmenteen, jotta käyttäjän selain suostuu protestoimatta tunnuksen ja salasanan kontrollerille syöttämään.

Näin ollen kirjautumissivu voi sijaita joko kontrollerissa (Web Authentication Type Internal) tai se voidaan enemmän dynaamisuutta tarvittaessa siirtää erillisen WWW-palvelimen hoidettavaksi. Esimerkkikonfiguraatioissa (Kuva 6) kirjautumissivu on konfiguroitu tulemaan kontrollerilta.

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		7 (18)

The screenshot shows the Cisco Security Manager configuration page for the Web Login Page. The configuration includes:

- Web Authentication Type:** Internal (Default)
- Redirect URL after login:** (Empty field)
- Cisco Logo:** Show Hide
- Headline:** Wireless Tampere for Mindtrek/Openmind
- Message:**

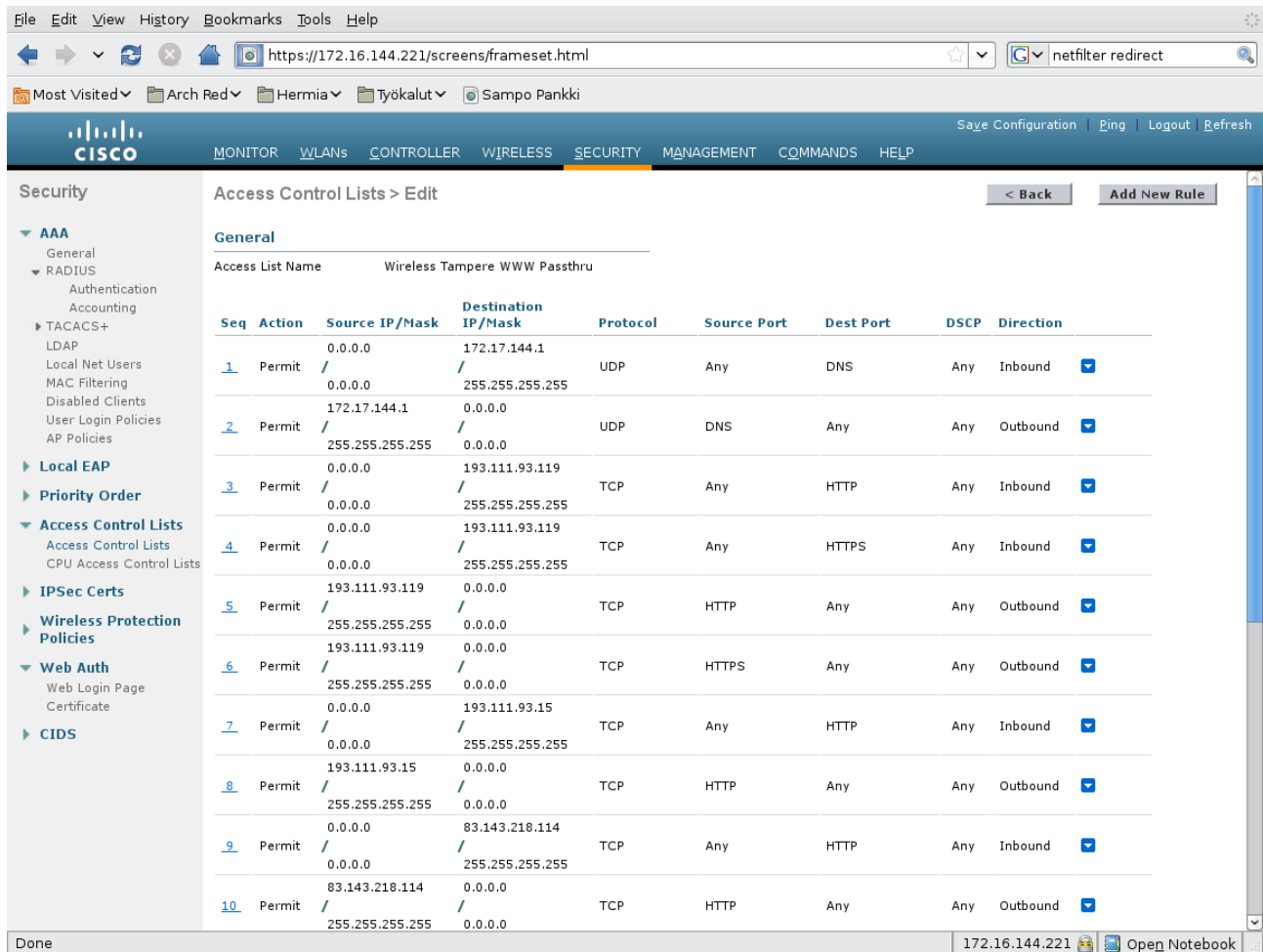
```

<p>
This is a Wireless Tampere WiFi community network, which is deployed
especially for <a href="http://www.mindtrek.org/">Mindtrek</a> / <a
href="http://www.mindtrek.org/openmind/">Openmind</a> conference.
The Wireless Tampere WiFi community network is available in several
locations (libraries, <a href="http://www.tampere.fi/">the Tampere
city</a> buildings, railway station etc.) and organisations (universities,
polytechnics etc.) here in Tampere and in the neighbouring cities and
municipalities.
</p>
<p>
Just look for WirelessTampere (Web Authentication) or LANGATON-WPA
(WPA Authentication) WiFi networks and you are able to access the
community WiFi network for free with your Mindtrek visitor credentials.
</p>
<p>
Wireless Tampere member organisation employees, Wireless Tampere
home and company users are able to utilise this network just like the
Wireless Tampere network in your home (organisation).
</p>
<p>

```

Kuva 6: WWW-kirjautumissivun asetukset

WWW-kirjautumissivua käytettäessä on mahdollista määritellä myös ilman autentikaatiota tavoitettavat palvelut, joita voivat olla esim tietyt WWW-palvelimet, SIP/VoIP-palvelimet jne. Näiden saavuttamiseksi täytyy kontrolleriin tehdä erillinen pääsylista (Access Control List = ACL), jossa määritellään ilman tunnistautumista käytössä olevat palvelut palomuurisääntöinä. Pääsylistaa määriteltäessä kannattaa muistaa suunnat: inbound on päätelaitteilta kontrollerin suuntaan, outbound on kontrollerilta päätelaitteiden suuntaan. Näiden sääntöjen lisäksi esimerkkikonfiguraatiota koostettaessa (kuva 7) havaittiin, että WWW-autentikointiin käytettävässä verkossa on myös erikseen sallittava DNS-liikenne DHCP:n mainostamalle DNS-palvelimelle/palvelimille ja takaisin (kaksi ensimmäistä sääntöä kuvassa 7). Vapaasti selattavassa olevia WWW-palvelimia varten tarvittiin kaksi sääntöä, HTTPS:n ollessa käytössä neljä.



The screenshot shows the Cisco configuration interface for 'Access Control Lists > Edit'. The configuration is for the 'Wireless Tampere WWW Passthru' access list. The table below represents the ACL rules shown in the interface:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	172.17.144.1 /	UDP	Any	DNS	Any	Inbound
2	Permit	172.17.144.1 /	0.0.0.0 /	UDP	DNS	Any	Any	Outbound
3	Permit	0.0.0.0 /	193.111.93.119 /	TCP	Any	HTTP	Any	Inbound
4	Permit	0.0.0.0 /	193.111.93.119 /	TCP	Any	HTTPS	Any	Inbound
5	Permit	193.111.93.119 /	0.0.0.0 /	TCP	HTTP	Any	Any	Outbound
6	Permit	255.255.255.255 /	0.0.0.0 /	TCP	HTTPS	Any	Any	Outbound
7	Permit	0.0.0.0 /	193.111.93.15 /	TCP	Any	HTTP	Any	Inbound
8	Permit	193.111.93.15 /	0.0.0.0 /	TCP	HTTP	Any	Any	Outbound
9	Permit	0.0.0.0 /	83.143.218.114 /	TCP	Any	HTTP	Any	Inbound
10	Permit	83.143.218.114 /	0.0.0.0 /	TCP	HTTP	Any	Any	Outbound

Kuva 7: Läpikäytilistan (ACL) määrittäminen

TUNNISTAUTUMISPALVELUIDEN KONFIGUROIINTI

Langattoman Tampereen tunnistautuminen pohjautuu RADIUS-palvelinhierarkian hyödyntämiseen sekä WWW- että WPA-tunnistautumista käytettäessä. Tätä varten kontrollerille täytyy kertoa RADIUS-palvelin/palvelimet, joiden kautta se voi liittyä mukaan yhteisöverkkoon. Tässä esimerkkikonfiguraatiossa konfiguroidaan kontrollerin tietoon Langattoman Tampereen yritystunnistuspalvelun palvelimet, jotka ovat tavoitettavissa Internetin yli operaattorista riippumatta. Kuvassa 8 kuvataan RADIUS-tunnistautumispalvelimen (authentication) asetukset ja kuvassa 9 RADIUS-tilastointipalvelimen (accounting) asetukset. Jaettu salaisuus kontrollerin ja yritystunnistuspalvelun määrytyy tukiasemia yritystunnistuspalveluun rekisteröitäessä ja se täytyy asettaa samaksi jokaiselle tukiasemalle.

The screenshot shows the Cisco configuration interface for RADIUS Authentication Servers. The left sidebar lists various configuration categories under 'Security', including AAA, RADIUS, TACACS+, Local EAP, Priority Order, Access Control Lists, IPsec Certs, Wireless Protection Policies, Web Auth, and CIDS. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays the following settings:

- Server Index: 2
- Server Address: 81.90.66.38
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Retransmit Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPsec: Enable

Buttons for '< Back' and 'Apply' are visible at the top right of the configuration area. The status bar at the bottom shows the IP address 172.16.144.221 and an 'Open Notebook' icon.

Kuva 8: RADIUS-tunnistuspalvelun asetukset

The screenshot shows the Cisco configuration interface for RADIUS Accounting Servers. The left sidebar is identical to the previous screenshot. The main content area is titled 'RADIUS Accounting Servers > Edit' and displays the following settings:

- Server Index: 2
- Server Address: 81.90.66.38
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Port Number: 1813
- Server Status: Enabled
- Retransmit Timeout: 2 seconds
- Network User: Enable
- IPsec: Enable

Buttons for '< Back' and 'Apply' are visible at the top right of the configuration area. The status bar at the bottom shows the IP address 172.16.144.221 and an 'Open Notebook' icon.

Kuva 9: RADIUS-tilastointipalvelimen asetukset

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		10 (18)

Langattoman Tampereen yritystunnistuspalvelun hyödyntäminen vaatii, että käytettävät tukiasemat rekisteröidään mukaan palveluun, ja että mahdollisesti käytetty kontrolleri osaa liittää RADIUS-viesteihin Called-Station-ID RADIUS-attribuutin, joka sisältää autentikoivan tukiaseman MAC-osoitteen. Käytettäessä Ciscon kontrolleria ja Langattoman Tampereen yritystunnistuspalvelua tämä tarkoittaa, että kaikkien alueeseen kuuluvien tukiasemien Base Radio Mac -osoite on rekisteröitävä Langattoman Tampereen yritystunnistuspalveluun samalla jaetulla salaisuudella, jolla kontrolleri yhdistettiin yritystunnistuspalvelun RADIUS-palvelimeen. Tukiasemien Base Radio Mac -osoitteet saadaan kontrollerista selville esimerkiksi kuvan 10 osoittamasta paikasta.

The screenshot shows the Cisco Wireless Controller configuration interface. The 'All APs > Details' page is open for AP001b.d561.5606. The 'General' tab is selected, displaying the following information:

- AP Name: AP001b.d561.5606
- Ethernet MAC Address: 00:1b:d5:61:56:06
- Base Radio MAC Address: 00:1c:0f:4c:8a:80
- Regulatory Domain: 802.11bg:-E 802.11a:-E
- Country Code: FI (Finland)
- AP IP Address: 10.11.12.245
- AP Static IP:
- AP ID: 0
- Admin Status: Enable
- AP Mode: local
- Mirror Mode: Disable
- Operational Status: REG
- Port Number: 1
- Cisco Discovery Protocol:
- MFP Frame Validation: (Global MFP Disabled)
- AP Group Name: --
- Location: default location
- Primary Controller Name:
- Secondary Controller Name:
- Tertiary Controller Name:

The 'Versions' tab shows:

- S/W Version: 4.1.185.0
- Boot Version: 12.3.8.0
- IOS Version: 12.4(3g)JA2
- Mini IOS Version: 3.0.51.0

The 'Inventory Information' tab shows:

- AP PID: AIR-LAP1131AG-E-K9
- AP VID: V01
- AP Serial Number: FCZ1122Q1C8
- AP Entity Name: Cisco AP
- AP Entity Description: Cisco Wireless Access Point
- AP Certificate Type: Manufacture Installed
- H-REAP Mode supported: Yes

The 'Power Over Ethernet Settings' tab shows:

- Pre-Standard State:
- Power Injector State:

Kuva 10: Base Radio MAC -osoite

Tukiasemien Base Radio MAC -osoitteet rekisteröidään Langattoman Tampereen yritystunnistuspalveluun WPA+WWW-kykyisinä tukiasemina. WWW-tunnistautumista varten on myös säädettävä Security → RADIUS → Authentication :in alta löytyvä Call Station ID Type asentoon AP MAC Address (kuva 11), jolloin tukiasema liittää WWW-autentikointia varten lähetettäviin RADIUS-viesteihin sen tukiaseman osoitteen, jota kautta päätelaite on verkkoon liittynyt. Toinen vaihtoehto on kääntää asetus asentoon System MAC Address, jolloin tukiasemien lisäksi Langattoman Tampereen yrityspalveluun on rekisteröitävä Controller → Inventory:sta löytyvä Burned-in MAC Address.

The screenshot shows the Cisco configuration interface for RADIUS Authentication Servers. The 'Call Station ID Type' is set to 'AP MAC Address'. The 'Credentials Caching' checkbox is unchecked. The 'Use AES Key Wrap' checkbox is also unchecked, with a note that it is designed for FIPS customers and requires a key wrap compliant RADIUS server. A table lists two RADIUS servers:

Network User	Management	Server Index	Server Address	Port	IPsec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	195.197.255.27	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	81.90.66.38	1812	Disabled	Enabled

Kuva 11: Call Station ID Type -asetus

WLAN-RADIOVERKKOJEN KONFIGUROINTI

RADIUS- ja muiden autentikaatioasetusten jälkeen voidaan aloittaa WLAN-radioverkkojen konfigurointi. Kuten VLANeja konfiguroitaessa, tännekin tulee erillinen WLAN-radioverkko WWW-tunnistautumiselle (WirelessTampere) ja toinen WPA-tunnistautumiselle (LANGATON-WPA) (Kuva 12).

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		12 (18)

The screenshot shows the Cisco WLAN configuration interface in a web browser. The browser address bar shows the URL `https://172.16.144.221/screens/frameWlan.html`. The interface has a navigation menu with options: MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The main content area displays a table of WLAN profiles.

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
Langaton Tampere (WPA)	1	LANGATON-WPA	Enabled	[WPA + WPA2][Auth(802.1X)]
Langaton Tampere (WWW)	2	WirelessTampere	Enabled	Web-Auth

Below the table, there is a note: ** WLAN IDs 9-16 will not be pushed to 11xx, 12xx and 13xx model APs.*

Kuva 12: WLAN-radioverkkojen konfigurointi

WPA-verkon (LANGATON-WPA) konfigurointi

WPA-verkon yleisessä konfiguroinnissa on huomattava valita asetuksista (kuva 13) se verkkoliityntä (interface), johon käyttäjät halutaan oletuksena pudottaa. Tässä tapauksessa kyseessä on wpa-vlan-verkkoliityntä. On myös mahdollista RADIUS-palvelimen ja kontrollerin yhteistyöllä sekä sopivalla konfiguraatiolla tiputtaa autentikoitunut käyttäjä esimerkiksi oman yrityksensä VLANiin suoraan, mutta tällaisen ratkaisun konfigurointi ei kuulu tämän oppaan alueeseen.

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		13 (18)

The screenshot shows the Cisco configuration interface for WLANs. The main content area is titled 'WLANs > Edit' and has tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'Security' tab is active, showing the following configuration:

- Profile Name: Langaton Tampere (WPA)
- WLAN SSID: LANGATON-WPA
- WLAN Status: Enabled
- Security Policies: **[WPA + WPA2][Auth(802.1X)]**
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface: wpa-vlan
- Broadcast SSID: Enabled

Below the configuration area, there are 'Foot Notes' with the following text:

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

The interface also shows a 'Done' status at the bottom left and a taskbar at the bottom right with the address '172.16.144.221' and an 'Open Notebook' icon.

Kuva 13: WPA-verkon yleisasetukset

Kaikki WPA-verkon turvallisuusasetukset ovat kerroksella 2 ja ne voidaan konfiguroida kuvien 14 ja 15 esimerkkien mukaan. Esimerkkikonfiguraation avulla saadaan aikaiseksi sekä WPA1 että WPA2 -tunnistautumista samassa WLAN-radioverkossa tukeva WLAN-verkko.

The screenshot shows the Cisco WLAN Controller configuration interface. The 'WLANs > Edit' page is open, with the 'Security' tab selected. Under the 'Layer 2' sub-tab, the 'WPA+WPA2 Parameters' section is visible. The 'WPA Policy' checkbox is checked. Under 'WPA Encryption', 'TKIP' is checked. Under 'WPA2 Policy', 'WPA2 Policy' is checked. Under 'WPA2 Encryption', 'AES' is checked. The 'Auth Key Mgmt' is set to '802.1X'. The '802.11 Data Encryption' section shows 'WEP' selected with a '104 bits' key size. The 'MMH Mode' and 'Key Permutation' checkboxes are unchecked. The 'Key Size' is 'not set', 'Key Index' is '1', and 'Key Format' is 'ASCII'. The 'Foot Notes' section contains five numbered notes regarding CKIP, Web Policy, H-REAP, client exclusion, and Client MFP.

Kuva 14: Kakkoskerroksen (Layer 2) asetukset 1/2

The screenshot shows the Cisco WLAN Controller configuration interface, continuing from the previous one. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'Static WEP Parameters' section shows '802.11 Data Encryption' with 'Current Key: 104 bits WEP Static Key (Key Index = 1)'. Below this, a table shows 'WEP' selected with 'not set' key size, '1' key index, and 'ASCII' key format. The 'Allow Shared Key Authentication' checkbox is unchecked. The 'CKIP Parameters' section shows '802.11 Data Encryption' with 'Current Key: 0 bits CKIP Key (Key Index = 0)'. The 'Foot Notes' section is identical to the previous screenshot.

Kuva 15: Kakkoskerroksen (Layer 2) asetukset 2/2

Kakkoskerroksen (Layer 2) asetusten lisäksi täytyy WPA-verkolle vielä määrittellä käytettävät RADIUS-palvelimet, jotka määritellään Security → AAA Servers -kohdassa (kuva 16).

The screenshot shows the Cisco WLAN configuration interface. The main content area is titled "WLANs > Edit" and has tabs for "General", "Security", "QoS", and "Advanced". Under the "Security" tab, there are sub-tabs for "Layer 2", "Layer 3", and "AAA Servers". The "AAA Servers" sub-tab is active, showing a section titled "Select AAA servers below to override use of default servers on this WLAN".

Under "AAA Servers", there are two main sections: "Radius Servers" and "LDAP Servers".

Radius Servers:

- Authentication Servers:**
 - Server 1: IP:81.90.66.38, Port:1812
 - Server 2: None
 - Server 3: None
- Accounting Servers:**
 - Enabled:
 - Server 1: IP:81.90.66.38, Port:1813
 - Server 2: None
 - Server 3: None

LDAP Servers:

- Server 1: None
- Server 2: None
- Server 3: None

Below the Radius Servers section, there is a "Local EAP Authentication" section with a checkbox for "Enabled" which is not checked.

At the bottom of the page, there are "Foot Notes":

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

Kuva 16: Käytettävien RADIUS-palvelimien määrittäminen

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		16 (18)

WWW-verkon (WirelessTampere) konfigurointi

Yleistasolla WWW-tunnistetun WLAN-verkon konfigurointi ei poikkea WPA-tunnistetun verkon asetuksista muuta kuin käytettävän verkkoliittynän/VLANin osalta (kuva 17).

The screenshot displays the Cisco WLAN configuration page for the 'Langaton Tampere (WWW)' profile. The 'Security' tab is active, showing the following settings:

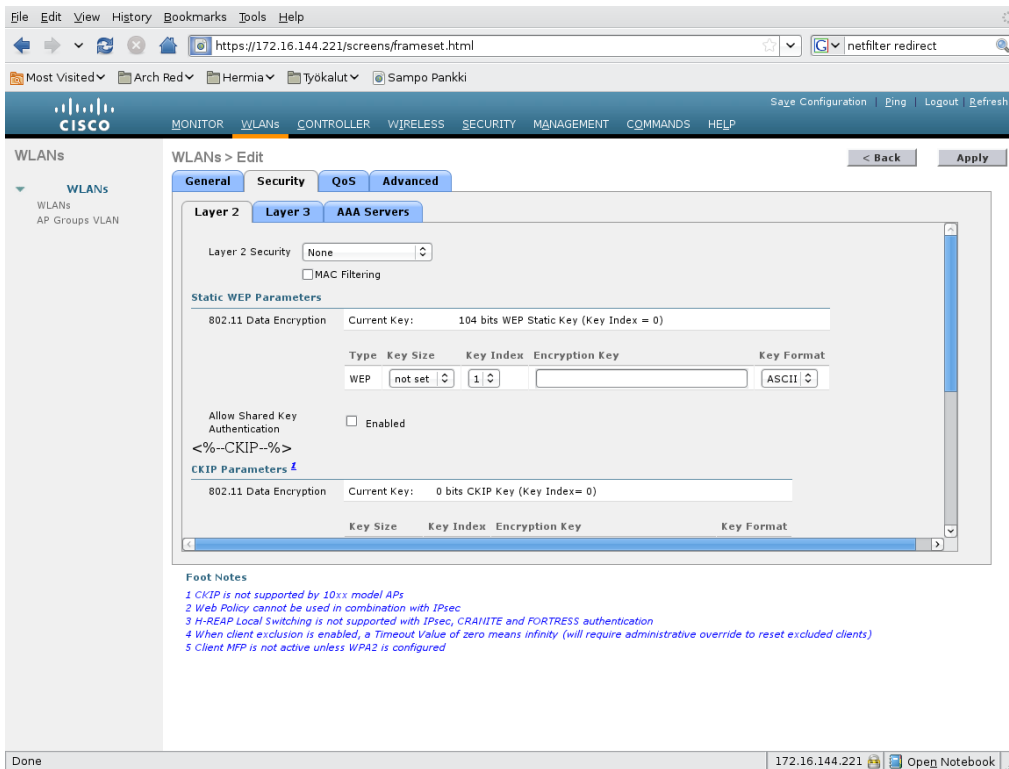
- Profile Name: Langaton Tampere (WWW)
- WLAN SSID: WirelessTampere
- WLAN Status: Enabled
- Security Policies: **Web-Auth**
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface: www-vlan
- Broadcast SSID: Enabled

Foot Notes:

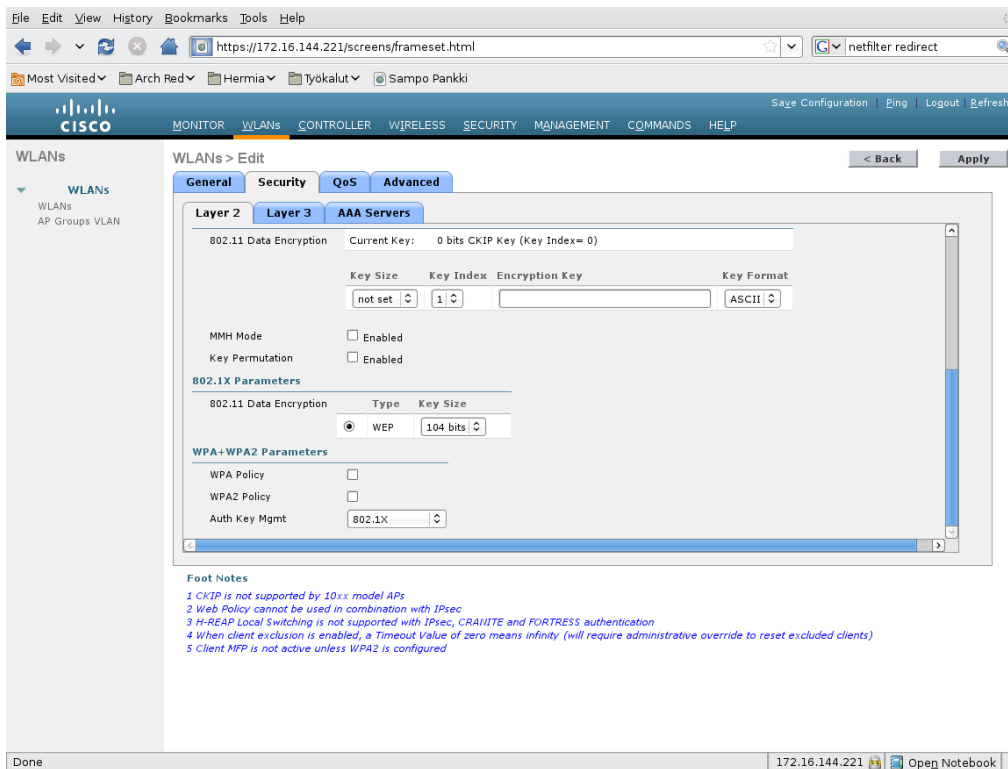
- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

Kuva 17: WWW-verkon yleisasetukset

Erot ovatkin sitten kakkos- ja kolmoskerroksen (Layer 2, Layer 3) konfiguraatiossa. Kakkoskerrokselta siivotaan pois kaikki tunnistaumisetukset (kuvat 18 ja 19).



Kuva 18: Kakkoskerroksen (Layer 2) asetukset 1/2



Kuva 19: Kakkoskerroksen (Layer 2) asetukset 2/2

Arch·Red	KÄYTTÖOHJE	JULKINEN
	Langaton Tampere: Cisco WLAN Controller konfigurointi	V1.0 15.10.2008
		18 (18)

Varsinaiset turvallisuusasetukset konfiguroidaan kolmoskerrokselle (Layer 3) kuvan 20 esimerkin mukaisesti. Kuvasta kannattaa huomioida Web Policy ja Preauthentication ACL -asetukset. Web Policyllä käännetään päälle WWW-autentikointi ja Preauthentication ACL:ään valittava pääsyylista (ACL) kertoo, mitä palveluita kontrollerin on päästettävä läpi ilman WWW-tunnistautumisen vaatimista.

The screenshot shows the Cisco WLAN configuration interface. The 'Layer 3 Security' dropdown is set to 'None', and the 'Web Policy' checkbox is checked. The 'Preauthentication ACL' dropdown is set to 'Wireless Tampere WWW Passthru'. The 'IPsec Parameters' section shows 'IPsec Authentication' as 'HMAC SHA1' and 'IPsec Encryption' as '3DES'. The 'IKE Authentication' section shows 'XAuth Pre-Shared Key' as the current setting. The 'Foot Notes' section contains five notes regarding CKIP, Web Policy, H-REAP, client exclusion, and MFP.

Kuva 20: Kolmoskerroksen (Layer 3) asetukset

Näiden lisäksi AAA Serversin asetukset määritellään samalla tavalla kuin aiemmin WPA-verkon konfiguraatiossa.

LISÄTIETOJA

Lisätietoja ja asiantuntijapalveluita Ciscon WLAN-järjestelmiin ja Langattomaan Tampereeseen liittyen saa muun muassa tämän oppaan kirjoittajilta osoitteesta:

Arch Red Oy
info@archred.fi
www.archred.fi