

# Documentation

C20/C2400 User Guide

A31003-W1050-U100-2-7619

Communication for the open minded

Siemens Enterprise Communications  
[www.siemens.com/open](http://www.siemens.com/open)

**SIEMENS**

## Communication for the open minded

Siemens Enterprise Communications  
[www.siemens.com/open](http://www.siemens.com/open)

Copyright © Siemens Enterprise  
Communications GmbH & Co. KG 2007  
Hofmannstr. 51, D-81359 München

Reference No.: A31003-W1050-U100-2-7619

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Subject to availability. Right of modification reserved. The trademarks used are owned by Siemens Enterprise Communications GmbH & Co. KG or their respective owners.

# Contents

<b>1 About this Guide</b> .....	<b>9</b>
1.1 Who should use this guide .....	9
1.2 What is in this guide .....	9
1.3 Formatting conventions .....	10
1.4 Documentation feedback .....	11
1.5 Safety Information .....	11
1.6 Sicherheitshinweise .....	13
1.7 Consignes de sécurité .....	14
<b>2 Overview of the Controller, Access Points and Convergence Software solution</b> .....	<b>17</b>
2.1 Conventional wireless LANS .....	17
2.2 Elements of the Controller, Access Points and Convergence Software solution .....	19
2.3 Controller, Access Points and Convergence Software and your network .....	22
2.3.1 Network traffic flow .....	24
2.3.2 Network security .....	25
2.3.2.1 Authentication .....	26
2.3.2.2 Privacy .....	27
2.3.3 Virtual Network Services .....	27
2.3.4 Static routing and routing protocols .....	28
2.3.5 Packet filtering policy .....	28
2.3.6 Mobility and roaming .....	29
2.3.7 Network availability .....	29
2.3.8 Quality of Service (QoS) .....	30
2.4 System Configuration Overview .....	30
<b>3 Configuring the HiPath Wireless Controller</b> .....	<b>33</b>
3.1 System configuration overview .....	34
3.2 Performing the first time setup of the HiPath Wireless Controller .....	37
3.2.1 Accessing the HiPath Wireless Controller .....	37
3.2.1.1 Changing the administrator password .....	41
3.2.2 Connecting the HiPath Wireless Controller to your enterprise network .....	41
3.2.3 Applying the product license key .....	41
3.2.4 Setting up the data ports .....	42
3.2.5 Setting up static routes .....	47
3.2.6 Setting up OSPF Routing .....	49
3.2.7 Filtering at the interface level .....	52
3.2.8 Built-in port-based exception filters .....	52
3.2.9 User defined port-based exception filters .....	54
3.3 Completing the system configuration .....	56
3.4 Ongoing Operations of the Controller, Access Points and Convergence Software .....	56
<b>4 Configuring the Wireless AP</b> .....	<b>57</b>
4.1 Wireless AP overview .....	57
4.1.1 HiPath Wireless AP .....	58
4.1.1.1 HiPath Wireless AP radios .....	58
4.1.2 HiPath Wireless Outdoor AP .....	60
4.1.3 HiPath Wireless 802.11n AP .....	61
4.1.3.1 HiPath Wireless 802.11n AP's radios .....	64

## Contents

4.1.4	Wireless AP international licensing	65
4.1.5	Wireless AP default IP address and first-time configuration	66
4.1.6	Assigning static IP address to Wireless AP	67
4.1.6.1	Enabling/Disabling telnet access and setting up new Telnet Access Password via the controller's user interface	70
4.2	Discovery and registration overview	71
4.2.1	Wireless AP discovery	72
4.2.2	Registration after discovery	73
4.2.2.1	Default Wireless AP configuration	74
4.2.3	Understanding the Wireless AP LED status	74
4.2.3.1	HiPath Wireless AP LED status	74
4.2.3.2	HiPath Wireless Outdoor AP LED status	78
4.2.3.3	HiPath Wireless 802.11n AP LED status	80
4.3	Configuring the Wireless APs for the first time	82
4.3.1	Defining properties for the discovery process	83
4.3.2	Connecting the Wireless AP to a power source and initiating the discovery and registration process	86
4.4	Adding and registering a Wireless AP manually	86
4.5	Configuring Wireless AP settings	87
4.5.1	Modifying a Wireless AP's status	88
4.5.2	Modifying a Wireless AP's properties	90
4.5.3	Modifying Wireless AP radio properties	95
4.5.3.1	Modifying <i>Wireless 802.11n AP 3610/3620 radio properties</i>	96
4.5.3.2	Modifying <i>Wireless AP 2610/2620 radio properties</i>	106
4.5.4	Setting up the Wireless AP using static configuration	114
4.5.5	Setting up 802.1x authentication for a Wireless AP	117
4.5.5.1	Configuring 802.1x PEAP authentication	119
4.5.5.2	Configuring 802.1x EAP-TLS authentication	120
4.5.5.3	Viewing 802.1x credentials	123
4.5.5.4	Deleting 802.1x credentials	124
4.5.6	Setting up 802.1x authentication for Wireless APs using Multi-edit	125
4.5.7	Configuring the default Wireless AP settings	128
4.6	Modifying a Wireless AP's properties based on a default AP configuration	138
4.7	Modifying the Wireless AP's default setting using the Copy to Defaults feature	139
4.8	Configuring Wireless APs simultaneously	139
4.9	Configuring an AP as a sensor	141
4.10	Performing Wireless AP software maintenance	142
<b>5</b>	<b>Virtual Network Services</b>	<b>147</b>
5.1	VNS overview	147
5.2	Setting up a VNS checklist	148
5.3	Topology of a VNS	150
5.4	RF assignment for a VNS	152
5.5	Authentication for a VNS	152
5.5.1	Authentication with SSID network assignment	152
5.5.2	Authentication with AAA (802.1x) network assignment	153
5.6	Filtering for a VNS	154
5.6.1	Final filter rule	155
5.6.2	Filtering sequence	155
5.7	Data protection on a VNS—WEP and WPA	156
5.8	VNS global settings	157
5.9	Setting up a new VNS	161
<b>6</b>	<b>Virtual Network configuration</b>	<b>163</b>

6.1 VNS Types	163
6.2 Creating a new VNS name	164
6.3 Topology for a VNS	164
6.3.1 Configuring topology for a VNS for Captive Portal	165
6.3.1.1 Defining session timeout parameters	166
6.3.1.2 Enabling management traffic	167
6.3.1.3 Enabling third-party APs on a VNS	168
6.3.1.4 Defining a next hop route and OSPF advertisement for a VNS	169
6.3.1.5 Defining the IP address for the VNS (for the DHCP server on the controller)	170
6.3.1.6 Modifying time limits for IP assignments	171
6.3.1.7 Setting the name server configuration	172
6.3.1.8 Using a DHCP relay for the VNS	172
6.3.2 Configuring topology for a VNS for AAA	173
6.3.3 Saving your topology properties	174
6.4 Assigning Wireless AP radios to a VNS	174
6.5 Deleting a VNS	176
6.6 Authentication for a VNS	176
6.6.1 Vendor Specific Attributes	177
6.6.2 Defining authentication for a VNS for Captive Portal	178
6.6.2.1 Defining the RADIUS server priority for RADIUS redundancy	181
6.6.2.2 Configuring Captive Portal for internal or external authentication	183
6.6.3 Defining authentication for a VNS for AAA	186
6.6.4 Defining MAC-based authentication for a VNS	189
6.7 Defining accounting methods for a VNS	191
6.8 Defining RADIUS filter policy for VNSs and VNS groups	193
6.9 Configuring filtering rules for a VNS	194
6.9.1 Filtering rules for an exception filter	195
6.9.2 Defining non-authenticated filters	197
6.9.2.1 Non-authenticated filter examples	200
6.9.3 Filtering rules for a filter ID group	201
6.9.3.1 Filtering rules by filter ID examples	203
6.9.4 Filtering rules for a default filter	203
6.9.4.1 Default filter examples	204
6.9.4.2 Filtering rules for an AAA child group VNS	205
6.9.4.3 Filtering rules between two wireless devices	205
6.10 Enabling multicast for a VNS	206
6.11 Configuring privacy for a VNS	208
6.11.1 Privacy for a VNS for Captive Portal	208
6.11.2 Privacy for a VNS for AAA	211
6.11.2.1 Dynamic WEP privacy for an AAA VNS	213
6.11.2.2 Wi-Fi Protected Access (WPA v1 and WPA v2) Privacy for an AAA VNS	213
6.11.2.3 Key Management Options	215
6.12 Defining a VNS with no authentication	218
6.13 Defining priority level and service class for VNS traffic	219
6.13.1 Defining the service class for the VNS	219
6.13.2 Configuring the priority override	220
6.14 Working with Quality of Service (QoS)	220
6.14.1 QoS modes	221
6.15 Configuring the QoS policy on a VNS	223
6.16 Bridging traffic locally	227
6.17 Wireless Distribution System	229
6.17.1 Simple WDS configuration	229

## Contents

6.17.2	Wireless Repeater configuration	230
6.17.3	Wireless Bridge configuration	231
6.17.4	Examples of deployment	231
6.17.5	WDS VNS	231
6.17.6	Key features of WDS	234
6.17.6.1	Tree-like topology	234
6.17.6.2	Radio Channels	236
6.17.6.3	Multi-root WDS topology	236
6.17.6.4	Automatic discovery of parent and backup parent Wireless APs	237
6.17.6.5	Link security	237
6.17.7	Deploying the WDS system	238
6.17.7.1	Connecting the WDS Wireless APs to the enterprise network for discovery and registration	239
6.17.7.2	Configuring the WDS Wireless APs through the HiPath Wireless Controller	239
6.17.7.3	Assigning the Satellite Wireless APs' radios to the network VNSs	246
6.17.7.4	Connecting the WDS Wireless APs to the enterprise network for provisioning	248
6.17.7.5	Moving the WDS Wireless APs to the target location	248
6.17.8	Changing the pre-shared key in WDS VNS	249
<b>7</b>	<b>Availability, mobility, and controller functionality</b>	<b>251</b>
7.1	Availability overview	251
7.1.1	Availability prerequisites	253
7.1.2	Viewing the Wireless AP availability display	256
7.1.3	Viewing SLP activity	257
7.1.4	Events and actions during a failover	257
7.2	Mobility manager	259
7.2.1	Displays for the mobility manager	264
7.3	Defining management users	264
7.4	Configuring network time	266
7.5	Configuring Check Point event logging	268
7.5.1	ELA Management Station events	270
7.6	Enabling SNMP	270
7.6.1	MIB support	271
7.6.2	Enabling SNMP on the HiPath Wireless Controller	272
7.7	Using controller utilities	273
7.8	Configuring Web session timeouts	275
<b>8</b>	<b>Working with third-party APs</b>	<b>277</b>
<b>9</b>	<b>Working with the Mitigator</b>	<b>281</b>
9.1	Mitigator overview	281
9.2	Enabling the Analysis and data collector engines	282
9.3	Running Mitigator scans	283
9.4	Analysis engine overview	286
9.5	Working with Mitigator scan results	287
9.6	Working with friendly APs	289
9.7	Maintaining the Mitigator list of APs	290
9.8	Viewing the Scanner Status report	292
<b>10</b>	<b>Working with reports and displays</b>	<b>293</b>
10.1	Viewing the displays	293
10.1.1	Viewing the Wireless AP availability display	295
10.1.2	Viewing statistics for Wireless APs	295
10.1.3	Viewing the System Information and Manufacturing Information displays	299
10.1.4	Viewing displays for the mobility manager	300

10.2 Viewing reports .....	303
<b>11 Performing system maintenance.....</b>	<b>309</b>
11.1 Performing Wireless AP client management .....	309
11.1.1 Disassociating a client .....	309
11.1.2 Blacklisting a client .....	310
11.2 Resetting the Wireless APs to their factory default settings.....	313
11.2.1 Resetting the HiPath Wireless AP to its factory default settings.....	314
11.2.1.1 Resetting the HiPath Wireless Outdoor AP to its factory default settings .....	315
11.2.1.2 Resetting the HiPath Wireless 802.11n AP to its factory default settings .....	316
11.3 Performing system maintenance tasks .....	317
11.4 Performing HiPath Wireless Controller software maintenance .....	320
11.4.1 Working with a flash memory card .....	321
11.4.2 Upgrading HiPath Wireless Controller software .....	324
11.4.2.1 Upgrading using a local or remote image file .....	325
11.4.2.2 Modifying a scheduled software upgrade .....	332
11.4.2.3 Deleting a software image .....	333
11.4.3 Backing up the HiPath Wireless Controller database .....	333
11.4.3.1 Uploading a backup to an FTP server .....	334
11.4.3.2 Scheduling a backup .....	335
11.4.3.3 Deleting a backup .....	337
11.4.4 Restoring the HiPath Wireless Controller database .....	337
11.4.5 Upgrading a HiPath Wireless Controller using SFTP .....	339
11.4.6 Maintaining the HiPath Wireless Controller product license keys.....	340
11.4.7 Configuring the HiPath Wireless Controller for interaction with the HiPath Wireless Manager .....	341
11.5 Working with system logs, trace messages, and audits.....	342
11.5.1 Logs, traces, audits, and DHCP messages .....	342
11.5.1.1 Working with logs .....	343
11.5.1.2 Working with trace messages .....	347
11.5.1.3 Working with audit messages .....	350
11.5.1.4 Working with DHCP messages .....	351
11.5.1.5 Working with software upgrade messages .....	351
11.5.1.6 Working with restore/import messages .....	353
<b>12 Glossary.....</b>	<b>355</b>
12.1 Networking terms and abbreviations .....	355
12.2 Controller, Access Points and Convergence Software terms and abbreviations.....	368
<b>A HiPath Wireless Controller's physical description .....</b>	<b>371</b>
A.1 HiPath Wireless C2400 Controller front panel.....	371
A.2 LED states and Seven Segment Display (SSD) codes .....	373
A.3 HiPath Wireless C2400 Controller back panel.....	375
A.4 HiPath Wireless C20 Controller.....	375
<b>B Regulatory information .....</b>	<b>379</b>
B.1 HiPath Wireless Controller C20/C2400 .....	380
B.2 Wireless APs 26XX and 36XX.....	381
<b>C optiPoint WL2 Configuration.....</b>	<b>409</b>
C.1 optiPoint WL2 wireless telephone configuration .....	409
C.2 HiPath Wireless Controller configuration.....	413
<b>D SpectraLink Wireless Telephones .....</b>	<b>419</b>
D.1 Network Topology .....	419
D.2 Configuring HiPath Wireless Controller for SpectraLink Telephones .....	420

## Contents



# 1 About this Guide

This guide describes how to install, configure, and manage the Controller, Access Points and Convergence Software software. This guide is also available as an online help system.

**To access the online help system:**

1. In the HiPath Wireless Assistant Main Menu bar, click **Help**. The **About HiPath Wireless Assistant** page is displayed.
2. In the left pane, click **Controller Documentation**. The online help system is launched.

## 1.1 Who should use this guide

This guide is a reference for system administrators who install and manage the HiPath Wireless Controller, Access Points and Convergence Software system.

Any administrator performing tasks described in this guide must have an account with administrative privileges.

## 1.2 What is in this guide

This guide contains the following:

- [Chapter 1, “About this Guide”](#), describes the target audience and content of the guide, the formatting conventions used in it, and how to provide feedback on the guide.
- [Chapter 2, “Overview of the Controller, Access Points and Convergence Software solution”](#), provides an overview of the product, its features and functionality.
- [Chapter 3, “Configuring the HiPath Wireless Controller”](#), describes how to perform the installation, first time setup and configuration of the HiPath Wireless Controller, as well as configuring the data ports and defining routing.
- [Chapter 4, “Configuring the Wireless AP”](#), describes how to install the Wireless AP, how it discovers and registers with the HiPath Wireless Controller, how to view and modify the radio configuration, and how to enable Dynamic Radio Frequency Management.
- [Chapter 5, “Virtual Network Services”](#), provides an overview of Virtual Network Services (VNS), the mechanism by which the HiPath Wireless Controller, Access Points and Convergence Software controls and manages network access.

## About this Guide

### Formatting conventions

- [Chapter 6, “Virtual Network configuration”](#), provides detailed instructions in how to configure a VNS, its topology, authentication, accounting, RADIUS policy, multicast, filtering and privacy. Both Captive Portal and AAA types of VNS are described.
- [Chapter 7, “Availability, mobility, and controller functionality”](#), describes how to set up the features that provide availability in the event of a controller failover, and mobility for a wireless device user.
- [Chapter 8, “Working with third-party APs”](#), describes how to use the Controller, Access Points and Convergence Software features with third-party wireless access points.
- [Chapter 9, “Working with the Mitigator”](#), explains the security tool that scans for, detects and reports on rogue APs.
- [Chapter 11, “Performing system maintenance”](#), describes maintenance activities, such as software upgrades on both the HiPath Wireless Controller and the Wireless AP. This chapter also includes information on the logs, traces, reports and displays available.
- [Chapter 12, “Glossary”](#), contains a list of terms and definitions for the HiPath Wireless Controller and the Wireless AP as well as standard industry terms used in this guide.
- [Appendix A, “HiPath Wireless Controller’s physical description”](#), describes the physical description and LED states of the HiPath Wireless Controller.
- [Appendix B, “Regulatory information”](#), provides the regulatory information for the HiPath C20/C2400 Wireless LAN Controllers and the HiPath Wireless Access Points (APs).
- [Appendix C, “optiPoint WL2 Configuration”](#), describes how to configure the WL2 phone.
- [Appendix D, “SpectraLink Wireless Telephones”](#), describes how to configure NetLink Wireless Telephones and WLAN infrastructure products.

## 1.3 Formatting conventions

The HiPath Wireless Controller, Access Points and Convergence Software documentation uses the following formatting conventions to make it easier to find information and follow procedures:

- **Bold** text is used to identify components of the management interface, such as menu items and section of pages, as well as the names of buttons and text boxes.

For example: Click **Logout**.

- `Monospace` font is used in code examples and to indicate text that you type.

For example: Type `https://<hwc-address>[:mgmt-port]`

- The following notes are used to draw your attention to additional information:

---

**Note:** Notes identify useful information, such as reminders, tips, or other ways to perform a task.

---

---

**Caution:** Cautionary notes identify essential information, which if ignored can adversely affect the operation of your equipment or software.

---

---

**Warning:** Warning notes identify essential information, which if ignored can lead to personal injury or harm.

---

## 1.4 Documentation feedback

If you have any problems using this document, please contact your next level of support:

- Siemens employees should contact the interactive Customer Engagement Team (i-CET).
- Customers should contact the Siemens Customer Support Center.

When you call, please have the following information ready. This will help us to identify the document that you are referring to.

- Title: HiPath Wireless Controller, Access Points and Convergence Software V5 R1 C20/C2400 User Guide
- Part Number: A31003-W1050-U100-2-7619

## 1.5 Safety Information

### Dangers

- Replace the power cable immediately if it shows any sign of damage.
- Replace any damaged safety equipment (covers, labels and protective cables) immediately.
- Use only original accessories or components approved for the system. Failure to observe these instructions may damage the equipment or even violate safety and EMC regulations.

## About this Guide

### Safety Information

- Only authorized Siemens service personnel are permitted to service the system.

#### Warnings

- This device must not be connected to a LAN segment with outdoor wiring.
- Ensure that all cables are run correctly to avoid strain.
- Replace the power supply adapter immediately if it shows any sign of damage.
- Disconnect all power before working near power supplies unless otherwise instructed by a maintenance procedure.
- Exercise caution when servicing hot swappable HiPath Wireless Controller components: power supplies or fans. Rotating fans can cause serious personal injury.
- This unit may have more than one power supply cord. To avoid electrical shock, disconnect all power supply cords before servicing. In the case of unit failure of one of the power supply modules, the module can be replaced without interruption of power to the HiPath Wireless Controller. However, this procedure must be carried out with caution. Wear gloves to avoid contact with the module, which will be extremely hot.
- There is a risk of explosion if a lithium battery is not correctly replaced. The lithium battery must be replaced only by an identical battery or one recommended by the manufacturer.
- Always dispose of lithium batteries properly.
- Do not attempt to lift objects that you think are too heavy for you.

#### Cautions

- Check the nominal voltage set for the equipment (operating instructions and type plate). High voltages capable of causing shock are used in this equipment. Exercise caution when measuring high voltages and when servicing cards, panels, and boards while the system is powered on.
- Only use tools and equipment that are in perfect condition. Do not use equipment with visible damage.
- To protect electrostatic sensitive devices (ESD), wear a wristband before carrying out any work on hardware.
- Lay cables so as to prevent any risk of them being damaged or causing accidents, such as tripping.

## 1.6 Sicherheitshinweise

### **Gefahrenhinweise**

- Sollte das Netzkabel Anzeichen von Beschädigungen aufweisen, tauschen Sie es sofort aus.
- Tauschen Sie beschädigte Sicherheitsausrüstungen (Abdeckungen, Typenschilder und Schutzkabel) sofort aus.
- Verwenden Sie ausschließlich Originalzubehör oder systemspezifisch zugelassene Komponenten. Die Nichtbeachtung dieser Hinweise kann zur Beschädigung der Ausrüstung oder zur Verletzung von Sicherheits- und EMV-Vorschriften führen.
- Das System darf nur von autorisiertem Siemens-Servicepersonal gewartet werden.

### **Warnhinweise**

- Dieses Gerät darf nicht über Außenverdrahtung an ein LAN-Segment angeschlossen werden.
- Stellen Sie sicher, dass alle Kabel korrekt geführt werden, um Zugbelastung zu vermeiden.
- Sollte das Netzteil Anzeichen von Beschädigung aufweisen, tauschen Sie es sofort aus.
- Trennen Sie alle Stromverbindungen, bevor Sie Arbeiten im Bereich der Stromversorgung vornehmen, sofern dies nicht für eine Wartungsprozedur anders verlangt wird.
- Gehen Sie vorsichtig vor, wenn Sie an Hotswap-fähigen HiPath Wireless Controller-Komponenten (Stromversorgungen oder Lüftern) Servicearbeiten durchführen. Rotierende Lüfter können ernsthafte Verletzungen verursachen.
- Dieses Gerät ist möglicherweise über mehr als ein Netzkabel angeschlossen. Um die Gefahr eines elektrischen Schlages zu vermeiden, sollten Sie vor Durchführung von Servicearbeiten alle Netzkabel trennen. Falls eines der Stromversorgungsmodule ausfällt, kann es ausgetauscht werden, ohne die Stromversorgung zum HiPath Wireless Controller zu unterbrechen. Bei dieser Prozedur ist jedoch mit Vorsicht vorzugehen. Das Modul kann extrem heiß sein. Tragen Sie Handschuhe, um Verbrennungen zu vermeiden.
- Bei unsachgemäßem Austausch der Lithium-Batterie besteht Explosionsgefahr. Die Lithium-Batterie darf nur durch identische oder vom Händler empfohlene Typen ersetzt werden.
- Achten Sie bei Lithium-Batterien auf die ordnungsgemäße Entsorgung.
- Versuchen Sie niemals, ohne Hilfe schwere Gegenstände zu heben.

## About this Guide

### Consignes de sécurité

#### Vorsichtshinweise

- Überprüfen Sie die für die Ausrüstung festgelegte Nennspannung (Bedienungsanleitung und Typenschild). Diese Ausrüstung arbeitet mit Hochspannung, die mit der Gefahr eines elektrischen Schlages verbunden ist. Gehen Sie mit großer Vorsicht vor, wenn Sie bei eingeschaltetem System Hochspannungen messen oder Karten, Schalttafeln und Baugruppen warten.
- Verwenden Sie nur Werkzeuge und Ausrüstung in einwandfreiem Zustand. Verwenden Sie keine Ausrüstung mit sichtbaren Beschädigungen.
- Tragen Sie bei Arbeiten an Hardwarekomponenten ein Armband, um elektrostatisch gefährdete Bauelemente (EGB) vor Beschädigungen zu schützen.
- Verlegen Sie Leitungen so, dass sie keine Unfallquelle (Stolpergefahr) bilden und nicht beschädigt werden.

## 1.7 Consignes de sécurité

#### Dangers

- Si le cordon de raccordement au secteur est endommagé, remplacez-le immédiatement.
- Remplacez sans délai les équipements de sécurité endommagés (caches, étiquettes et conducteurs de protection).
- Utilisez uniquement les accessoires d'origine ou les modules agréés spécifiques au système. Dans le cas contraire, vous risquez d'endommager l'installation ou d'enfreindre les consignes en matière de sécurité et de compatibilité électromagnétique.
- Seul le personnel de service Siemens est autorisé à maintenir/réparer le système.

#### Avertissements

- Cet appareil ne doit pas être connecté à un segment de LAN à l'aide d'un câblage extérieur.
- Vérifiez que tous les câbles fonctionnent correctement pour éviter une contrainte excessive.
- Si l'adaptateur d'alimentation présente des dommages, remplacez-le immédiatement.
- Coupez toujours l'alimentation avant de travailler sur les alimentations électriques, sauf si la procédure de maintenance mentionne le contraire.

- Prenez toutes les précautions nécessaires lors de l'entretien/réparations des modules du HiPath Wireless Controller pouvant être branchés à chaud : alimentations électriques ou ventilateurs. Les ventilateurs rotatifs peuvent provoquer des blessures graves.
- Cette unité peut avoir plusieurs cordons d'alimentation. Pour éviter tout choc électrique, débranchez tous les cordons d'alimentation avant de procéder à la maintenance. En cas de panne d'un des modules d'alimentation, le module défectueux peut être changé sans éteindre le HiPath Wireless Controller. Toutefois, ce remplacement doit être effectué avec précautions. Portez des gants pour éviter de toucher le module qui peut être très chaud.
- Le remplacement non conforme de la batterie au lithium peut provoquer une explosion. Remplacez la batterie au lithium par un modèle identique ou par un modèle recommandé par le revendeur.
- Sa mise au rebut doit être conforme aux prescriptions en vigueur.
- N'essayez jamais de soulever des objets qui risquent d'être trop lourds pour vous.

#### **Précautions**

- Contrôlez la tension nominale paramétrée sur l'installation (voir le mode d'emploi et la plaque signalétique). Des tensions élevées pouvant entraîner des chocs électriques sont utilisées dans cet équipement. Lorsque le système est sous tension, prenez toutes les précautions nécessaires lors de la mesure des hautes tensions et de l'entretien/réparation des cartes, des panneaux, des plaques.
- N'utilisez que des appareils et des outils en parfait état. Ne mettez jamais en service des appareils présentant des dommages visibles.
- Pour protéger les dispositifs sensibles à l'électricité statique, portez un bracelet antistatique lors du travail sur le matériel.
- Acheminez les câbles de manière à ce qu'ils ne puissent pas être endommagés et qu'ils ne constituent pas une source de danger (par exemple, en provoquant la chute de personnes).

## About this Guide

*Consignes de sécurité*



## 2 Overview of the Controller, Access Points and Convergence Software solution

This chapter describes HiPath Controller, Access Points and Convergence Software concepts, including:

- [Conventional wireless LANS](#)
- [Elements of the Controller, Access Points and Convergence Software solution](#)
- [Controller, Access Points and Convergence Software and your network](#)
- [System Configuration Overview](#)

The next generation of Siemens wireless networking devices provides a truly scalable WLAN solution. Siemens Wireless APs are fit access points controlled through a sophisticated network device, the HiPath Wireless Controller. This solution provides the security and manageability required by enterprises and service providers.

The Controller, Access Points and Convergence Software system is a highly scalable Wireless Local Area Network (WLAN) solution developed by Siemens. Based on a third generation WLAN topology, the Controller, Access Points and Convergence Software system makes wireless practical for service providers as well as medium and large-scale enterprises.

The Controller, Access Points and Convergence Software system provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points.

This chapter provides an overview of the fundamental principles of the Controller, Access Points and Convergence Software system.

### 2.1 Conventional wireless LANS

Wireless communication between multiple computers requires that each computer is equipped with a receiver/transmitter—a WLAN Network Interface Card (NIC)—capable of exchanging digital information over a common radio frequency. This is called an ad hoc network configuration. An ad hoc network configuration allows wireless devices to communicate together. This setup is defined as an independent basic service set (IBSS).

An alternative to the ad hoc configuration is the use of an access point. This may be a dedicated hardware bridge or a computer running special software. Computers and other wireless devices communicate with each other through this

## Overview of the Controller, Access Points and Convergence Software solution

### Conventional wireless LANS

access point. The 802.11 standard defines access point communications as devices that allow wireless devices to communicate with a distribution system. This setup is defined as a basic service set (BSS) or infrastructure network.

To allow the wireless devices to communicate with computers on a wired network, the access points must be connected to the wired network providing access to the networked computers. This topology is called bridging. With bridging, security and management scalability is often a concern.

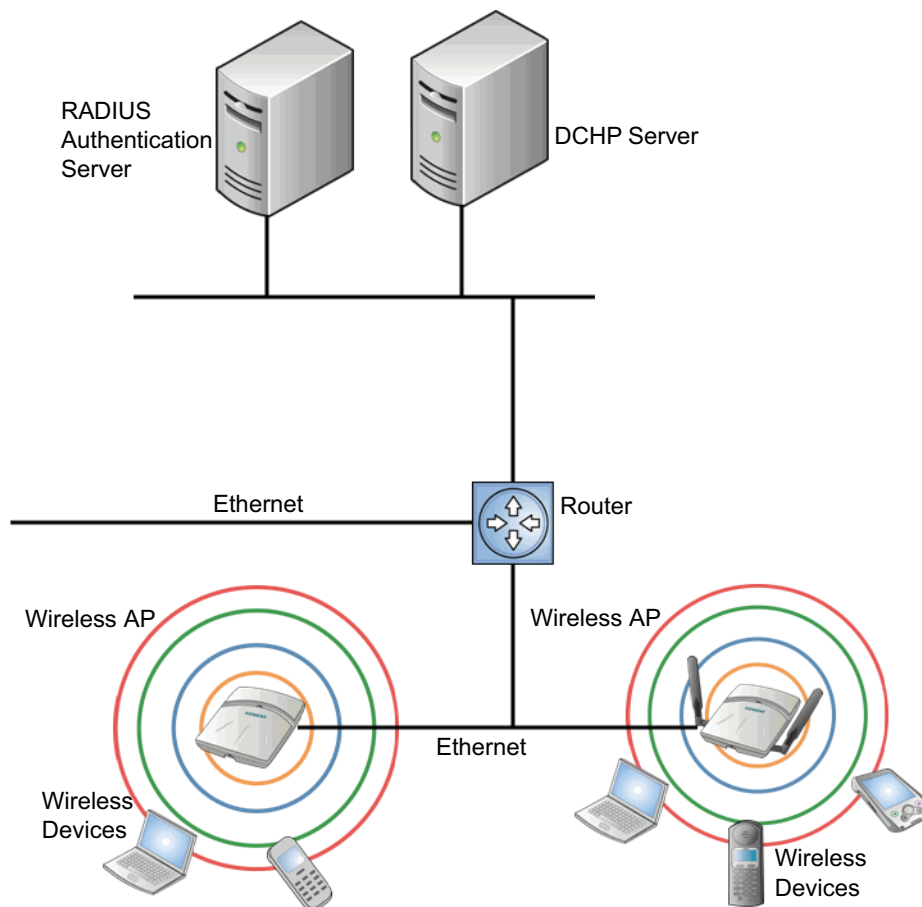


Figure 1 Standard wireless network solution example

The wireless devices and the wired networks communicate with each other using standard networking protocols and addressing schemes. Most commonly, Internet Protocol (IP) addressing is used.

## **2.2 Elements of the Controller, Access Points and Convergence Software solution**

The Controller, Access Points and Convergence Software solution consists of two devices:

- HiPath Wireless Controller
- Wireless APs

This architecture allows a single HiPath Wireless Controller to control many Wireless APs, making the administration and management of large networks much easier.

There can be several HiPath Wireless Controllers in the network, each with a set of registered Wireless APs. The HiPath Wireless Controllers can also act as backups to each other, providing stable network availability.

In addition to the HiPath Wireless Controllers and Wireless APs, the solution requires three other components, all of which are standard for enterprise and service provider networks:

- RADIUS Server (Remote Access Dial-In User Service) or other authentication server
- DHCP Server (Dynamic Host Configuration Protocol)
- SLP (Service Location Protocol)

## Overview of the Controller, Access Points and Convergence Software solution

### Elements of the Controller, Access Points and Convergence Software solution

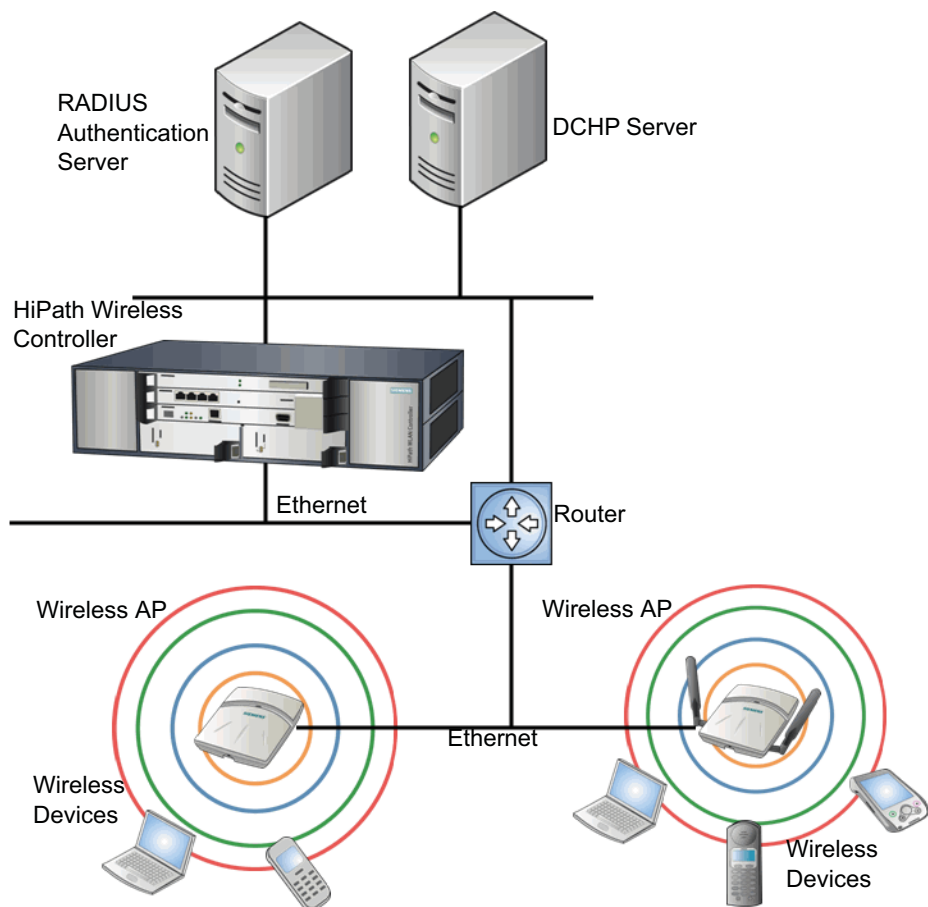


Figure 2 Siemens HiPath Wireless Controller solution

As illustrated in Figure 2, the HiPath Wireless Controller appears to the existing network as if it were an access point, but in fact one HiPath Wireless Controller controls many Wireless APs. The HiPath Wireless Controller has built-in capabilities to recognize and manage the Wireless APs. The HiPath Wireless Controller:

- Activates the Wireless APs
- Enables Wireless APs to receive wireless traffic from wireless devices
- Processes the data traffic from the Wireless APs
- Forwards or routes the processed data traffic out to the network
- Authenticates requests and applies access policies

Simplifying the Wireless APs makes them cost-effective, easy to manage, and easy to deploy. Putting control on an intelligent centralized HiPath Wireless Controller enables:

- Centralized configuration, management, reporting, and maintenance
- High security

## Overview of the Controller, Access Points and Convergence Software solution

### *Elements of the Controller, Access Points and Convergence Software solution*

- Flexibility to suit enterprise
- Scalable and resilient deployments with a few HiPath Wireless Controllers controlling hundreds of Wireless APs

The HiPath Wireless Controller, Access Points and Convergence Software system:

- **Scales up to Enterprise capacity** – One HiPath Wireless Controller C20 controls as many as 32 Wireless APs and one HiPath Wireless Controller C2400 controls as many as 200 Wireless APs. In turn each Wireless AP can handle up to 254 wireless devices, with each radio supporting a maximum of 128. With additional HiPath Wireless Controllers, the number of wireless devices the solution can support can reach into the thousands.
- **Integrates with existing network** – A HiPath Wireless Controller can be added to an existing enterprise network as a new network device, greatly enhancing its capability without interfering with existing functionality. Integration of the HiPath Wireless Controllers and Wireless APs does not require any reconfiguration of the existing infrastructure (for example, VLANs).
- **Offers centralized management and control** – An administrator accesses the HiPath Wireless Controller in its centralized location to monitor and administer the entire wireless network. From the HiPath Wireless Controller the administrator can recognize, configure, and manage the Wireless APs and distribute new software releases.
- **Provides easy deployment of Wireless APs** – The initial configuration of the Wireless APs on the centralized HiPath Wireless Controller can be done with an automatic “discovery” technique. For more information, see [Section 4.2, “Discovery and registration overview”](#), on page 71.
- **Provides security via user authentication** – Uses existing authentication (AAA) servers to authenticate and authorize users.
- **Provides security via filters and privileges** – Uses virtual networking techniques to create separate virtual networks with defined authentication and billing services, access policies, and privileges.
- **Supports seamless mobility and roaming** – Supports seamless roaming of a wireless device from one Wireless AP to another on the same HiPath Wireless Controller or on a different HiPath Wireless Controller.
- **Integrates third-party access points** – Uses a combination of network routing and authentication techniques.
- **Prevents rogue devices** – Unauthorized access points are detected and identified as harmless or dangerous rogue APs.

## Overview of the Controller, Access Points and Convergence Software solution

### *Controller, Access Points and Convergence Software and your network*

- **Provides accounting services** – Logs wireless user sessions, user group activity, and other activity reporting, enabling the generation of consolidated billing records.
- **Offers troubleshooting capability** – Logs system and session activity and provides reports to aid in troubleshooting analysis.
- **Offers dynamic RF management** – Automatically selects channels and adjusts Radio Frequency (RF) signal propagation and power levels without user intervention.

## 2.3 Controller, Access Points and Convergence Software and your network

This section is a summary of the components of the Controller, Access Points and Convergence Software solution on your enterprise network. The following are described in detail in this guide, unless otherwise stated:

- **HiPath Wireless Controller** – A rack-mountable network device that provides centralized control over all access points (both Wireless APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
- **Wireless AP** – A wireless LAN fit access point (IEEE 802.11) that communicates only with a HiPath Wireless Controller. A Wireless AP can also be configured as a sensor, which monitors and interdicts intrusions by rogue APs and rogue clients.
- **HiPath Wireless Manager** – An optional component of the solution, the HiPath Wireless Manager monitors the performance and health of the wireless network. The HiPath Wireless Manager is particularly valuable for installations that incorporate more than one HiPath Wireless Controller. For more information, see the *HiPath Wireless Manager User Guide*.
- **RADIUS Server** (Remote Access Dial-In User Service) (RFC2865), or other authentication server – An authentication server that assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users in either 802.1x or Captive Portal security modes. The RADIUS Server system can be set up for certain standard attributes, such as filter ID, and for the Vendor Specific Attributes (VSAs). In addition, Radius Disconnect (RFC3576) which permits dynamic adjustment of user policy (user disconnect) is supported.
- **DHCP Server** (Dynamic Host Configuration Protocol) (RFC2131) – A server that assigns IP addresses, gateways, and subnet masks dynamically. IP address assignment for clients can be done by the DHCP server internal to the HiPath Wireless Controller, or by existing servers using DHCP relay. It is also used by the Wireless APs to discover the location of the HiPath Wireless

## Overview of the Controller, Access Points and Convergence Software solution

### *Controller, Access Points and Convergence Software and your network*

Controller during the initial registration process. For SLP, DHCP should have Option 78 enabled. Option 78 specifies the location of one or more SLP Directory Agents.

- **Service Location Protocol (SLP)** (SLP RFC2608) – Client applications are User Agents and services that are advertised by a Service Agent. In larger installations, a Directory Agent collects information from Service Agents and creates a central repository. The Siemens solution relies on registering “siemens” as an SLP Service Agent.
- **Domain Name Server (DNS)** – A server used as an alternate mechanism (if present on the enterprise network) for the automatic discovery process. Controller, Access Points and Convergence Software relies on the DNS for Layer 3 deployments and for static configuration of Wireless APs. The controller can be registered in DNS, to provide DNS assisted AP discovery.
- **Web Authentication Server** – A server that can be used for external Captive Portal and external authentication. The HiPath Wireless Controller has an internal Captive portal presentation page, which allows Web authentication (Web redirection) to take place without the need for an external Captive Portal server.
- **RADIUS Accounting Server** (Remote Access Dial-In User Service) (RFC2866) – A server that is required if RADIUS Accounting is enabled.
- **Simple Network Management Protocol (SNMP)** – A Manager Server that is required if forwarding SNMP messages is enabled.
- **Check Point Server** (Check Point Event Logging API) – A server for security event logging that is required if a firewall application is enabled. Checkpoint ELA certification for OPSEC is provided.
- **Network infrastructure** – The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple HiPath Wireless Controllers for the following features to operate successfully:
  - Availability
  - Mobility
  - Mitigator for detection of rogue access pointsSome features also require the definition of static routes.
- **Web Browser** – A browser provides access to the HiPath Wireless Controller Management user interface to configure the Controller, Access Points and Convergence Software.
- **SSH Enabled Device** – A device that supports Secure Shell (SSH) is used for remote (IP) shell access to the system.

## Overview of the Controller, Access Points and Convergence Software solution

### Controller, Access Points and Convergence Software and your network

- **Zone Integrity** – The Zone integrity server enhances network security by ensuring clients accessing your network are compliant with your security policies before gaining access. Zone Integrity Release 5 is supported.
- **HiPath HiGuard** – Provides continuous active intrusion detection and prevention capabilities. For more information, see the HiPath HiGuard documentation.

### 2.3.1 Network traffic flow

Figure 3 illustrates a simple configuration with a single HiPath Wireless Controller and two Wireless APs, each supporting a wireless device. A RADIUS server on the network provides authentication, and a DHCP server is used by the Wireless APs to discover the location of the HiPath Wireless Controller during the initial registration process. Network inter-connectivity is provided by the infrastructure routing and switching devices.

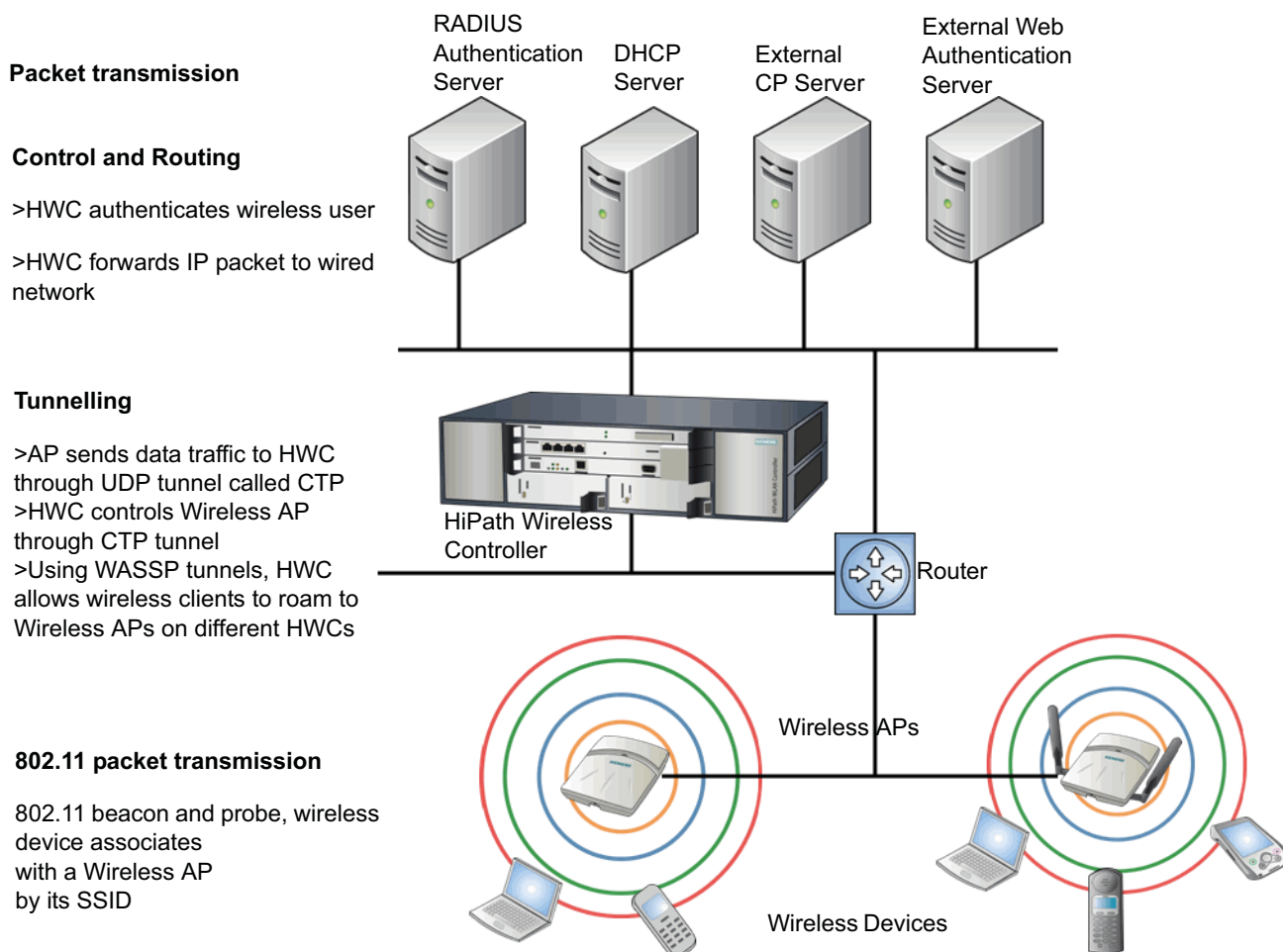


Figure 3 Traffic Flow diagram



## Overview of the Controller, Access Points and Convergence Software solution

*Controller, Access Points and Convergence Software and your network*

Each wireless device sends IP packets in the 802.11 standard to the Wireless AP. The Wireless AP uses a UDP (User Datagram Protocol) based tunnelling protocol to encapsulate the packets and forward them to the HiPath Wireless Controller. In a typical configuration, access points can be configured to locally bridge traffic (to a configured VLAN) directly at their network point of attachment. The HiPath Wireless Controller decapsulates the packets and routes these to destinations on the network.

The HiPath Wireless Controller functions like a standard router, except that it is configured to route only network traffic associated with wireless connected users. The HiPath Wireless Controller can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred.

### 2.3.2 Network security

The Controller, Access Points and Convergence Software system provides features and functionality to control network access. These are based on standard wireless network security practices.

Current wireless network security methods provide protection. These methods include:

- Shared Key authentication that relies on Wired Equivalent Privacy (WEP) keys
- Open System that relies on Service Set Identifiers (SSIDs)
- 802.1x that is compliant with Wi-Fi Protected Access (WPA)
- Captive Portal based on Secure Sockets Layer (SSL) protocol

The Controller, Access Points and Convergence Software system provides the centralized mechanism by which the corresponding security parameters are configured for a group of APs.

- Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the 802.11b standard
- Wi-Fi Protected Access version 1 (WPA1™) with Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access version 2 (WPA2™) with Advanced Encryption Standard (AES) and Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP)

#### HiPath HiGuard

The HiPath HiGuard solution provides network security, including:

- **Monitoring** – 2.4 GHz and 5 GHz, all channels association activity

## Overview of the Controller, Access Points and Convergence Software solution

### *Controller, Access Points and Convergence Software and your network*

- **Identifying** – Detect all Wi-Fi activity and correlate information from multiple sensors
- **Auto-Classifying** – Limit user intervention to maximize the protection of all devices from all threats
- **Preventing** – Automatically block threats through dedicated sensors to prevent any impact on the service level
- **Visualizing** – Visualize measured coverage for service, detection, and prevention
- **Locating** – Position rogue APs and clients on the floor-plan for permanent removal

### 2.3.2.1 Authentication

The HiPath Wireless Controller relies on a RADIUS server, or authentication server, on the enterprise network to provide the authentication information (whether the user is to be allowed or denied access to the network). A RADIUS client is implemented to interact with infrastructure RADIUS servers.

The HiPath Wireless Controller provides authentication using:

- Captive Portal – a browser-based mechanism that forces users to a Web page
- RADIUS (using IEEE 802.1x)

The 802.1x mechanism is a standard for authentication developed within the 802.11 standard. This mechanism is implemented at the wireless Port, blocking all data traffic between the wireless device and the network until authentication is complete. Authentication by 802.1x standard uses Extensible Authentication Protocol (EAP) for the message exchange between the HiPath Wireless Controller and the RADIUS server.

When 802.1x is used for authentication, the HiPath Wireless Controller provides the capability to dynamically assign per-wireless-device WEP keys (called per session WEP keys in 802.11). Or in the case of WPA, the HiPath Wireless Controller is not involved in key assignment. Instead, the controller is involved in the path between RADIUS server and the user to negotiate the appropriate set of keys. With WPA2 the material exchange produces a Pairwise Master Key which is used by the AP and the user to derive their temporal keys. (The keys change over time.)

In the Controller, Access Points and Convergence Software, a RADIUS redundancy feature is provided, where you can define a failover RADIUS server (up to 2 servers) in the event that the active RADIUS server fails.

### 2.3.2.2 Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

Controller, Access Points and Convergence Software supports the Wired Equivalent Privacy (WEP) standard common to conventional access points.

It also provides Wi-Fi Protected Access version 1 (WPA v.1) encryption, based on Pairwise Master Key (PMK) and Temporal Key Integrity Protocol (TKIP). The most secure encryption mechanism is WPA version 2, using Advanced Encryption Standard (AES).

### 2.3.3 Virtual Network Services

Virtual Network Services (VNS) provide a versatile method of mapping wireless networks to the topology of an existing wired network.

When you set up VNS on the HiPath Wireless Controller you are defining subnets for groups of wireless users. The VNS definition provides the binding between VNS IP topology configuration (Routing, DHCP policy) and the RF configuration parameters that advertise and control network access (SSID, Privacy policy: WEP and WPA). This technique enables policies and authentication to be applied to the groups of wireless users on a VNS, as well as the collecting of accounting information on user sessions that can be used for billing.

When a VNS is set up on the HiPath Wireless Controller:

- One or more Wireless APs (by radio) are associated with it
- A range of IP addresses is set aside for the HiPath Wireless Controller's DHCP server to assign to wireless devices

If routing protocol is enabled, the HiPath Wireless Controller advertises the VNS as a routable network segment to the wired network and routes traffic between the wireless devices and the wired network. The HiPath Wireless Controller C20/C2400 also supports VLAN-bridged assignment for VNSs. This allows the controller to directly bridge the set of wireless devices associated with a VNS directly to a specified core VLAN. The HiPath Wireless Controller can support the following:

- C2400 – Up to 64 VNSs
- C20 – Up to 8 VNSs

The Wireless AP radios can be assigned to each of the configured VNSs in a system. Each Wireless AP can be the subject of 16 VNS assignments — 8 VNS assignments per radio — which corresponds to the number of SSIDs it can support. Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

### 2.3.4 Static routing and routing protocols

Routing can be used on the HiPath Wireless Controller to support the VNS definitions. Through the user interface you can configure routing on the HiPath Wireless Controller to use one of the following routing techniques:

- **Static routes** – Use static routes to set the default route of a HiPath Wireless Controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- **Open Shortest Path First (OSPF, version 2) (RFC2328)** – Use OSPF to allow the HiPath Wireless Controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route definition and OSPF dynamic learning can be combined, but a static route definition will take precedence over dynamic rules.
- **Next-hop routing** – Use next-hop routing to specify a unique gateway to which traffic on a VNS is forwarded. Defining a next-hop for a VNS forces all the traffic in the VNS to be forwarded to the indicated network device, bypassing any routing definitions of the controller's route table.

### 2.3.5 Packet filtering policy

Policy refers to the rules that allow different groups of users access to the network. The Controller, Access Points and Convergence Software system can link authorized users to user groups. These user groups then can be confined to predefined portions of the network.

In the Controller, Access Points and Convergence Software system, network access policy is carried out by means of packet filtering within a VNS.

In the HiPath Wireless Controller user interface, you set up a packet filtering policy by defining a set of hierarchical rules that allow or deny traffic to specific IP addresses, IP address ranges, or service ports. The sequence and hierarchy of these filtering rules must be carefully designed based on your enterprise user access plan.

The authentication technique selected determines how filtering is carried out:

- If authentication is by SSID and Captive Portal, a non-authenticated filter allows all users to get as far as the Captive Portal Web page, where logon authentication occurs. When authentication is returned, then filters are applied, based on user ID and permissions.
- If authentication is by AAA (802.1x), users have logged on and have been authenticated before being assigned an IP address. When authentication is completed, the authenticated filter is assigned by default unless a more user-

## Overview of the Controller, Access Points and Convergence Software solution

### *Controller, Access Points and Convergence Software and your network*

specific filter is returned or indicated by the authentication mechanism. The characteristics and level of access for a filter are controlled and defined by the system administrator.

### **2.3.6 Mobility and roaming**

In typical configurations that are not HiPath Wireless, APs are setup as bridges that bridge wireless traffic to the local subnet. In bridging configurations, the user obtains an IP address from the same subnet as the AP. If the user roams within APs on the same subnet, it is able to keep using the same IP address. However, if the user roams to another AP outside of that subnet, its IP address is no longer valid. The user's client device must recognize that the IP address it has is no longer valid and re-negotiate a new one on the new subnet. The protocol does not mandate any action on the user. The recovery procedure is entirely client dependent. Some clients automatically attempt to obtain a new address on roam (which affects roaming latency), while others will hold on to their IP address. This loss of IP address continuity seriously affects the client's experience in the network, because in some cases it can take minutes for a new address to be negotiated.

The Controller, Access Points and Convergence Software solution centralizes the user's network point of presence, therefore abstracting and decoupling the user's IP address assignment from that of the APs location subnet. That means that the user is able to roam across any AP without losing its own IP address, regardless of the subnet on which the serving APs are deployed.

In addition, a HiPath Wireless Controller can learn about other HiPath Wireless Controllers on the network and then exchange client session information. This enables a wireless device user to roam seamlessly between different Wireless APs on different HiPath Wireless Controllers.

### **2.3.7 Network availability**

The Controller, Access Points and Convergence Software provides availability against Wireless AP outages, HiPath Wireless Controller outages, and even network outages. The HiPath Wireless Controller (C20/C2400 platforms) in a VLAN bridged VNS can potentially allow the user to retain the IP address in a failover scenario, if the VNS/VLAN is common to both controllers. For example, availability is provided by defining a paired controller configuration by which each peer can act as the backup controller for the other's APs. APs in one controller are allowed to failover and register with the alternate controller.

If a HiPath Wireless Controller fails, all of its associated Wireless APs can automatically switch over to another HiPath Wireless Controller that has been defined as the secondary or backup HiPath Wireless Controller. If the AP reboots, the original HiPath Wireless Controller is restored. The original HiPath Wireless

## Overview of the Controller, Access Points and Convergence Software solution

### System Configuration Overview

Controller is restored if it is active. However, active APs will continue to be attached to the failover controller until the administrator releases them back to the original home controller.

### 2.3.8 Quality of Service (QoS)

Controller, Access Points and Convergence Software provides advanced Quality of Service (QoS) management to provide better network traffic flow. Such techniques include:

- **WMM (Wi-Fi Multimedia)** – WMM is enabled per VNS. The HiPath Wireless Controller provides centralized management of these AP features. For devices with WMM enabled, the standard provides multimedia enhancements for audio, video, and voice applications. WMM shortens the time between transmitting packets for higher priority traffic. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service) or DSCP (Diffserv Codepoint)** – The **ToS/DSCP** field in the IP header of a frame indicates the priority and QoS for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header—this is referred to as Adaptive QoS.

Quality of Service (QoS) management is also provided by:

- Assigning high priority to an SSID (configurable)
- Adaptive QoS (automatic)
- Support for legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic (configurable)

## 2.4 System Configuration Overview

To set up and configure the HiPath Wireless Controller and Wireless APs, follow these steps:

1. **First time Setup** – Perform “First Time Setup” of the HiPath Wireless Controller on the physical network to modify the Management Port IP address for the enterprise network.
2. **Product Key** – Apply a Product Key file, for licensing purposes. If no Product Key is enabled, the HiPath Wireless Controller functions with some features enabled in demonstration mode. Not all features are enabled in this mode. For example, mobility is not enabled and cannot be used.

3. Data Port Setup – Set up the HiPath Wireless Controller on the network by configuring the physical data ports and their function as “host port”, “router port”, or “3rd party AP port”.
4. Routing Setup – Configure static routes and OSPF parameters for any port defined as a router port, if appropriate to the network.
5. Wireless AP Initial Setup – Connect the Wireless APs to the HiPath Wireless Controller. They will automatically begin the Discovery of the HiPath Wireless Controller, based on factors that include:

- Their Registration mode (on the **Wireless AP Registration** page)
- The enterprise network services that will support the discovery process

The default AP configuration allows for a definition of a default configuration template, whereby APs automatically receive complete configuration. For typical deployments where all APs are to all have the same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including VNS assignment) upon initial registration with the HiPath Wireless Controller.

6. Wireless AP Configuration – Modify properties or settings of the Wireless AP, if applicable.
7. Virtual Network Services (VNS) Setup – Set up one or more virtual subnetworks on the HiPath Wireless Controller. For each VNS, configure the following:
  - **Topology** – Configure the VNS.
  - **RF** – Assign the Wireless APs’ radios to the VNS.
  - **Authentication and Accounting** – Configure the authentication method for the wireless device user and enable the accounting method.
  - **RAD Policy** – Define filter ID values and VNS Groups
  - **Filtering** – Define filtering rules to control network access
  - **Multicast** – Define groups of IP addresses for multicast traffic
  - **Privacy** – Select and configure the wireless security method on the VNS.
  - **QoS Policy** – Configure the Qos Policy.

**Overview of the Controller, Access Points and Convergence Software solution**  
*System Configuration Overview*



### 3 Configuring the HiPath Wireless Controller

This chapter introduces the HiPath Wireless Controller and describes the steps involved in its initial configuration and setup, including:

- [System configuration overview](#)
- [Performing the first time setup of the HiPath Wireless Controller](#)
- [Completing the system configuration](#)
- [Ongoing Operations of the Controller, Access Points and Convergence Software](#)

The HiPath Wireless Controller is a network device designed to integrate with an existing wired Local Area Network (LAN). The rack-mountable HiPath Wireless Controller provides centralized management, network access, and routing to wireless devices that use Wireless APs to access the network. It can also be configured to handle data traffic from third-party access points.

The HiPath Wireless Controller provides the following functionality:

- Controls and configures Wireless APs, providing centralized management
- Authenticates wireless devices that contact a Wireless AP
- Assigns each wireless device to a VNS when it connects
- Routes traffic from wireless devices, using VNS, to the wired network
- Applies filtering policies to the wireless device session
- Provides session logging and accounting capability

**HiPath Wireless Controller product family and license:**

The HiPath Wireless Controller is available in the following product families:

HiPath Wireless Controller Model Number	Specifications
C20 (Office license)	<ul style="list-style-type: none"> <li>• Two GigE ports supporting up to 32 Wireless APs</li> <li>• One management port (10/100 Base T)</li> <li>• One console port (DB9 serial)</li> <li>• One USB Server Port</li> <li>• Power supply standard (R)</li> </ul>
C2400 (Campus license)	<ul style="list-style-type: none"> <li>• Four GigE ports supporting up to 100 Wireless APs</li> <li>• One management port (10/100 BaseT)</li> <li>• One console port (DB9 serial)</li> <li>• Redundant dual power supply unit</li> </ul>

Table 1 HiPath Wireless Controller product families

## Configuring the HiPath Wireless Controller

### System configuration overview

HiPath Wireless Controller Model Number	Specifications
C2400 (Enterprise license)	<ul style="list-style-type: none"><li>• Four GigE ports supporting up to 100 Wireless APs</li><li>• One management port (10/100 BaseT)</li><li>• One console port (DB9 serial)</li><li>• Redundant dual power supply unit</li></ul>

Table 1 HiPath Wireless Controller product families

## 3.1 System configuration overview

The following section provides a high-level overview of the steps involved in the initial configuration of your system:

### Step 1 – Before you begin configuration

Research the type of WLAN deployment that is required.

### Step 2 – Preparing the network

Ensure relevant DHCP servers and RADIUS servers (if applicable) are available and configured.

### Step 3 – Installing the hardware

Install the HiPath Wireless Controller C20/C2400. For more information, see the following:

- *HiPath Wireless Controller, Access Points and Convergence Software Controller C2400 Installation Instructions.*
- *HiPath Wireless Controller, Access Points and Convergence Software Controller C20 Installation Instructions*

---

**Note:** The connection of a separate protective earth wire at the terminal on the rear side of the HiPath Wireless Controller C20 is optional.

---

### Step 4 – Performing the first time setup

Perform the first time Setup of the HiPath Wireless Controller on the physical network, which includes configuring the physical port IP:

- Configure the default IP address to be the relevant subnet point of attachment to the existing network. The default IP address is 10.0.#.1.
- Setup the routing protocol table.
- Configure the time zone, and then restart the HiPath Wireless Controller. Because changing the time zone requires restarting the HiPath Wireless Controller, it is recommended that you configure the time zone during the

initial installation and configuration of the HiPath Wireless Controller to avoid network interruptions. For more information, see [Section 7.4, “Configuring network time”](#), on page 266.

- To configure a physical port to attach to a VLAN, define the VLAN as part of the IP address assignment.

### Applying the product license key

Apply a product license key file. If a product license key is not applied, the HiPath Wireless Controller functions with some features enabled in demonstration mode. Not all features are enabled in demonstration mode. For example, mobility is not enabled and cannot be used.

---

**Caution:** Whenever the licensed region changes on the HiPath Wireless Controller, all Wireless APs are changed to **Auto Channel Select** to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost.

Installing the new license key before upgrading will prevent the HiPath Wireless Controller from changing the licensed region, and in addition, manually configured channel settings will be maintained. For more information, see [Section 11.4, “Performing HiPath Wireless Controller software maintenance”](#), on page 320.

---

### Configuring for remote access

In addition, the first time setup also involves configuring for remote access, which includes:

- Setting up an administration station (laptop) on subnet 192.168.10.0/24. By default, the controller's interface is configured with static IP 192.168.10.1.
- Configuring the system management interface.
- Configuring the data interfaces.

Set up the HiPath Wireless Controller on the network by configuring the physical data ports and their function as “host port”, “router port”, or “3rd party AP port”.

- Configure the routing table.

Configure static routes or OSPF parameters for any port defined as a router port, if appropriate to the network.

For more information, see [Section 3.2, “Performing the first time setup of the HiPath Wireless Controller”](#), on page 37.

## Configuring the HiPath Wireless Controller

### System configuration overview

#### Step 5 – Configuring the VNS

Research and then configure the traffic topologies your network must support. Set up one or more virtual subnetworks on the HiPath Wireless Controller. For each VNS, configure the following:

- **Topology** – Configure the VNS.
- **RF** – Assign the Wireless APs' radios to the VNS.
- **Authentication and Accounting** – Configure the authentication method for the wireless device user and enable the accounting method. The authentication and accounting configuration is optional. It only applies to Captive Portal or AAA VNSs.
- **RAD Policy** – Define filter ID values and VNS Groups. This configuration is optional.
- **Filtering** – Define filtering rules to control network access
- **Multicast** – Define groups of IP addresses for multicast traffic. This configuration is optional. By default, the multicast feature is disabled.
- **Privacy** – Select and configure the wireless security method on the VNS.
- **QoS Policy** – Configure the Qos Policy.

For more information, see [Chapter 5, “Virtual Network Services”](#).

#### Step 6 – Registering and assigning APs to the VNS

Deploy Wireless APs to their corresponding network locations. Connect the Wireless APs to the HiPath Wireless Controller. Once the Wireless APs are powered on, they automatically begin the Discovery process of the HiPath Wireless Controller, based on factors that include:

- Their Registration mode (on the **Wireless AP Registration** page)
- The enterprise network services that will support the discovery process

A new feature available in the 4.0 release is a default AP configuration. The default AP configuration allows for a definition of a default configuration template, whereby APs automatically receive complete configuration. For typical deployments where all APs are to all have same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including VNS assignment) upon initial registration with the HiPath Wireless Controller. If applicable, modify the properties or settings of the Wireless APs.

For more information, see [Chapter 4, “Configuring the Wireless AP”](#).

#### Step 7 – Confirming the AP firmware version

Confirm the latest firmware version is loaded. For more information, see [Section 4.10, “Performing Wireless AP software maintenance”](#), on page 142.

## 3.2 Performing the first time setup of the HiPath Wireless Controller

Before you can connect the HiPath Wireless Controller to the enterprise network, you must change the IP address of the HiPath Wireless Controller management port from its factory default to the IP address suitable for your enterprise network. Access the HiPath Wireless Controller by one of two methods:

- Use a device supporting VT100 emulation, attached to the DB9 serial port (COM1 port) of the HiPath Wireless Controller via a cross-over (null modem) cable. Use the Command Line Interface (CLI) commands. For more information, see the *HiPath Wireless Controller, Access Points and Convergence Software CLI Reference Guide*.
- Use a laptop computer with a Web browser. Connect the supplied cross-over Ethernet cable between the laptop and management Ethernet port of the HiPath Wireless Controller. Follow the steps below.

### 3.2.1 Accessing the HiPath Wireless Controller

1. Statically assign an unused IP address in the 192.168.10.0/24 subnet for the Ethernet port of the computer. For example, 192.168.10.205.
2. Launch your Web browser (Internet Explorer version 6.0 or higher, or FireFox).
3. In the browser address bar, type the following:

`https://192.168.10.1:5825`

This launches the HiPath Wireless Assistant. The logon page is displayed.



4. In the **User Name** box, type your user name. The default is `admin`.

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

5. In the **Password** box, type your password. The default is abc123.

---

**Note:** To reinforce security protection, the login password length has now been increased to eight characters. Please note the following:

- The HiPath Wireless Controller continues to be shipped from the factory with a six character default password (abc123). Although, when the HiPath Wireless Controller is installed and you elect to change the default password, the eight character constraint will be applied.
  - The new password length constraint is not applied to existing passwords. When a six character password is already being used and an upgrade of the software to V5 occurs, the software does not require the password to be changed to eight characters. However, once the upgrade is completed and a new account is created, or the password of an existing account is changed, the new password length requirement will be enforced.
  - If you reset the HiPath Wireless Controller, the login user name and the password will also reset to the factory defaults (admin and abc123).
- 

6. Click **Login**. The HiPath Wireless Assistant main menu page is displayed.



## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

**Note:** All images of the HiPath Wireless Assistant in this User Guide represent the HiPath Wireless Controller C2400. In the footer of the HiPath Wireless Assistant, the following is displayed:

- **[host name | product name | up time]**

For example, [HWC-206 | C2400 | 01 days, 06:29]. If your HiPath Wireless Assistant is running the C2400 license, the footer will display C2400.

- If there is no key (unlicensed), the product name will not be displayed.

- **User** is the user id you used to login in. For example, admin.

- **Port Status** is the connectivity state of the port. M represents the Management interface, which is on eth0 and the numbered lights reflect the esa ports on the system. Green indicates the interface is up and running. Red indicates the interface is down. The F icon represents the flash drive status: green if the flash drive is mounted, and red if the flash drive is not mounted.

7. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.

8. In the left pane, click **IP Addresses**. The factory default settings for the HiPath Wireless Controller are displayed.

SIEMENS HiPath Wireless Controller Configuration

Home | Logs & Traces | Reports | **Wireless Controller** | Wireless APs | VNS Configuration | Mitigator | Help | LOGOUT

System Maintenance  
Routing Protocols  
**IP Addresses**  
Port Exception Filters  
Check Point  
Mitigator  
Mobility Manager  
SNMP  
Network Time  
Management Users  
Software Maintenance  
Utilities  
Web Settings  
Secure Connections  
Flash

Management Port Settings

Hostname: HWC-206 Management Gateway:  
Domain: siemens.com Primary DNS:  
IP Address: 192.168.4.206 Secondary DNS:  
Subnet mask: 255.255.255.0

Modify

Interfaces

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
<input type="checkbox"/>	esa0	U	10.21.3.2	08:00:06:81:C2:81	255.255.255.0	Router	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa1	100	10.109.0.4	08:00:06:81:C2:82	255.255.255.0	Router	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	esa2	U	10.0.2.1	08:00:06:81:C2:83	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	esa3	U	10.0.3.1	08:00:06:81:C2:84	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>

IP address: 10.21.3.2 Function: Router  
Subnet mask: 255.255.255.0 MTU: 1500  
VLAN ID:  Tagged - ID:   Untagged

Internal VLAN ID: 1 Multicast Support: Disabled

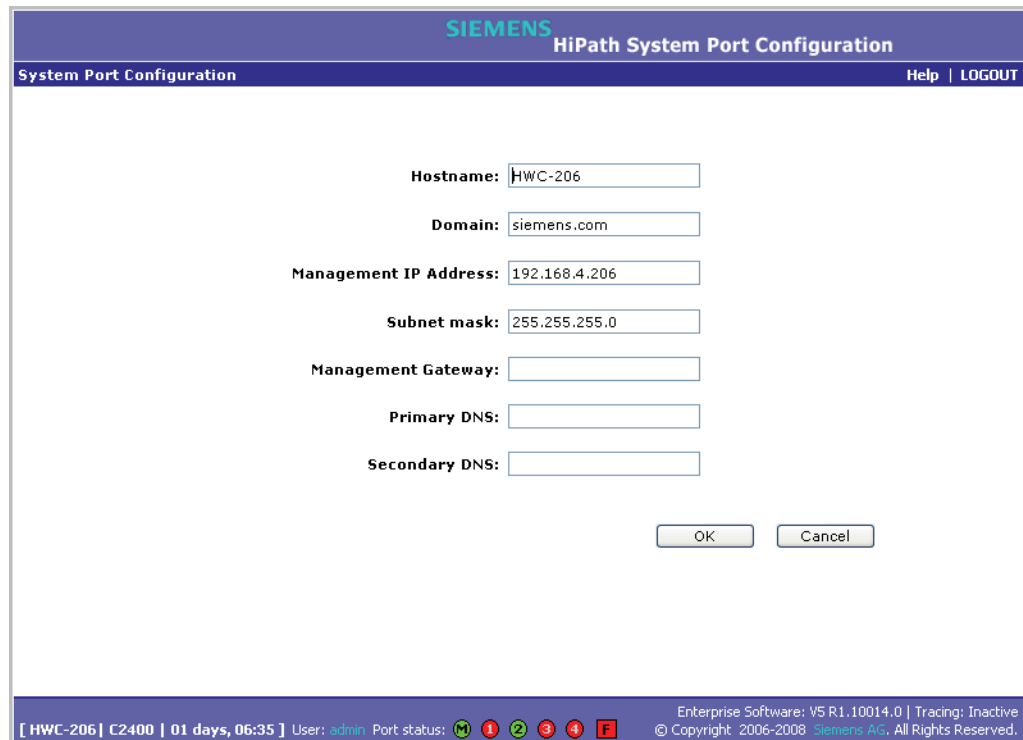
Save Cancel

[ HWC-206 | C2400 | 01 days, 06:33 ] User: admin Port status: [M] [1] [2] [3] [4] [F] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive  
© Copyright 2006-2008 Siemens AG. All Rights Reserved.

9. In the **Management Port Settings** section, click **Modify**. The **System Port Configuration** page is displayed.

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller



SIEMENS HiPath System Port Configuration

System Port Configuration Help | LOGOUT

Hostname:

Domain:

Management IP Address:

Subnet mask:

Management Gateway:

Primary DNS:

Secondary DNS:

[ HWC-206 | C2400 | 01 days, 06:35 ] User: admin Port status: [M][1][2][3][4][F] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved.

10. Type the following information:

- **Hostname** – Specifies the name of the HiPath Wireless Controller
- **Domain** – Specifies the IP domain name of the enterprise network
- **Management IP Address** – Specifies the new IP address for the HiPath Wireless Controller's management port. Change this as appropriate for the enterprise network.
- **Subnet mask** – Specifies the appropriate subnet mask for the IP address to separate the network portion from the host portion of the address (typically 255.255.255.0)
- **Management Gateway** – Specifies the default gateway of the network
- **Primary DNS** – Specifies the primary DNS server used by the network
- **Secondary DNS** – Specifies the secondary DNS server used by the network

11. To save your changes, click **OK**.

---

**Note:** The Web connection between the computer and the HiPath Wireless Controller is now lost. The IP addresses are now set to the network you defined.

---



#### 3.2.1.1 Changing the administrator password

It is recommended to change your default administrator password once your system is installed.

**To change the administrator password:**

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **Management Users**.
3. In the user\_admin table, click **admin**.
4. In the **Modify User Password** box, type the new administrator password.
5. In the **Modify User Confirm Password** box, type the new administrator password again.
6. Click **Change Password**.

#### 3.2.2 Connecting the HiPath Wireless Controller to your enterprise network

Once you have modified the management port configuration settings, the next step is to connect the HiPath Wireless Controller to your enterprise network.

**To connect the HiPath Wireless Controller to your enterprise network:**

1. Disconnect your computer from the HiPath Wireless Controller management port.
2. Connect the HiPath Wireless Controller management port to the enterprise Ethernet LAN. The HiPath Wireless Controller resets automatically.
3. Log on to the HiPath Wireless Assistant. The system is visible to the enterprise network.

#### 3.2.3 Applying the product license key

To ensure all available system functionality is enabled, your product license key must be applied.

**To apply the product license key:**

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **Software Maintenance**.
3. Click the **HWC Product Keys** tab.

## Configuring the HiPath Wireless Controller

Performing the first time setup of the HiPath Wireless Controller

4. In the **Apply Product Key** section, click **Browse** to navigate to the location of the product key file and click the file.
5. Click **Apply Now**. The product license key is applied, and the HiPath Wireless Controller reboots.

### 3.2.4 Setting up the data ports

The next step in the initial setup of the HiPath Wireless Controller is to configure the physical data ports.

A new HiPath Wireless Controller is shipped from the factory with all its data ports set up as host ports. Support of management traffic is disabled on all data ports. Port configuration allows for the explicit state of the administration state for each interface. By default, data interface states will be disabled. You can then enable each of the data interfaces individually. A disabled interface does not allow data to flow (receive/transmit).

#### **VLAN ID parameter**

You can define a specific VLAN tag to be applied to a particular interface. All packets associated with that port will be tagged with the corresponding VLAN. This allows the HiPath Wireless Controller to directly attach to a VLAN network without the need to remove VLAN tags at the connection port.

You can redefine the data ports to function as one of three types:

- **Host Port**

Use a host port definition for connecting Wireless APs with no OSPF routing function on this port.

- **Third-Party AP Port**

Use a third-party AP port definition for a port to which you will connect thirdparty APs. Only one port can be configured for third-party APs.

Selecting this option prepares the port to support a third-party AP setup allowing the mapping of a VNS to the physical port. The VNS settings permit the definition of policy, such as filters and Captive Portal, which manage the traffic flow for wireless users connected to these APs.

The third-party APs must operate as layer-2 bridges. The third-party AP VNS is isolated from the rest of the network. The HiPath Wireless Controller assumes control over the layer-3 functions including DHCP.

- **Router Port**

Use a router port definition for a port that you want to connect to a OSPF area to exchange routes to other OSPF routers.

Wireless APs can be attached to a router port. The HiPath Wireless Controller will create a virtual VNS port and handle wireless device traffic in the same manner as a host port.

---

**Note:** Third-party access points must not be directly connected to a router or host port.

---

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

There is a fourth port type that is not configurable in the HiPath Wireless Assistant:

- **Virtual Network Services (VNS) interface**

A VNS port is a virtual port created automatically on the HiPath Wireless Controller when a new VNS is defined. The VNS port becomes the default gateway for wireless devices on this VNS. No Wireless APs can be associated with a VNS port and no routing is permitted on this port.

The chart below summarizes the port types and their functions:

Port Type	Host	3rd-Party AP	Router	VNS
OSPF route advertisement	No	No	Selectable. Route wireless device traffic only.	No
Wireless AP support	Yes	No	Yes	No
Mgmt traffic support (SNMP, HTTP, TELNET, SLP, RADIUS, DHCP)	Selectable	Selectable	Selectable	Selectable
Routing protocol support (IP, OSPF and PIM)	No	No	Selectable	No

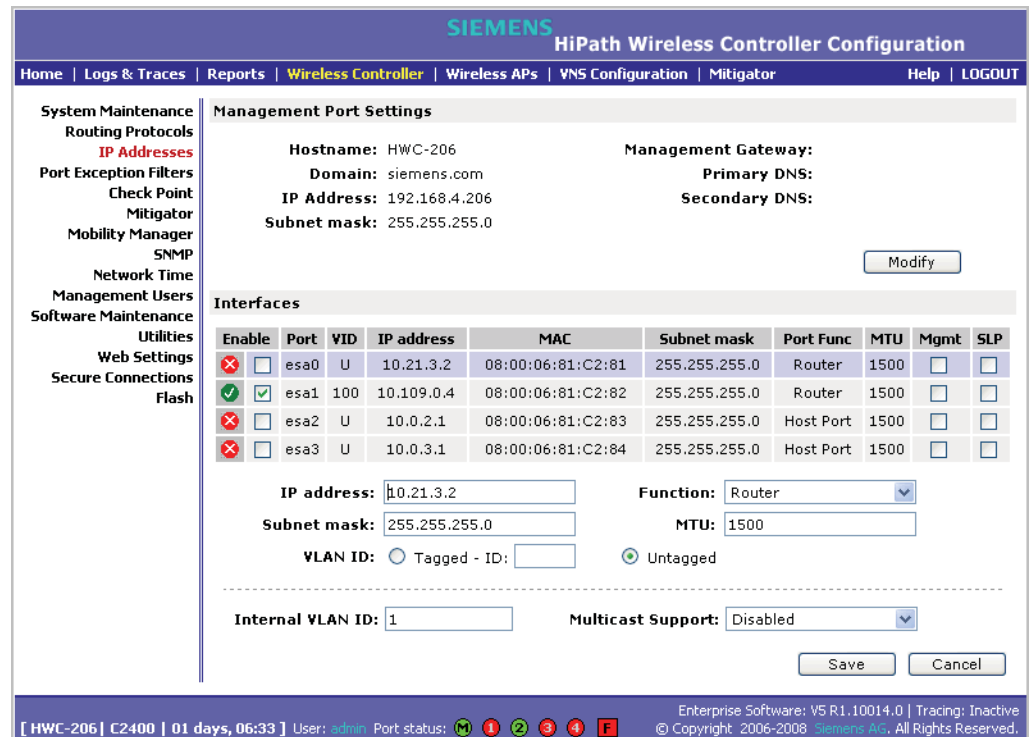
Table 2 Port types and functions

#### To configure the data port interfaces on the HiPath Wireless Controller:

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **IP Addresses**. The **Management Port Settings and Interfaces** page is displayed.

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller



The screenshot displays the configuration page for the HiPath Wireless Controller. The 'Management Port Settings' section shows the following configuration:

- Hostname: HWC-206
- Domain: siemens.com
- IP Address: 192.168.4.206
- Subnet mask: 255.255.255.0
- Management Gateway: (empty)
- Primary DNS: (empty)
- Secondary DNS: (empty)

The 'Interfaces' table is as follows:

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
<input checked="" type="checkbox"/>	esa0	U	10.21.3.2	08:00:06:81:C2:81	255.255.255.0	Router	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa1	100	10.109.0.4	08:00:06:81:C2:82	255.255.255.0	Router	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa2	U	10.0.2.1	08:00:06:81:C2:83	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa3	U	10.0.3.1	08:00:06:81:C2:84	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>

Below the table, the configuration for the selected interface (esa1) is shown:

- IP address: 10.21.3.2
- Subnet mask: 255.255.255.0
- Function: Router
- MTU: 1500
- VLAN ID:  Tagged - ID:   Untagged
- Internal VLAN ID:
- Multicast Support: Disabled

The lower portion of the **HiPath Wireless Controller Configuration** page displays the number of Ethernet ports of the HiPath Wireless Controller:

- **HiPath Wireless Controller C2400** – Four Ethernet ports
- **HiPath Wireless Controller C20** – Two Ethernet ports

**Note:** All images of the HiPath Wireless Assistant in this User Guide represent the HiPath Wireless Controller C2400.

#### 3. Click a port.

Port configuration allows for the explicit state of the administration state for each interface. By default, data interface states will be enabled. If they are not enabled, you can enable them each of them individually. A disabled interface does not allow data to flow (receive/transmit).

#### 4. Type the following:

- **IP address** – The IP Address of the physical Ethernet port.
- **Subnet mask** – The appropriate subnet mask for the IP address, which separates the network portion from the host portion of the address (typically 255.255.255.0).

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

- **MTU** – The Maximum Transmission Unit or maximum packet size for this port. The default setting is 1500. If you change this setting and are using OSPF, be sure that the MTU of each port in the OSPF link matches.

---

**Note:** If the routed connection to an AP traverses a link that imposes a lower MTU than the default 1500 bytes, the HiPath Wireless Controller and AP both participate in MTU discovery to automatically learn the correct MTU and adjust their settings accordingly. At the HiPath Wireless Controller, MTU adjustments are tracked on a per AP basis.

---

5. In the **Function** drop-down list, click one of the following:

- **Host Port** – Specifies a port for connecting Wireless APs with no OSPF routing function on this port..
- **Third-Party AP Port** – Specifies a port to which you will connect third-party access points.
- **Router Port** – Specifies a port that you want to connect to an upstream, next-hop router for OSPF route advertisement in the network.

---

**Note:** For OSPF routing on a port, the port must be configured as a router port.

---

6. To enable management traffic, select the **Mgmt** checkbox. Enabling management provides access to SNMP (v2, get), SSH, and HTTPs management interfaces.

---

**Note:** This option does not override the built-in protection filters on the port. The built-in protection filters for the port, which are restrictive in the types of packets that are allowed to reach the management plane, are extended with a set of definitions that allow for access to system management services through that interface (SSH, SNMP, HTTPS:5825).

---

7. To enable the SLP protocol, select the **SLP** checkbox.

Wireless APs use this port for discovery and registration. Other controllers can use this port to enable inter-controller device mobility if this port is configured to use SLP or the HiPath Wireless Controller is running as a manager and SLP is the discovery protocol used by the agents.

8. From the allow **Multicast Support** drop-down list, click the port: esa0, esa1, esa2 and esa3.

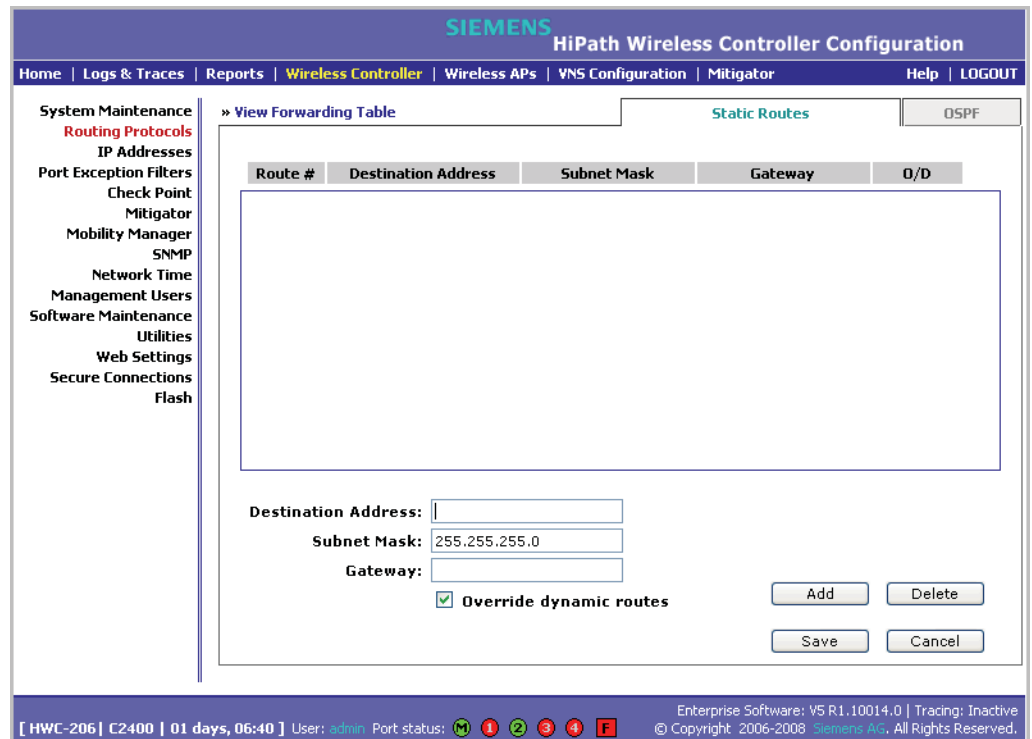
9. To save your changes, click **Save**.

### 3.2.5 Setting up static routes

It is recommended that you define a default route to your enterprise network, either with a static route or by using OSPF protocol. A default route enables the HiPath Wireless Controller to forward packets to destinations that do not match a more specific route definition.

To set a static route on the HiPath Wireless Controller:

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.



3. To add a new route, in the **Destination Address** box type the destination IP address of a packet. To define a default static route for any unknown address not in the routing table, type **0.0.0.0**.
4. In the **Subnet Mask** box, type the appropriate subnet mask to separate the network portion from the host portion of the IP address (typically 255.255.255.0). To define the default static route for any unknown address, type 0.0.0.0.
5. In the **Gateway** box, type the IP address of the specific router port or gateway on the same subnet as the HiPath Wireless Controller to which to forward these packets. This is the IP address of the next hop between the HiPath Wireless Controller and the packet's ultimate destination.

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

6. Click **Add**. The new route is added to the list of routes.
7. Select the **Override dynamic routes** checkbox to give priority over the OSPF learned routes, including the default route, which the HiPath Wireless Controller uses for routing. This option is enabled by default.

To remove this priority for static routes, so that routing is controlled dynamically at all times, clear the **Override dynamic routes** checkbox.

---

**Note:** If you enable dynamic routing (OSPF), the dynamic routes will normally have priority for outgoing routing. For internal routing on the HiPath Wireless Controller, the static routes normally have priority.

---

8. To save your changes, click **Save**.

#### To view the forwarding table on the HiPath Wireless Controller:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** page is displayed.
2. To view the static routes that have been defined for the HiPath Wireless Controller, click **Forwarding Table**. The **Forwarding Table** is displayed.

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.109.0.2	esa1	OSPF	Active
2	1.1.1.0	255.255.255.0		esa9	OSPF	InActive
3	1.1.1.0	255.255.255.0		esa9	Connected	Active
4	3.3.3.0	255.255.255.0	10.109.0.5	esa1	OSPF	Active
5	8.8.8.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
6	10.1.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
7	10.1.99.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
8	10.2.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
9	10.3.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
10	10.4.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
11	10.5.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
12	10.6.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
13	10.7.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
14	10.8.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
15	10.9.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
16	10.11.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
17	10.13.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
18	10.14.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
19	10.15.0.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active
20	10.20.30.0	255.255.255.0	10.109.0.2	esa1	OSPF	Active

This report displays all defined routes, whether static or OSPF, and their current status.

3. To update the display, click **Refresh**.



### **3.2.6 Setting up OSPF Routing**

To enable OSPF (OSPF RFC2328) routing, you must:

- Define one data port as a router port in the **IP Addresses** page
- Enable OSPF globally on the HiPath Wireless Controller
- Define the global OSPF parameters
- Enable (or disable) OSPF on the port that you defined as a router port

Ensure that the OSPF parameters defined here for the HiPath Wireless Controller are consistent with the adjacent routers in the OSPF area. This consistency includes the following:

- If the peer router has different timer settings, the protocol timer settings in the HiPath Wireless Controller must be changed to match, in order to achieve OSPF adjacency.
- The MTU of the ports on either end of an OSPF link must match. The MTU for ports on the HiPath Wireless Controller is defined as 1500, on the **IP Addresses** page, during data port setup. This matches the default MTU in standard routers.

**To set OSPF Routing Global Settings on the HiPath Wireless Controller:**

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.
3. Click the **OSPF** tab.

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

The screenshot shows the 'HiPath Wireless Controller Configuration' web interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar lists various system maintenance and configuration options, with 'Routing Protocols' highlighted. The main content area is titled 'View Forwarding Table' and contains 'Static Routes' and 'OSPF' tabs. The 'OSPF' tab is active, showing 'Global Settings' and 'Port Settings' sections. In the 'Global Settings' section, 'OSPF Status' is set to 'On', 'Router id' is empty, 'Area id' is '0.0.0.4', and 'Area Type' is 'Default'. A 'Save' button is present. The 'Port Settings' section contains a table with columns: I/F, Enabled, Authentication, Password, Cost, H/I, D/I, RT/I, and Delay. Two rows are shown for interfaces 'esa0' and 'esa1', both with 'Enabled' status and 'None' authentication. Below the table, 'Port Status' is 'Enabled', 'Link Cost' is '10', 'Authentication' is 'None', and 'Password' is empty. 'Hello Interval' is '10 (s)', 'Dead Interval' is '40 (s)', 'Retransmit Interval' is '5 (s)', and 'Transmit Delay' is '1 (s)'. A 'Save' button is at the bottom right. The footer shows system information: '[ HWC-206 | C2400 | 01 days, 06:44 ] User: admin Port status: [ M 1 2 3 4 F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright: 2006-2008 Siemens AG. All Rights Reserved.'

4. From the **OSPF Status** drop-down list, click **On** to enable OSPF.
5. In the **Router ID** box, type the IP address of the HiPath Wireless Controller. This ID must be unique across the OSPF area. If left blank, the OSPF daemon automatically picks a router ID from one of the HiPath Wireless Controller's interface IP addresses.
6. In the **Area ID** box, type the area. 0.0.0.0 is the main area in OSPF.
7. In the **Area Type** drop-down list, click one of the following:
  - **Default** – The default acts as the backbone area (also known as area zero). It forms the core of an OSPF network. All other areas are connected to it, and inter-area routing happens via a router connected to the backbone area.
  - **Stub** – The stub area does not receive external routes. External routes are defined as routes which were distributed in OSPF via another routing protocol. Therefore, stub areas typically rely on a default route to send traffic routes outside the present domain.
  - **Not-so-stubby** – The not-so-stubby area is a type of stub area that can import autonomous system (AS) external routes and send them to the default/backbone area, but cannot receive AS external routes from the backbone or other areas.
8. To save your changes, click **Save**.

#### **To set OSPF Routing Port Settings on the HiPath Wireless Controller:**

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **Routing Protocols**.
3. Click the **OSPF** tab. The **OSPF Settings** page is displayed.
4. In the **Port Status** drop-down list, click **Enabled** to enable OSPF on the port. The default setting is **Disabled**.
5. In the **Link Cost** box, type the OSPF standard for your network for this port. This is the cost of sending a data packet on the interface. The lower the cost, the more likely the interface is to be used to forward data traffic.

---

**Note:** If more than one port is enabled for OSPF, it is important to prevent the HiPath Wireless Controller from serving as a router for other network traffic (other than the traffic from wireless device users controlled by the HiPath Wireless Controller). To ensure that the HiPath Wireless Controller is never the preferred OSPF route, set the Link Cost to its maximum value of 65535. Filters should also be defined that will drop routed packets. For more information, see [Section 6.9, "Configuring filtering rules for a VNS"](#), on page 194.

---

6. In the **Authentication** drop-down list, click the authentication type for OSPF on your network: **None** or **Password**. The default setting is **None**.
7. If **Password** is selected as the authentication type, in the **Password** box, type the password. If **None** is selected as the Authentication type, leave this box empty. This password must match on either end of the OSPF connection.
8. Type the following:
  - **Hello-Interval** – Specifies the time in seconds (displays OSPF default). The default setting is **10** seconds.
  - **Dead-Interval** – Specifies the time in seconds (displays OSPF default). The default setting is **40** seconds.
  - **Retransmit-Interval** – Specifies the time in seconds (displays OSPF default). The default setting is **5** seconds.
  - **Transmit Delay**– Specifies the time in seconds (displays OSPF default). The default setting is **1** second.
9. To save your changes, click **Save**.

## Configuring the HiPath Wireless Controller

### *Performing the first time setup of the HiPath Wireless Controller*

#### **To confirm that ports are set for OSPF:**

1. To confirm that the ports are set up for OSPF, and that advertised routes from the upstream router are recognized, click **View Forwarding Table**. The **Forwarding Table** is displayed.

The following additional reports display OSPF information when the protocol is in operation:

- **OSPF Neighbor** – Displays the current neighbors for OSPF (routers that have interfaces to a common network)
  - **OSPF Linkstate** – Displays the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies.
2. To update the display, click **Refresh**.

### **3.2.7 Filtering at the interface level**

The HiPath Wireless solution has a number of built-in filters that protect the system from unauthorized traffic. These filters are specific only to the HiPath Wireless Controller. These filters are applied at the network interface level and are automatically invoked. By default, these filters provide stringent-level rules to allow only access to the system's externally visible services. In addition to these built-in filters, the administrator can define specific exception filters at the interface-level to customize network access. These filters do not depend on a VNS definition.

### **3.2.8 Built-in port-based exception filters**

On the HiPath Wireless Controller, various port-based exception filters are built in and invoked automatically. These filters protect the HiPath Wireless Controller from unauthorized access to system management functions and services via the ports. Access to system management functions is granted if the administrator selects the **allow management** option.

Allow management traffic is now specific to the interface being allowed. For example, if allow management is allowed on a physical port (esa0), only users connected through ESA0 will be able to get access to the system. Users connecting on any other interface such as a VNS (esa6) will no longer be able to target ESA0 to gain management access to the system. In order to allow access

## Configuring the HiPath Wireless Controller

### *Performing the first time setup of the HiPath Wireless Controller*

for users connected on a VNS, the VNS configuration itself must have **allow management** enabled and users will only be able to target the VNS interface specifically.

---

**Note:** You can also enable management traffic in the VNS definition.

---

For example, on the HiPath Wireless Controller's data interfaces (both physical interfaces and VNS virtual interfaces), the built-in exception filter prohibits invoking SSH, HTTPS, or SNMP. However, such traffic is allowed, by default, on the management port.

If management traffic is explicitly enabled for any interface (physical port or VNS), access is implicitly extended to that interface through any of the other interfaces (VNS). Only traffic specifically allowed by the interface's exception filter is allowed to reach the HiPath Wireless Controller itself. All other traffic is dropped. Exception filters are dynamically configured and regenerated whenever the system's interface topology changes (for example, a change of IP address for any interface).

Enabling management traffic on an interface adds additional rules to the exception filter, which opens up the well-known IP(TCP/UDP) ports, corresponding to the HTTPS, SSH, and SNMP applications.

The port-based built-in exception filtering rules, in the case of traffic from VNS users, are applicable to traffic targeted directly for the VNSs interface. For example, a VNS filter may be generic enough to allow traffic access to the HiPath Wireless Controller's management (for example, Allow All [\*.\*.\*]). Exception filter rules are evaluated after the user's VNS assigned filter policy, as such, it is possible that the VNS policy allow the access to management functions that the exception filter denies. These packets are dropped.

#### **To enable SSH, HTTPS, or SNMP access through a data interface:**

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **IP Addresses**. The **Management Port Settings** page is displayed.

## Configuring the HiPath Wireless Controller

### Performing the first time setup of the HiPath Wireless Controller

**Management Port Settings**

Hostname: HWC-206      Management Gateway:  
Domain: siemens.com      Primary DNS:  
IP Address: 192.168.4.206      Secondary DNS:  
Subnet mask: 255.255.255.0

Modify

**Interfaces**

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
<input checked="" type="checkbox"/>	esa0	U	10.21.3.2	08:00:06:81:C2:81	255.255.255.0	Router	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa1	100	10.109.0.4	08:00:06:81:C2:82	255.255.255.0	Router	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa2	U	10.0.2.1	08:00:06:81:C2:83	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa3	U	10.0.3.1	08:00:06:81:C2:84	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>

IP address: 10.21.3.2      Function: Router  
Subnet mask: 255.255.255.0      MTU: 1500  
VLAN ID:  Tagged - ID:        Untagged

Internal VLAN ID: 1      Multicast Support: Disabled

Save      Cancel

[ HWC-206 | C2400 | 01 days, 06:33 ] User: admin Port status: M 1 2 3 4 F Enterprise Software: V5 R1.10014.0 | Tracing: Inactive  
© Copyright: 2006-2008 Siemens AG, All Rights Reserved.

3. On the **IP Addresses** page, click the appropriate interface.
4. Select the corresponding **Management** checkbox.
5. To save your changes, click **Save**.

### 3.2.9 User defined port-based exception filters

You can add specific filtering rules at the port level in addition to the built-in rules. Such rules give you the capability of restricting access to a port, for specific reasons, such as a Denial of Service (DoS) attack.

The filtering rules are set up in the same manner as filtering rules defined for a VNS — specify an IP address and then either allow or deny traffic to that address. For more information, see [Section 6.9, “Configuring filtering rules for a VNS”](#), on page 194.

The rules defined for port exception filters are prepended to the normal set of restrictive exception filters and have precedence over the system's normal protection enforcement.

**Warning:** If defined improperly, user exception rules may seriously compromise the systems normal security enforcement rules. They may also disrupt the system's normal operation and even prevent system functionality altogether. It is advised to only augment the exception-filtering mechanism if absolutely necessary.

#### To define port exception filters:

1. From the main menu, click **Wireless Controller Configuration**. The **HiPath Wireless Controller Configuration** page is displayed.
2. In the left pane, click **Port Exception Filters**. The **Port Exception Filters** page is displayed.

The screenshot shows the Siemens HiPath Wireless Controller Configuration web interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar contains a menu with 'Port Exception Filters' highlighted. The main content area is titled 'Port Exception Filters' and features a 'Port:' dropdown menu set to 'esa0 (10.21.3.2)'. Below this is a table with columns 'Allow', 'IP : Port', and 'Protocol'. The table is currently empty. At the bottom of the table area, a note reads 'Rules with Allow unchecked are denied \*'. Below the table are input fields for 'IP/subnet:port:' and 'Protocol:' (set to 'N/A'), and buttons for 'Up', 'Down', 'Add', 'Delete', and 'Save'. The footer of the page displays system information: '[ HWC-206 | C2400 | 01 days, 06:46 ] User: admin Port status: [ M 1 2 3 4 F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved.'

3. In the **Port** drop-down list, click the applicable data port.
4. In the **IP / subnet: port** box, type the destination IP address. You can also specify an IP range, a port designation or a port range on that IP address.
5. In the **Protocol** drop-down list, click the protocol you want to specify for the filter. This list may include **UDP, TCP, IPsec-ESP, IPsec-AH, ICMP**. The default is N/A.

## Configuring the HiPath Wireless Controller

### *Completing the system configuration*

6. Click **Add**. The new filter is displayed on the **Filter** section of the page.
7. Click the new filter.
8. To allow traffic, select the **Allow** checkbox.
9. To adjust the order of the filtering rules, click **Up** or **Down** to position the rule. The filtering rules are executed in the order defined here.
10. To save your changes, click **Save**.

## 3.3 Completing the system configuration

Once you have performed the initial configuration of the HiPath Wireless Controller, you are now ready to do the following:

- **Configuring the VNS** – For more information, see [Chapter 5, “Virtual Network Services”](#).
- **Registering and assigning APs to the VNS** – For more information, see [Chapter 4, “Configuring the Wireless AP”](#).

## 3.4 Ongoing Operations of the Controller, Access Points and Convergence Software

Once you have configured the VNS and registered and assigned APs to the VNS, the Controller, Access Points and Convergence Software system configuration is complete. Ongoing operations of the Controller, Access Points and Convergence Software system can include the following:

- HiPath Wireless Controller System Maintenance
- Wireless AP Maintenance
- Client Disassociate
- Logs and Traces
- Reports and Displays

For more information, see [Chapter 11, “Performing system maintenance”](#).



## 4 Configuring the Wireless AP

This chapter discusses the Wireless AP and its role in the Controller, Access Points and Convergence Software solution, including:

- [Wireless AP overview](#)
- [Discovery and registration overview](#)
- [Configuring the Wireless APs for the first time](#)
- [Adding and registering a Wireless AP manually](#)
- [Configuring Wireless AP settings](#)
- [Configuring the default Wireless AP settings](#)
- [Modifying a Wireless AP's properties based on a default AP configuration](#)
- [Modifying the Wireless AP's default setting using the Copy to Defaults feature](#)
- [Configuring Wireless APs simultaneously](#)
- [Configuring an AP as a sensor](#)
- [Performing Wireless AP software maintenance](#)

### 4.1 Wireless AP overview

The Wireless AP is a wireless LAN access point that uses the 802.11 wireless standards (802.11a/b/g/n) for network communications. The Wireless AP bridges network traffic to an Ethernet LAN. The Wireless AP is provided with proprietary software that allows it to communicate only with the HiPath Wireless Controller.

The Wireless AP physically connects to a LAN infrastructure and establishes an IP connection to the HiPath Wireless Controller. The Wireless AP has no user interface — instead the Wireless AP is managed through the HiPath Wireless Assistant. The Wireless AP's configuration is centrally managed and applied from the HiPath Wireless Controller. In addition, the HiPath Wireless Controller provides centralized management (verification and upgrade) of the Wireless AP firmware image.

All communication with the HiPath Wireless Controller is carried out using a UDP-based protocol, which encapsulates IP traffic from the Wireless AP and directs it to the HiPath Wireless Controller. The HiPath Wireless Controller decapsulates the packets and routes them to the appropriate destinations, while managing sessions and applying policy.

## Configuring the Wireless AP

### Wireless AP overview

The Wireless AP comes in the following variants:

- HiPath Wireless AP
- HiPath Wireless Outdoor AP
- HiPath Wireless 802.11n AP

---

**Note:** The term, 'Wireless AP', is used in this document to encompass all three variants — HiPath Wireless AP, HiPath Wireless Outdoor AP, and HiPath Wireless 802.11n AP. The variants are only specifically identified in the documentation where it is necessary to do so.

---

### 4.1.1 HiPath Wireless AP

The HiPath Wireless AP is meant for indoor environments. It can be mounted on walls or ceilings, using special brackets, and can be kept completely out of sight.

The HiPath Wireless AP is available in the following models:

- **Model AP2610** – Internal antenna, internal dual (multimode) diversity antennas
- **Model AP2620** – External antenna (dual external antennas), RP-SMA connectors

#### 4.1.1.1 HiPath Wireless AP radios

The HiPath Wireless AP is equipped with two radios — radio **a** and radio **b/g**. The following is a block diagram of the HiPath Wireless AP equipped with external antennas.

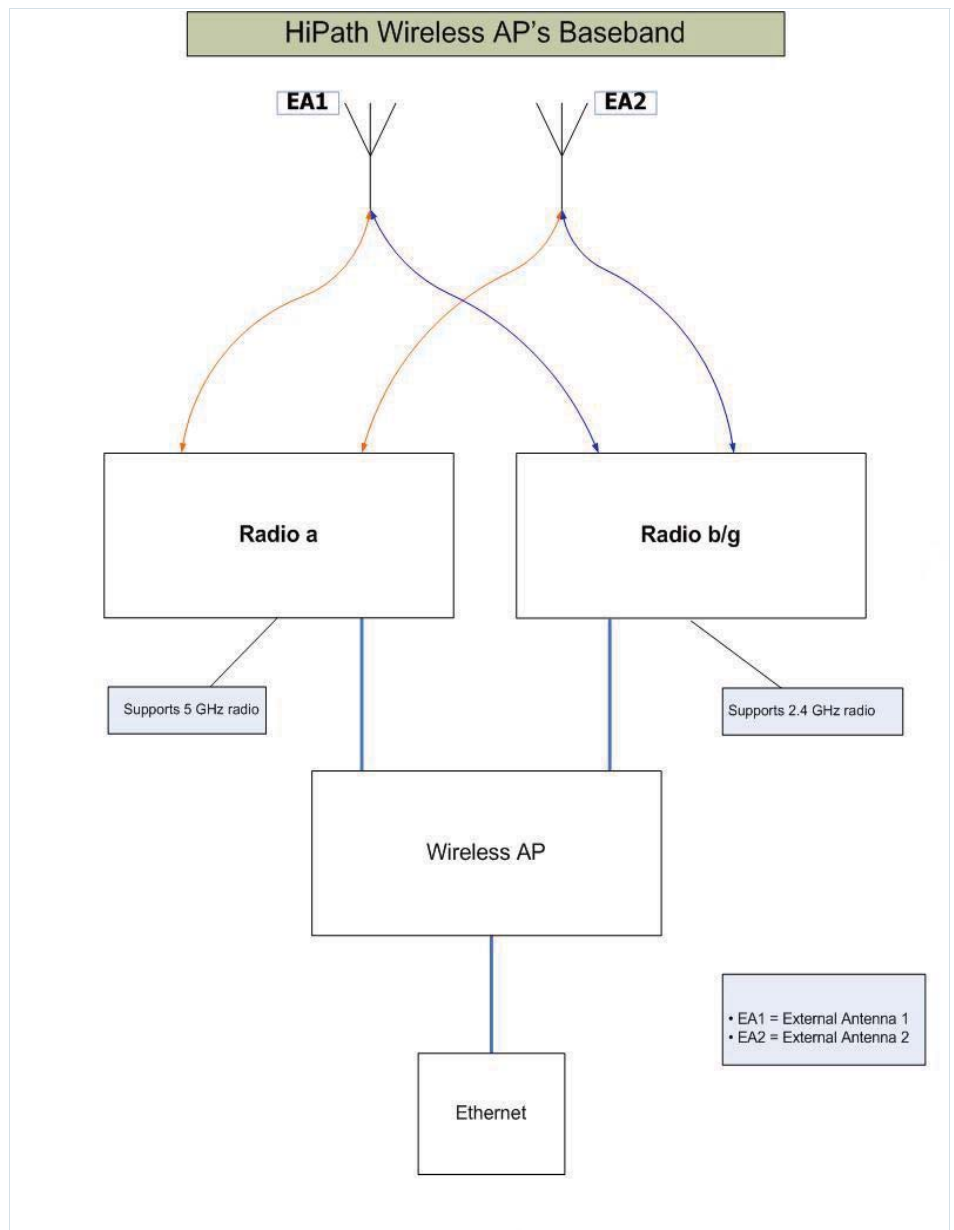


Figure 4 HiPath Wireless AP's Baseband

The Figure 4 illustrates the following:

- The HiPath Wireless AP has two radios— **a** radio and **b/g** radio.
- The **a** radio supports 5 GHz radio
- The **b/g** radio supports 2.4 GHz radio
- The **a** radio and the **b/g** radio are connected to both the external antennas — EA1 and EA2.

## Configuring the Wireless AP

### Wireless AP overview

**5 GHz radio supporting the 802.11a standard** – The 802.11a standard is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5-GHz band. The 802.11a standard uses an orthogonal frequency division multiplexing encoding scheme, rather than Frequency-Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS).

**2.4 GHz radio supporting the 802.11b/g standards** – The 802.11g standard applies to wireless LANs and specifies a transmission rate of 54 Mbps. The 802.11b (High Rate) standard is an extension to 802.11 that specifies a transmission rate of 11 Mbps. Since 802.11g uses the same communication frequency range as 802.11b (2.4 GHz), 802.11g devices can co-exist with 802.11b devices on the same network.

The radios are enabled or disabled through the HiPath Wireless Assistant. Both radios can be enabled to offer service simultaneously. For more information, see Section 7.3, “Topology for a VNS”, on page 168.

The Unlicensed National Information Infrastructure (U-NII) bands are three frequency bands of 100 MHz each in the 5 GHz band, designated for short-range, high-speed, wireless networking communication.

The Wireless AP supports the full range of 802.11a:

- 5.15 to 5.25 GHz – U-NII Low Band
- 5.25 to 5.35 GHz – U-NII Middle Band
- 5.725 to 5.825 GHz – U-NII High Band

### 4.1.2 HiPath Wireless Outdoor AP

The HiPath Wireless Outdoor AP enables you to extend your Wireless LAN beyond the confines of indoor locations. They are resistant to harsh outdoor conditions and extreme temperatures. Using the advanced wireless distribution feature of the HiPath Wireless LAN, the HiPath Wireless Outdoor AP can extend your Wireless LAN to outdoor locations without Ethernet cabling. A mounting bracket is available to enable quick and easy mounting of the HiPath Wireless Outdoor APs to walls, rails, and poles.

The HiPath Wireless Outdoor AP supports the 802.11a, 802.11g, and full backward compatibility with legacy 802.11b devices.

The HiPath Wireless Outdoor AP is available in the following two models:

- **Model AP2650** – Internal antenna, internal dual (multimode) diversity antennas

- **Model AP2660** – External antenna (dual external antennas), RP-SMA connectors

---

**Note:** Since the HiPath Wireless Outdoor AP is meant for outdoor environments, it is also referred to as the Outdoor AP.

Although the HiPath Wireless Outdoor AP is meant for outdoor environments, it can also be deployed in indoor environments.

---

---

**Note:** The configuration process is identical for HiPath Wireless APs, HiPath Wireless Outdoor APs and HiPath Wireless 802.11n APs, unless specified otherwise.

---

---

**Note:** The radio specifications of the HiPath Wireless Outdoor AP is identical to the HiPath Wireless AP. For more information, see [Section 4.1.1.1, “HiPath Wireless AP radios”](#), on page 58

---

### 4.1.3 HiPath Wireless 802.11n AP

The HiPath Wireless 802.11n AP is an IEEE 802.11n (draft)-compliant access point that offers significant increase in data throughput and coverage range without additional bandwidth or transmit power. With both 2.4 GHz and 5 GHz 802.11n (draft) standard radio modules, the 802.11n AP delivers total data rates of up to 300 Mbps. Given that the improved throughput of 300 Mbps will be spread over a number of simultaneous users, the performance of 802.11n AP will be close to that of a wired 100 Mbps Ethernet connection — the standard for desktop connectivity. With the 802.11n AP, mobile users get a similar experience to wired networks while accessing high-bandwidth data, voice, and video applications.

---

**Note:** The Wireless 802.11n AP is backward-compatible with existing 802.11a/b/g networks.

---

---

**Note:** The Wireless 802.11n AP cannot operate as a stand-alone access point.

---

#### MIMO

The mainstay of 802.11 AP is MIMO (multiple input, multiple output) — a technology that uses advanced signal processing with multiple antennas to improve the throughput. MIMO takes the advantage of multipath propagation to decrease packet retries to improve the fidelity of the wireless network.

## Configuring the Wireless AP

### Wireless AP overview

The 802.11n AP's MIMO radio sends out one or two radio signals through its three antennas. Each of these signals is called a spatial stream. Because the location of the antennas on the 802.11n AP is spaced out, each spatial stream follows a slightly different path to the client device. Furthermore, the three spatial streams get multiplied into several streams as they bounce off the obstructions in the vicinity. This phenomenon is called multipath. Since these streams are bounced from different surfaces, they follow different paths to the client device. The client device, which is also 802.11n compliant, also has multiple antennas. Each of the antennas independently decodes the arriving signal. Then each antenna's decoded signal is combined with the decoded signals from the other antennas. The software algorithm uses the redundancy to extract one or two spatial streams and enhances the streams' "signal to noise ratio".

The client device too sends out one or two spatial streams through its multiple antennas. These spatial streams get multiplied into several streams as they bounce off the obstructions in the vicinity enroute to 802.11n AP. The 802.11n AP's MIMO receiver receives these multiple streams with three antennas. Each of the three antennas independently decodes the arriving signal. Then each antenna's decoded signal is combined with the decoded signals from the other antennas. The 802.11n AP's MIMO receiver again uses the redundancy to extract one or two spatial streams and enhances the streams' "signal to noise ratio".

By using the multiple streams, MIMO doubles the throughput.

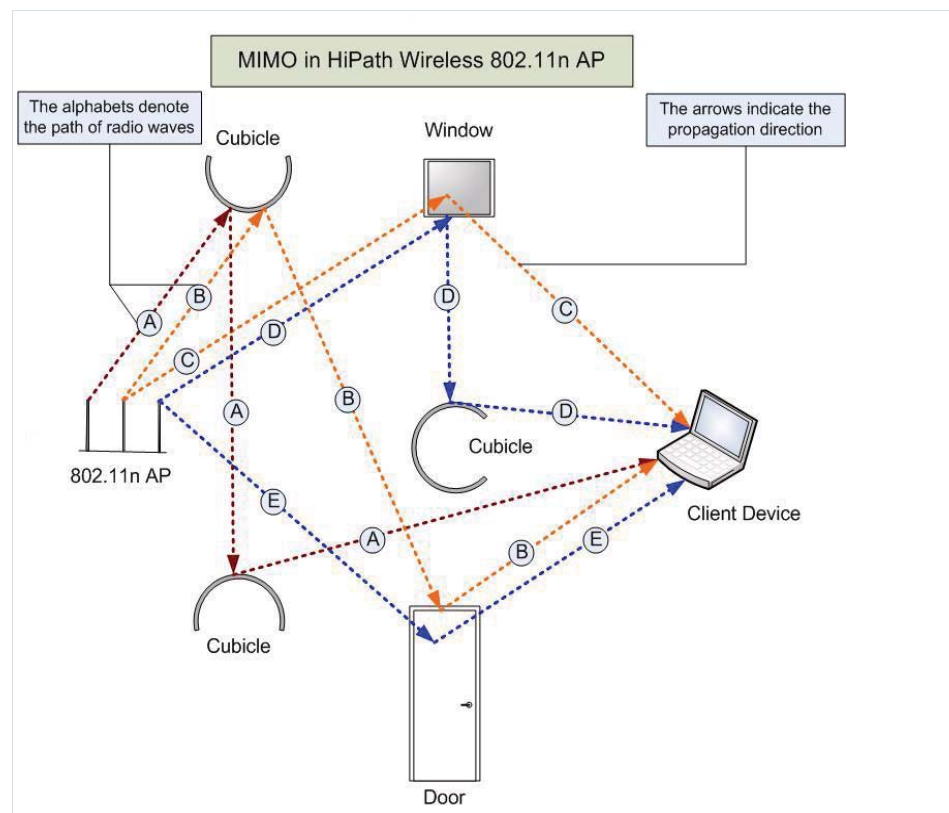


Figure 5 MIMO in HiPath Wireless 802.11n AP

---

**Note:** MIMO should not be confused with the **Diversity** feature. While **Diversity** is the use of two antennas to increase the odds that a better radio stream is received on either of the antennas, MIMO antennas radiate and receive multi-streams of the same packet to achieve the increased throughput.

The **Diversity** feature is meant to offset the liability of RF corruption, arising out of multipath, whereas MIMO converts the liability of multipath to its advantage.

---

Because the 802.11n AP operates with multiple-antennas, it is capable of picking-up even the weakest signals from the client devices.

### Channel bonding

In addition to MIMO technology, the 802.11n AP makes a number of additional changes to the radio to increase the effective throughput of the Wireless LAN. The radios of regular HiPath Wireless APs use radio channel that are 20 MHz wide. This means that the channels must be spaced at 20 MHz to avoid interference. The radios of 802.11n AP can use two channels at the same time to create a 40 MHz wide channel. By using the two 20 MHz channels in this manner, the 802.11n AP achieves more than double throughput. The 40-MHz channels in 802.11n are two adjacent 20-MHz channels, bonded together. This technique of using two channels at the same time is called channel bonding.

### Shortened guard interval

The purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections of symbols in orthogonal frequency division multiplexing (OFDM) — a method by which information is transmitted via a radio signal in Wireless APs.

In OFDM method, the beginning of each symbol is preceded by a guard interval. As long as the echoes fall within this interval, they will not affect the safe decoding of the actual data, as data is only interpreted outside the guard interval. Longer guard periods reduce the channel efficiency. The 802.11n AP provides reduced guard periods, thereby increasing the throughput.

### MAC enhancements

The 802.11n AP also has an improved MAC layer protocol that reduces the overheads (in the MAC layer protocol) and the contention losses. This results in increased throughput.

The 802.11n AP is available in the following two models:

- **Model AP3610** – Six internal antennas

## Configuring the Wireless AP

### Wireless AP overview

- **Model AP3620** – Three external antennas

---

**Note:** The 802.11n AP cannot be deployed in an outdoor environment.

---

#### 4.1.3.1 HiPath Wireless 802.11n AP's radios

The HiPath Wireless 802.11n AP is equipped with two radios — radio **a/n** and radio **b/g/n**. The following is a block diagram of the HiPath Wireless 802.11n AP equipped with external antennas.

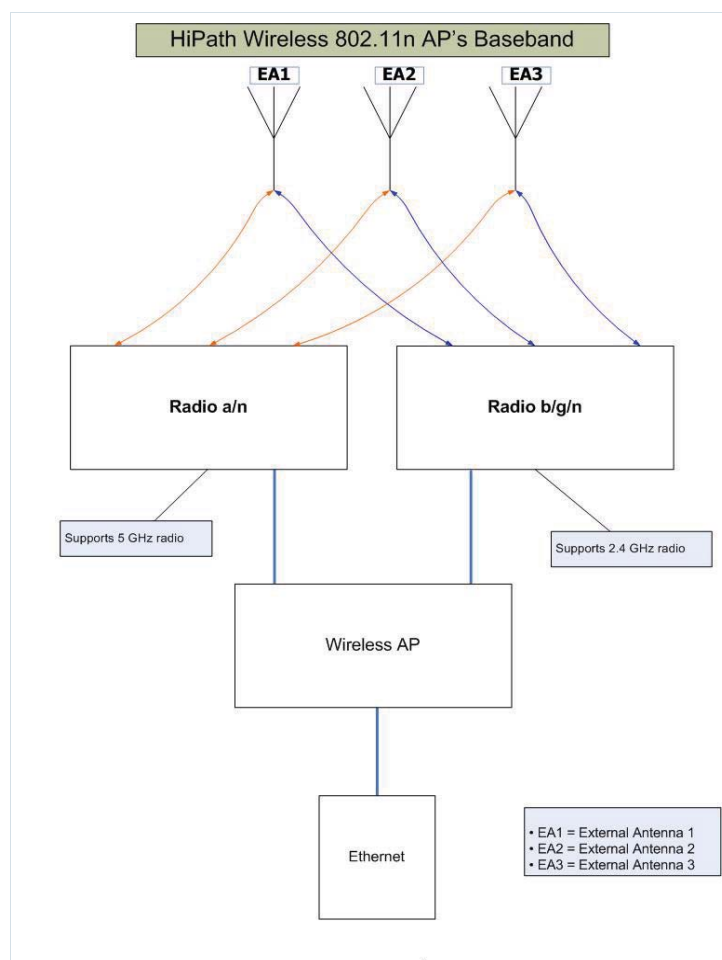


Figure 6 HiPath Wireless 802.11n AP's Baseband

The Figure 6 illustrates the following:

- The HiPath Wireless 802.11n AP has two radios — **a/n** radio and **b/g/n** radio.
- Both the radios are connected to all three antennas — EA1, EA2 and EA3.



- The **a/n** radio supports 5 GHz radio
- The **b/g/n** radio supports 2.4 GHz radio

**5 GHz radio supporting the 802.11a/n standard** — When in legacy 802.11a mode, the AP36xx supports data rates up to 54Mbps identical to the AP26xx. The modulation used is OFDM. In 802.11n mode there are 2 supported channel bandwidths, 20MHz and 40MHz. The 802.11n AP supports up to 300Mbps in 40MHz channels and 130Mbps in 20MHz channels. The modulation used is 3x3 MIMO (multiple input, multiple output).

**2.4 GHz radio supporting the 802.11b/g/n standard** — When in legacy 802.11b/g mode, the AP36xx supports data rates up to 54Mbps identical to the AP26xx. The modulation used is OFDM for 11g and CCK for 11b. In 802.11n mode there are 2 supported channel bandwidths, 20MHz and 40MHz. The AP36xx supports up to 300Mbps in 40MHz channels and 130Mbps in 20MHz channels. The modulation used is 3x3 MIMO (multiple input multiple output).

The radios are enabled or disabled through the HiPath Wireless Assistant. For more information, see [Section 4.5.3.1, “Modifying Wireless 802.11n AP 3610/3620 radio properties”](#), on page 96.

The Unlicensed National Information Infrastructure (U-NII) bands are three frequency bands of 100 MHz each in the 5 GHz band, designated for short-range, high-speed, wireless networking communication.

The 802.11n AP supports the full range of frequencies available in the 5GHz band:

- 5150 to 5250 MHz - U-NII Low band
- 5250 to 5350 MHz - U-NII middle band
- 5470 to 5700 MHz - New FCC approved band
- 5725 to 5825 MHz - U-NII high band

#### **4.1.4 Wireless AP international licensing**

The Wireless AP is licensed to operate in North America, the European Union countries, and European Union free trade countries. Each European Union country is assigned a particular radio band. The Wireless AP must be configured to operate on the appropriate radio band according to each European Union country. For more information, see [Section B.2.5, “European community”](#), on page 396.

To configure the appropriate radio band according to each European Union country, use the HiPath Wireless Assistant. For more information, see [Section 4.5, “Configuring Wireless AP settings”](#), on page 87.

#### 4.1.5 Wireless AP default IP address and first-time configuration

The HiPath Wireless AP and the HiPath Wireless Outdoor AP are shipped from the factory with a default IP address — 192.168.1.20. The default IP address simplifies the first-time IP address configuration process for Wireless APs. The Wireless AP returns to its default IP address if the Wireless AP is not successful in its discovery process, which determines the IP address of the Wireless AP and of the HiPath Wireless Controller. Wireless AP behaviour ensures that only one Wireless AP at a time on a subnet can use the default IP address. For more information, see [Section 4.2, “Discovery and registration overview”, on page 71](#).

Wireless AP LEDs indicate when it is possible to connect the Wireless AP using the default IP address. For more information, see [Section 4.2.3, “Understanding the Wireless AP LED status”, on page 74](#).

Wireless APs can have their IP addresses assigned using two methods, either a Dynamic Host Configuration Protocol (DHCP) server assigns the IP address or an administrator can assign the IP address using the static configuration option. The DHCP IP address assignment method is the default method for Wireless AP configuration. The Wireless AP returns to its default IP address assignment if the DHCP assignment is not successful. DHCP assignment is part of the discovery process. For more information, see [Section 4.2, “Discovery and registration overview”, on page 71](#). The Wireless AP default IP address impacts the first-time configuration processes for both methods:

- **DHCP server** – If successful, the Wireless AP is assigned an IP address by the network’s DHCP server when the Wireless AP is powered on.
  - If the DHCP assignment is not successful in the first 60 seconds, the Wireless AP returns to its default IP address.
  - The Wireless AP waits for 30 seconds in default IP address mode before attempting again to acquire the IP address from the DHCP.
  - The process repeats itself until the DHCP assignment is successful, or until an administrator assigns the Wireless AP an IP address using static configuration.

---

**Note:** You can telnet the Wireless AP during the 30 seconds the Wireless AP is assigned its default IP address. If a static IP address is assigned during this period, you must reboot the Wireless AP for the configuration to take effect.

---

- **Static configuration** – You can assign a static IP address to the Wireless AP. For more information, see the following section.

## 4.1.6 Assigning static IP address to Wireless AP

In order to establish the telnet session, you have to ping the Wireless AP's IP address. You must know the correct IP address to ping. The Wireless AP's IP address may have the default values or the DHCP-assigned values, depending upon the network condition. The concept is explained with the help of the following network conditions:

### DHCP server is available on the network

- The Wireless AP gets the IP address via the DHCP assignment, and successfully discovers the controller.
  - If the Wireless AP gets the IP address via the DHCP assignment and it successfully discovers the controller, you can configure its static IP address via the controller's user interface. For more information, see [Section 4.5.4, "Setting up the Wireless AP using static configuration"](#), on page 114.
- The Wireless AP gets the IP address via the DHCP assignment, but fails to discover the controller.
  - Ping the IP address that is assigned to the Wireless AP via the DHCP assignment.

### DHCP server is not available on the network

- The DHCP server is not available on the network, and the Wireless AP reverts to its factory defaults after trying for 60 seconds to get the IP address via the DHCP assignment.
  - Ping the default IP address.

---

**Note:** The default IP address of all the Wireless AP variants — Wireless AP, Wireless Outdoor AP and the Wireless 802.11n AP — is 192.168.1.20.

---

### To assign the static IP address to the Wireless AP:

1. Connect the Wireless AP to network.
2. Ping the Wireless AP's IP address.
3. When the ping is successful, telnet the Wireless AP.

## Configuring the Wireless AP

### Wireless AP overview

---

**Note:** If the telnet session is not established within 30 seconds of successful pinging, the Wireless AP again initiates the process of getting the IP address via the DHCP assignment.

---

---

**Note:** The default user name and the password for telnet access are:

- User Name – **admin**
- Password – **new2day**

You can override the default password by setting up a new telnet access password on the **Wireless Registration** screen. For more information see, Section 4.1.6.1, “Enabling/Disabling telnet access and setting up new Telnet Access Password via the controller’s user interface”, on page 70.

---

4. Configure the static configuration, using the following CLI commands.

#### CLI commands for configuring static IP address in the HiPath Wireless AP:

---

**Note:** The CLI commands to configure the static IP address in the HiPath Wireless AP and the HiPath Wireless Outdoor APs are identical.

---

#### Syntax

```
set <dhcp disable>
```

```
set <ipaddr>
```

```
set <ipmask>
```

#### Parameters

Parameter Name	Description
dhcp disable	By default, the Wireless AP is configured to acquire its IP address via the DHCP assignment. The command disables the DHCP server.
ipaddr	Specifies the static IP address.
ipmask	Specifies the subnet

Table 3 CLI command to configure static IP address in the HiPath Wireless AP

---

**Note:** After you run these commands, you must reboot the Wireless AP for the configuration to take effect.

---

**CLI commands to configure static IP address in the HiPath Wireless 802.11n AP:**

**Syntax**

```
cset <dhcp disable>
cset <ipaddr>
cset <ipmask>
cset <gateway>
capply
csave
```

**Parameters**

Parameter Name	Description
dhcp disable	By default, the Wireless AP is configured to acquire its IP address via the DHCP assignment. The command disables the DHCP server.
ipaddr	Specifies the IP address.
ipmask	Specifies the subnet.
gateway	Specifies the IP address of the network gateway.
capply	Applies the configuration.
csave	Saves the configuration.

*Table 4 CLI command to configure static IP address in the HiPath Wireless 802.11n AP*

---

**Note:** After you run these commands, you must reboot the Wireless 802.11n AP for the configuration to take effect.

---

## Configuring the Wireless AP

### Wireless AP overview

#### 4.1.6.1 Enabling/Disabling telnet access and setting up new Telnet Access Password via the controller's user interface

You can **enable/disable** the telnet access, and set up a new **Telnet Access Password** via the controller's user interface. The Wireless AP must successfully discover the controller to pick up this configuration.

---

**Note:** The new telnet access password that you set up over the controller's user interface overrides the default telnet access password.

---

#### Enabling/disabling telnet access via the controller's user interface

To enable/disable telnet access:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen appears.
2. In the Wireless AP list, click the Wireless AP for which you want to enable/disable telnet.

The screenshot displays the Siemens HiPath Wireless AP configuration interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The main content area is titled 'AP Properties' and shows configuration details for an AP with IP address 192.168.4.30 and MAC address 0002000000051504. The configuration includes fields for Serial #, Name, Description, Port (esa0), AP Environment (Indoor), Hardware Version (A&D Scalance W788-2RR), Application Version (V5 R1.10026.0), Status (Approved), Active Clients (0), Poll Timeout (11 seconds), Poll Interval (3 seconds), and Telnet Access (Enable). There are also checkboxes for 'Maintain client sessions in event of poll failure', 'Restart service in the absence of controller', and 'Use broadcast for disassociation'. The Country is set to Austria. At the bottom, there are buttons for 'Copy to Defaults', 'Reset to Defaults', 'Add Wireless AP', and 'Save'. The footer shows the user is 'admin' and the system is running Enterprise Software V5 R1.10034.0.

3. From the **Telnet Access** drop-down menu, select **Enable** to enable the telnet access, or select **Disable** to disable the telnet access.
4. Click **Save**.

### Setting up a new Telnet Access Password via the controller's user interface

To set up a new Telnet Access Password:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen appears.
2. From the left pane, click **AP Registration**. The **Wireless AP Registration** screen appears.

The screenshot shows the Siemens HiPath Wireless AP configuration interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar lists various configuration options, with 'AP Registration' highlighted in red. The main content area is titled 'Wireless AP Registration' and contains the following sections:

- Registration Mode:** Radio buttons for 'Stand-alone' and 'Paired'. The 'Paired' option is selected. Below it is a text box for 'Wireless Controller IP Address' containing '10.109.0.1' and a checkbox for 'Current Wireless Controller is primary connection point'.
- Security Mode:** Radio buttons for 'Allow all Wireless APs to connect' and 'Allow only approved Wireless APs to connect'. The 'Allow all Wireless APs to connect' option is selected.
- Discovery Timers:** Two text boxes: 'Number of retries' with value '3' (range 1 - 255) and 'Delay between retries' with value '1' (range 1 - 10 seconds).
- Telnet Access:** Two text boxes for 'Password' and 'Confirm password'.

At the bottom of the main area are two buttons: 'View SLP Registration' and 'Save'. The footer of the interface shows system information: '[ HWC ] C2400 | 01 days, 04:15 | User: admin | Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] [ F ]' and 'Software: V5 R1.10034.0 | Tracing: Inactive | © Copyright 2006-2008 Siemens AG, All Rights Reserved.'

3. Under the **Telnet Access** section, type the new password in the **Password** box.
4. Retype the password in the **Confirm Password** box.
5. Click **Save**.

## 4.2 Discovery and registration overview

When the Wireless AP is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the HiPath Wireless Controller. When the discovery process is successful, the Wireless AP registers with the HiPath Wireless Controller.

---

**Warning:** Only use power supplies that are recommended by Siemens. For example, PHIHONG PSA18U-480C.

---

#### 4.2.1 Wireless AP discovery

Wireless APs discover the IP address of a HiPath Wireless Controller using a sequence of mechanisms that allow for the possible services available on the enterprise network. The discovery process is successful when the Wireless AP successfully locates a HiPath Wireless Controller to which it can register.

You must ensure that the appropriate services on your enterprise network are prepared to support the discovery process. The following five steps summarize the discovery process:

- **Step 1 – Use the IP address of the last successful connection to a HiPath Wireless Controller.**

Once a Wireless AP has successfully registered with a HiPath Wireless Controller, it recalls that controller's IP address, and uses that address on subsequent reboots. The Wireless AP bypasses discovery and goes straight to registration.

If this discovery method fails, it cycles through the remaining steps until successful.

- **Step 2 – Use the predefined static IP addresses for the HiPath Wireless Controllers on the network (if configured).**

You can specify a list of static IP addresses of the HiPath Wireless Controllers on your network. On the **Static Configuration** tab, add the addresses to the **Wireless Controller Search List**.

---

**Caution:** Wireless APs configured with a static Wireless Controller Search List can only connect to HiPath Wireless Controllers in the list. Improperly configured Wireless APs cannot connect to a non-existent HiPath Wireless Controller address, and therefore cannot receive a corrected configuration.

---

- **Step 3 – Use Dynamic Host Configuration Protocol (DHCP) Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.**

To use the DHCP and unicast SLP discovery method, you must ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The Wireless APs use this method to discover the HiPath Wireless Controller.

This solution takes advantage of two services that are present on most networks:

- **DHCP (Dynamic Host Configuration Protocol)** – The standard is a means of providing IP addresses dynamically to devices on a network.



- **SLP (Service Location Protocol)** – A means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services using a Service Agent (SA). In larger installations, a Directory Agent (DA) collects information from SAs and creates a central repository (SLP RFC2608).

The HiPath Wireless Controller contains an SLP SA that, when started, queries the DHCP server for Option 78 and if found, registers itself with the DA as service type Siemens. The HiPath Wireless Controller contains a DA (SLPD).

The Wireless AP queries DHCP servers for Option 78 in order to locate any DAs. The Wireless APs SLP User Agent then queries the DAs for a list of Siemens SAs.

Option 78 must be set for the subnets connected to the ports of the HiPath Wireless Controller and the subnets connected to the Wireless APs. These subnets must contain an identical list of DA IP addresses.

- **Step 4 – Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.**

If no DA is found, or if it has no Siemens SAs registered, the Wireless AP attempts to locate a HiPath Wireless Controller via DNS.

If you use this method for discovery, place an A record in the DNS server for Controller.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

- **Step 5 – Use a multicast SLP request to find SLP SAs**

If all of the preceding methods fail to locate a HiPath Wireless Controller, the Wireless AP sends a multicast SLP request, looking for any SLP Service Agents providing the Siemens service.

## 4.2.2 Registration after discovery

Any of the discovery steps 2 through 5 can inform the Wireless AP of a list of multiple IP addresses to which the Wireless AP may attempt to connect. Once the Wireless AP has discovered these addresses, it sends out connection requests to each of them. These requests are sent simultaneously. The Wireless AP will attempt to register only with the first which responds to its request.

When the Wireless AP obtains the IP address of the HiPath Wireless Controller, it connects and registers, sending its serial number identifier to the HiPath Wireless Controller, and receiving from the HiPath Wireless Controller a port IP address and binding key.

## Configuring the Wireless AP

### *Discovery and registration overview*

Once the Wireless AP is registered with a HiPath Wireless Controller, the Wireless AP must be configured. After the Wireless AP is registered and configured, it can be assigned to a Virtual Network Segment (VNS) to handle wireless traffic.

#### **4.2.2.1 Default Wireless AP configuration**

Default Wireless AP configuration simplifies the registration after discovery process. Default Wireless AP configuration acts as a configuration template that can be automatically assigned to new registering Wireless APs. The default Wireless AP configuration allows you to specify common sets of radio configuration parameters and VNS assignments for Wireless APs. For more information, see [Section 4.5.7, “Configuring the default Wireless AP settings”](#), on [page 128](#).

#### **4.2.3 Understanding the Wireless AP LED status**

When the Wireless AP is powered on and boots, you can follow its progress through the registration process by observing the LED sequence as described in the following sections.

##### **4.2.3.1 HiPath Wireless AP LED status**

The following figure depicts the location of the three LEDs on the HiPath Wireless AP.

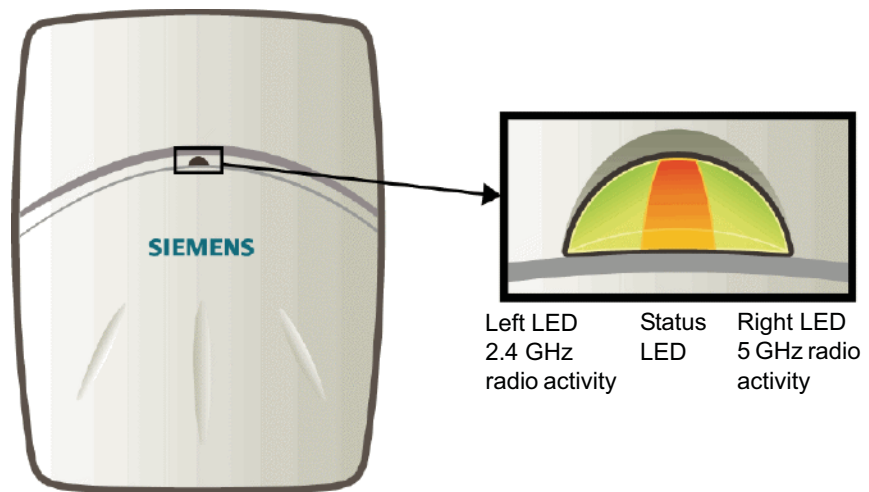


Figure 7 HiPath Wireless AP LEDs

---

**Warning:** Never disconnect a Wireless AP from its power supply during a firmware upgrade. Disconnecting a Wireless AP from its power supply during a firmware upgrade may cause firmware corruption rendering the AP unusable.

---

**LEDs color codes**

The AP LEDs indicate “normal-operation”, “warning/special”, or “failed” state of the Wireless AP in the following color codes:

- Green – Indicates the normal-operation state.
- Orange/Amber – Indicates the warning, or special state such as WDS.
- Red – Indicates the error state.
- Blinking – Indicates that the state, such as initialization, or discovery is in progress.
- Steady – Indicates that the state is stable/completed. For example, initialization finished, or discovery completed.

**Center LED**

The Center LED indicates the general status of the Wireless AP:

Center LED	HiPath Wireless AP’s status
Blinking Green	Initialization and discovery in progress via Ethernet link
Blinking Orange/Amber	Initialization and discovery in progress via WDS link
Blinking Red	Error during initialization/discovery process

Table 5 Center LED and Wireless AP’s status

## Configuring the Wireless AP

### Discovery and registration overview

Center LED	HiPath Wireless AP's status
Solid Red	Irrecoverable error
Solid Green	Discovery finished via Ethernet link
Solid Orange/Amber	Discovery finished via WDS link

Table 5 Center LED and Wireless AP's status

### Left LED

The Left LED indicates the high-level state of the Wireless AP during the initialization and discovery process:

Left LED	HiPath Wireless AP's high-level state
Off	Initialization
Blinking Green	Network Discovery
Solid Green	Connecting with the HiPath Wireless Controller

Table 6 Left LED and Wireless AP's high-level state

### Left and Right LEDs

The Right LED indicates the detailed state during the initialization and discovery processes:

Left LED	Right LED	HiPath Wireless AP's detailed state
Off	Off	Initialization: Power-on self-test (POST)
	Blinking Green	Initialization: Random delay
	Solid Green	Initialization: Vulnerable period
Blinking Green	Off	Network Discovery: 802.1X authentication
	Blinking Green	Network Discovery: Attempting to obtain IP address via DHCP
	Solid Green	Network Discovery: Discovered HiPath Wireless Controller
Solid Green	Off	Connecting to HiPath Wireless Controller: Attempting to register with the HiPath Wireless Controller
	Blinking Green	Connecting to HiPath Wireless Controller: Upgrading to higher version
	Solid Green	Connecting to HiPath Wireless Controller: Configuring itself

Table 7 Left and Right LEDs and Wireless AP's detailed state

### Composite view of the three LEDs

The Center, Left and the Right LEDs work in conjunction to indicate the general, high-level state and the detailed state respectively.

The following table provides a composite view of the three LED lights of the Wireless AP's state:

**Configuring the Wireless AP**  
Discovery and registration overview

Left LED	Right LED	Center LED	HiPath Wireless AP's Detailed state
Off	Off	Blinking Green	Initialization: Power-on self-test (POST)
	Blinking Green	Blinking Green	Initialization: Random delay
	Solid Green	Blinking Green	Initialization: Vulnerable period
		Blinking Red	Reset to factory defaults
	Solid Green	Blinking Orange	WDS scanning
Blinking Green	Off	Blinking Green / Orange	Network discovery: 802.1x authentication
		Blinking Red	Failed 802.1x authentication
	Blinking Green	Blinking Green / Orange	Network discovery: DHCP
		Blinking Red	Default IP address
	Solid Green	Blinking Green / Orange	Network discovery: HWC discovery / connect
		Blinking Red	Discovery failed
Solid Green	Off	Blinking Green / Orange	Connecting with HiPath Wireless Controller: Registration
		Blinking Red	Registration failed
	Blinking Green	Blinking Green / Orange	Connecting with HiPath Wireless Controller: Image upgrade
		Blinking Red	Image upgrade failed
	Solid Green	Blinking Green / Orange	Connecting with HiPath Wireless Controller: Configuration
		Blinking Red	Configuration failed
	Blinking Green	Solid Green / Orange	AP operating normally: Forced image upgrade
		Blinking Red	Image upgrade failed

Table 8 Composite view of three LED lights

## Configuring the Wireless AP

### Discovery and registration overview

---

**Note:** The Left and Right LEDs turn on after the center LED. This allows you to distinguish easily between the Center LED and the Left/Right LEDs.

---

---

**Note:** If the Center LED begins blinking RED, it indicates that the Wireless AP's state has failed.

---

---

**Note:** Random delays do not occur during normal reboot. A random delay only occurs after vulnerable period power-down.

---

The Wireless AP can be reset to its factory default settings. For more information, see Section 11.2, "Resetting the Wireless APs to their factory default settings", on page 313.

---

#### 4.2.3.2 HiPath Wireless Outdoor AP LED status

The following figure depicts the location of the LEDs on the HiPath Wireless Outdoor AP.

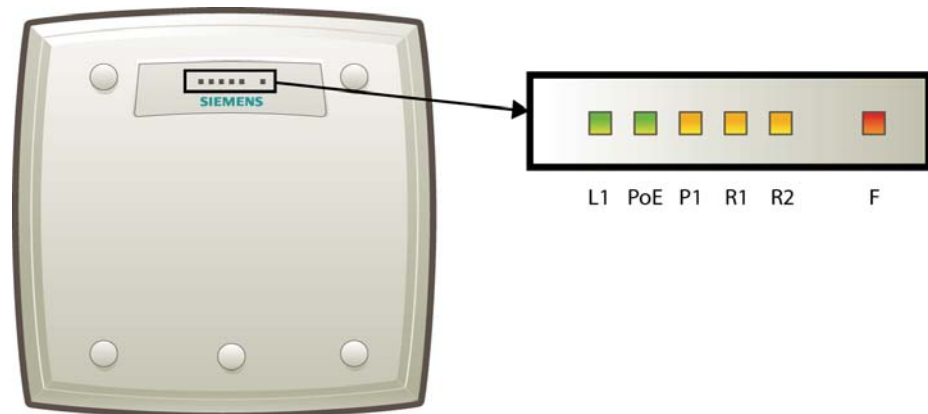


Figure 8 HiPath Wireless Outdoor AP LEDs

---

**Note:** Although the HiPath Wireless Outdoor AP has six LEDs, only R1, R2 and F LEDs are used in the current release. The remaining LEDs are disabled.

---

The Center, Left, and the Right LEDs work in conjunction to indicate the general, high-level and detailed state respectively.

The following table provides a composite view of the three LED lights of the HiPath Wireless Outdoor AP's state:

R1 LED	R2 LED	F LED	HiPath Wireless Outdoor AP's detailed status
Off	Off	Blinking Red	Initialization: Power-on-self test (POST)
	Blinking Green	Blinking Red	Initialization: Random delay
	Solid Green	Blinking Red	Initialization: Vulnerable Period
		Solid Red	Reset to factory defaults
	Solid Green	Blink Red	WDS scanning
Blinking Green/ Yellow	Off	Blinking Red	Network discovery: 802.1x authentication
		Solid Red	Failed 802.1x authentication
	Blinking Green/Yellow	Blinking Red	Network discovery: DHCP
		Solid Red	Default IP address
	Solid Green/ Yellow	Blinking Red	Network discovery: HWC discovery/ connect
		Solid Red	Discovery failed
Solid Green	Off	Blinking Red	Connecting with HWC: Registration
		Solid Red	Registration failed
	Blinking Green/Yellow	Blinking Red	Connecting with HWC: Image upgrade
		Solid Red	Image upgrade failed
	Solid Green/ Yellow	Blinking Red	Connecting with HWC: Configuration
		Solid Red	Configuration failed
	Blinking Green/Yellow	Off	AP operating and running normally: Forced image upgrade
		Solid Red	Image upgrade failed

Table 9 HiPath Wireless Outdoor AP LED status

---

**Note:** After discovery is finished, Left and Right LEDs will be Green for Ethernet uplink, and Yellow for WDS uplink.

---



---

**Note:** If the fatal AP error occurs, the Status LED will be solid Red.

---

## Configuring the Wireless AP

### Discovery and registration overview

#### 4.2.3.3 HiPath Wireless 802.11n AP LED status

Figure 9 depicts the location of the LEDs on the HiPath Wireless 802.11n .

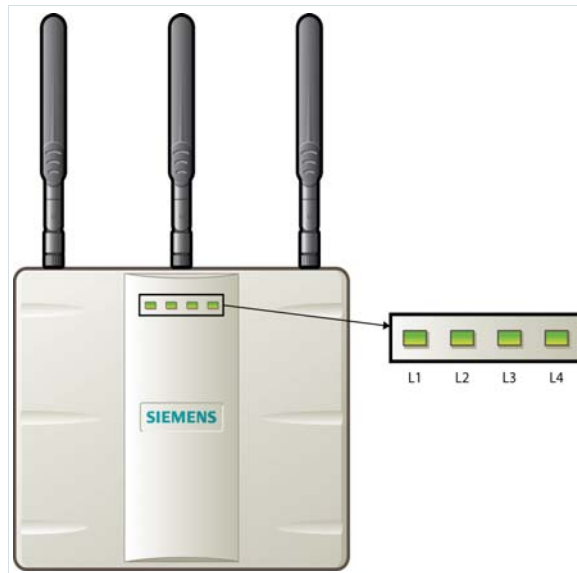


Figure 9 HiPath Wireless 802.11n AP LEDs

The LEDs, L1, L3 and L4 work in conjunction to indicate the general, high-level, and detailed state respectively.

After initialization and discovery is completed and the 802.11n AP is connected to the HiPath Wireless Controller, the LEDs L3 and L4 indicate the state of the corresponding radio — L3 for Radio 5 GHz, and L4 for Radio 2.4 GHz.

The LED L2 indicates the status of the Ethernet port.

#### LEDs color codes

The 802.11n AP LEDs indicate “normal-operation”, “warning/special”, or “failed” state of the Wireless AP in the following color codes:

- Green – Indicates the normal-operation state.
- Orange/Amber – Indicates the warning, or special state such as WDS.
- Red – Indicates the error state.
- Blinking – Indicates that the state, such as initialization, or discovery is in progress.
- Steady – Indicates that the state is stable/completed. For example, initialization finished, or discovery completed.

#### LED L1

The LED L1 indicates the general state of the 802.11n AP:



L1	HiPath Wireless 802.11n AP's general state
Blink Green	Initialization and discovery in progress
Blink Red	Error during initialization and discovery
Solid Green	Discovery finished; AP connected to the HiPath Wireless Controller

Table 10 LED L1 and Wireless AP's status

### LEDs L3 and L4

The LEDs L3 and L4 indicate the detailed state of the Wireless AP. The LED1, and LEDs L3 and L4 work in conjunction to indicate the general and detailed state of the 802.11n AP.

Table 11 provides a composite view of the three LEDs and the corresponding state of the 802.11n AP:

L3	L4	L1	HiPath Wireless 802.11n AP's detailed state
Off	Off	Blink Green	Initialization: Power-on self test (POST)
	Blink Green	Blink Green	Initialization: Random delay
	Solid Green	Blink Green	Initialization: Vulnerable period / WDS scanning
		Blink Red	Reset to factory defaults
Blink Green	Off	Blink Green	Network discovery: 802.1x authentication
		Blink Red	Failed 802.1x authentication
	Blink Green	Blink Green	Network discovery: DHCP
		Blink Red	Default IP address
	Solid Green	Blink Green	Network discovery: HWC discovery / connect
		Blink Red	Discovery failed
Solid Green	Off	Blink Green	Connecting to HWC: Registration
		Blink Red	Registration failed
	Blink Green	Blink Green	Connecting to HWC: Image upgrade
		Blink Red	Image upgrade failed
	Solid Green	Blink Green	Connecting to HWX: Configuration
		Blink Red	Configuration failed
	Blink Green	Solid Green	AO operating normally: Forced image upgrade
		Blink Red	Image upgrade failed

Table 11 LEDs L3, L4 and L1, and Wireless 802.11n AP's detailed state

After initialization and discovery is completed and the 802.11n AP is connected to the HiPath Wireless Controller, the LEDs L3 and L4 indicate the state of the corresponding radio — L3 for Radio 5 GHz, and L4 for Radio 2.4 GHz.

Figure 9 provides a view of the LEDs L3 and L4 and the corresponding radio state after the discovery is completed.

## Configuring the Wireless AP

Configuring the Wireless APs for the first time

L3/L4	Radio status
Off	Radio off
Solid Blue	Radio in HT mode
Solid Green	Radio in legacy mode

Table 12 LEDs L3 and L4, and corresponding radio state

### LED L2

The LED L2 indicates the status of the Ethernet port:

L2	Ethernet port's status
Off	No Ethernet connection
Solid Blue	1 Gb Ethernet connection
Solid Green	100 Mb connection
Solid Orange	10 Mb connection

Table 13 LED L2 and Ethernet port's status

---

**Note:** A 10 Mb Ethernet connection is considered a warning state since it is not sufficient to sustain a single radio in the legacy 11g or 11a modes.

---

## 4.3 Configuring the Wireless APs for the first time

Before the Wireless AP is configured for the first time, you must first confirm that the following has already occurred:

- The HiPath Wireless Controller has been set up. For more information, see [Chapter 3, "Configuring the HiPath Wireless Controller"](#).
- The Controller, Access Points and Convergence Software has been configured. For more information, see [Chapter 3, "Configuring the HiPath Wireless Controller"](#).
- The Wireless APs have been installed.

---

**Note:**

- If you are installing the HiPath Wireless AP, see the *HiPath Wireless AP Installation Instructions*.
  - If you are installing the HiPath Wireless 802.11n AP, see the *HiPath Wireless 802.11n AP Installation Instructions*.
  - If you are installing the HiPath Wireless Outdoor AP, see the *HiPath Wireless Outdoor AP Installation Instructions* and the *HiPath Wireless Outdoor AP Installation Guide*.
- 

Once the above processes are complete, you can then continue with the Wireless AP initial configuration. The Wireless AP initial configuration involves two steps:

- **Step One** – Define parameters for the discovery process. For more information, see [Section 4.3.1, “Defining properties for the discovery process”](#), on page 83.
- **Step Two** – Connect the Wireless AP to a power source to initiate the discovery and registration process. For more information, see [Section 4.3.2, “Connecting the Wireless AP to a power source and initiating the discovery and registration process”](#), on page 86.

### Adding a Wireless AP manually option

An alternative to the automatic discovery and registration process of the Wireless AP is to manually add and register a Wireless AP to the HiPath Wireless Controller. For more information, see [Section 4.4, “Adding and registering a Wireless AP manually”](#), on page 86.

## 4.3.1 Defining properties for the discovery process

Before a Wireless AP is configured, you must define properties for the discovery process. The discovery process is the process by which the Wireless APs determine the IP address of the HiPath Wireless Controller.

The properties that need to be defined are:

- Security mode
- Discovery timers

### Security mode

Security mode is a HiPath Wireless Controller property. It defines how the controller behaves when registering new, unknown devices. During the registration process, the HiPath Wireless Controller’s approval of the Wireless AP’s serial number depends on the security mode that has been set:

- **Allow all Wireless APs to connect**

## Configuring the Wireless AP

### Configuring the Wireless APs for the first time

- If the HiPath Wireless Controller does not recognize the registering serial number, a new registration record is automatically created for the AP (if within MDL license limit). The AP receives a default configuration. The default configuration can be the default template assignment.
- If the HiPath Wireless Controller recognizes the serial number, it indicates that the registering device is pre-registered with the controller. The controller uses the existing registration record to authenticate the AP and the existing configuration record to configure the AP.
- **Allow only approved Wireless APs to connect (this is also known as secure mode)**
  - If HiPath Wireless Controller does not recognize the AP, the AP's registration record is created in pending state (if within MDL limits). The administrator is required to manually approve a pending AP for it to provide active service. The pending AP receives minimum configuration, which only allows it to maintain an active link with the controller for future state change. The AP's radios are not configured or enabled. Pending APs are not eligible for configuration operations (VNS Assignment, default template, Radio parameters) until approved.
  - If the HiPath Wireless Controller recognizes the serial number, the controller uses the existing registration record to authenticate the AP. Following successful authentication, the AP is configured according to its stored configuration record.

---

**Note:** During the initial setup of the network, it is recommended to select the **Allow all Wireless APs to connect** option. This option is the most efficient way to get a large number of Wireless APs registered with the HiPath Wireless Controller.

Once the initial setup is complete, it is recommended that the security mode is reset to the **Allow only approved Wireless APs to connect** option. This option ensures that no unapproved Wireless APs are allowed to connect. For more information, see [Section 4.5, "Configuring Wireless AP settings"](#), on page 87.

---

### Discovery timers

The discovery timer parameters dictate the number of retry attempts and the time delay between each attempt.

#### To define the discovery process parameters:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **AP Registration**. The **Wireless AP Registration** page is displayed.

## Configuring the Wireless AP

### Configuring the Wireless APs for the first time

3. In the **Security Mode** section, select one of the following:

- **Allow all Wireless APs to connect**
- **Allow only approved Wireless APs to connect**

The **Allow all Wireless APs to connect** option is selected by default. For more information, see Section 4.3.1, “Security mode”, on page 83.

4. In the **Discovery Timers** section, type the discovery timer values in the following boxes:

- **Number of retries**
- **Delay between retries**

The number of retries is limited to 255 in a five minutes discovery period. The default number of retries is 3, and the default delay between retries is 1 second.

5. To save your changes, click **Save**.

Once the discovery parameters are defined, you can connect the Wireless AP to a power source.

## Configuring the Wireless AP

*Adding and registering a Wireless AP manually*

### 4.3.2 Connecting the Wireless AP to a power source and initiating the discovery and registration process

When a Wireless AP is powered on, it automatically begins the discovery and registration process with the HiPath Wireless Controller.

#### HiPath Wireless AP

The HiPath Wireless AP can be connected and powered in the following ways:

- Power over Ethernet (802.3af):
  - PoE enabled switch port
  - PoE Injector
- Power by AC adaptor

#### HiPath Wireless Outdoor AP

The HiPath Wireless Outdoor AP can be connected and powered in the following ways:

- Power over Ethernet
- Power by 48VDC (Direct Current)
- 110-230 VAC (Alternating Current)

For more information, see the *HiPath Wireless Outdoor Access Point V5 Installation Guide*.

#### HiPath Wireless 802.11n AP

The HiPath Wireless 802.11n can be connected and powered in the following ways:

- Power over Ethernet
- Power by AC adaptor

## 4.4 Adding and registering a Wireless AP manually

An alternative to the automatic discovery and registration process of the Wireless AP is to manually add and register a Wireless AP to the HiPath Wireless Controller. The Wireless AP is added with default settings. For more information, see [Section 4.5, "Configuring Wireless AP settings"](#), on page 87.

**To add and register a Wireless AP manually:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. Click **Add Wireless AP**. The **Add Wireless AP** page is displayed.

The screenshot shows the 'Add Wireless AP' configuration window. The title bar includes the Siemens logo and the window title 'Add Wireless AP'. The form contains the following fields:

- Serial #:** A text input field.
- Hardware Type:** A drop-down menu with 'HiPath Wireless AP2610 Internal' selected.
- Name:** A text input field.
- Role<sup>1</sup>:** A drop-down menu with 'Access Point' selected.
- Description:** A text area with up and down arrow controls.

Below the fields is an 'Add Wireless AP' button. Underneath the button, a note states: 'Wireless APs are added with default settings. Individual Wireless AP settings may be modified via Wireless AP Configuration application.'

A red footnote at the bottom left reads: '1 Sensor role is not available until TFTP is configured in Sensor Management.'

A 'Close' button is located at the bottom right of the window.

3. In the **Serial #** box, type the unique identifier.
4. In the **Hardware Type** drop-down list, click the hardware type of the Wireless AP.
5. In the **Name** box, type a unique name for the Wireless AP.
6. In the **Role** drop-down list, click the Wireless AP's role — Access Point or Sensor.
7. In the **Description** box, type descriptive comments for the Wireless AP.
8. Click **Add Wireless AP**. The Wireless AP is added and registered.  
  
When a Wireless AP is added manually, it is added to the controller database only and does not get assigned.
9. Click **Close**.

## 4.5 Configuring Wireless AP settings

Wireless APs are added with default settings, which you can adjust and configure according to your network requirements. In addition, you can modify the properties and the settings for each radio on the Wireless AP.

## Configuring the Wireless AP

### Configuring Wireless AP settings

You can also locate and select Wireless APs in specific registration states to modify their settings. For example, this feature is useful when approving pending Wireless APs when there are a large number of other Wireless APs that are already registered. On the **Access Approval** page, click **Pending** to select all pending Wireless APs, then click **Approve** to approve all selected Wireless APs.

Configuring Wireless AP settings can include the following processes:

- [Modifying a Wireless AP's status](#)
- [Modifying a Wireless AP's properties](#)
- [Modifying Wireless AP radio properties](#)
- [Setting up the Wireless AP using static configuration](#)
- [Setting up 802.1x authentication for a Wireless AP](#)

When configuring Wireless APs, you can choose to configure individual Wireless APs or simultaneously configure a group of Wireless APs. For more information, see [Section 4.8, "Configuring Wireless APs simultaneously"](#), on page 139.

### 4.5.1 Modifying a Wireless AP's status

If during the discovery process, the HiPath Wireless Controller security mode was **Allow only approved Wireless APs to connect**, then the status of the Wireless AP is Pending. You must modify the security mode to **Allow all Wireless APs to connect**. For more information, see [Section 4.3.1, "Security mode"](#), on page 83.

**To modify a Wireless AP's registration status:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **Access Approval**. The **Access Approval** page is displayed, along with the registered Wireless APs and their status.



## Configuring the Wireless AP

### Configuring Wireless AP settings

The screenshot shows the Siemens HiPath Wireless AP configuration interface. The main content area is titled "Access Approval" and contains a table of Wireless APs. The table has columns for "Wireless APs", "Home", and "Status". Each row has a checkbox in the "Wireless APs" column. To the right of the table are two sections of buttons: "Select Wireless APs:" with buttons for "Select All", "Approved", "Pending", "Local", "Foreign", and "Clear All"; and "Perform action on selected Wireless AP:" with buttons for "Approved", "Sensor", "Pending", "Release", and "Delete".

Wireless APs	Home	Status
<input type="checkbox"/> 0002000007515346 00:0E:8C:8F:E6:71	Local	Approved
<input type="checkbox"/> 0409920201202222	Local	Approved
<input type="checkbox"/> 0500006052050362	Local	Approved
<input type="checkbox"/> 0500006052050423	Local	Approved
<input type="checkbox"/> 0500006062051024	Local	Approved
<input type="checkbox"/> 0500006062051033	Local	Approved
<input type="checkbox"/> 0500006062051040	Local	Approved
<input type="checkbox"/> 0500006062051048	Local	Approved
<input type="checkbox"/> 0500006062051111	Local	Approved
<input type="checkbox"/> 0500006062051121	Local	Approved
<input type="checkbox"/> 0500006062051124	Local	Approved
<input type="checkbox"/> 0500006062051130	Local	Approved
<input type="checkbox"/> 0500006062051151	Local	Approved
<input type="checkbox"/> 0500006062051154	Local	Approved
<input type="checkbox"/> 0500006062051157	Local	Approved
<input type="checkbox"/> 0500006062051159	Local	Approved

3. To select the Wireless APs for status change, do one of the following:
  - For a specific Wireless AP, select the corresponding checkbox.
  - For Wireless APs by category, click one of the **Select Wireless APs** options.

**Note:** You must consider all the three AP variants — HiPath Wireless AP, HiPath Wireless Outdoor AP, and HiPath Wireless 802.11n AP — as **Local**.

To clear your Wireless AP selections, click **Clear All**.

4. Click the appropriate **Perform action on selected Wireless APs** option:
  - **Approved** – Change a Wireless AP's status from Pending to Approved, if the **AP Registration** page was set to register only approved Wireless APs.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Approved as Sensor** – AP ceases performing RF services and begins performing scanning services. For more information, see [Section 4.9, “Configuring an AP as a sensor”](#), on page 141.

---

**Note:** Only approve an AP as a sensor if HiPath HiGuard has been installed on your HiPath Wireless Manager. For more information, see the *HiPath Wireless Manager User Guide*.

---

---

**Note:** The HiPath Wireless Outdoor AP and the Wireless 802.11n AP cannot work as a sensor; you cannot assign the sensor role to the HiPath Wireless Outdoor AP or the Wireless 802.11n AP.

---

- **Pending** – AP is removed from the Active list, and is forced into discovery.
- **Release** – Release foreign Wireless APs after recovery from a failover. Releasing an AP corresponds to the Availability functionality. For more information, see [Chapter 7, “Availability, mobility, and controller functionality”](#).
- **Delete** – Releases the Wireless AP from the HiPath Wireless Controller and deletes the Wireless AP’s entry in the HiPath Wireless Controller’s management database.

## 4.5.2 Modifying a Wireless AP’s properties

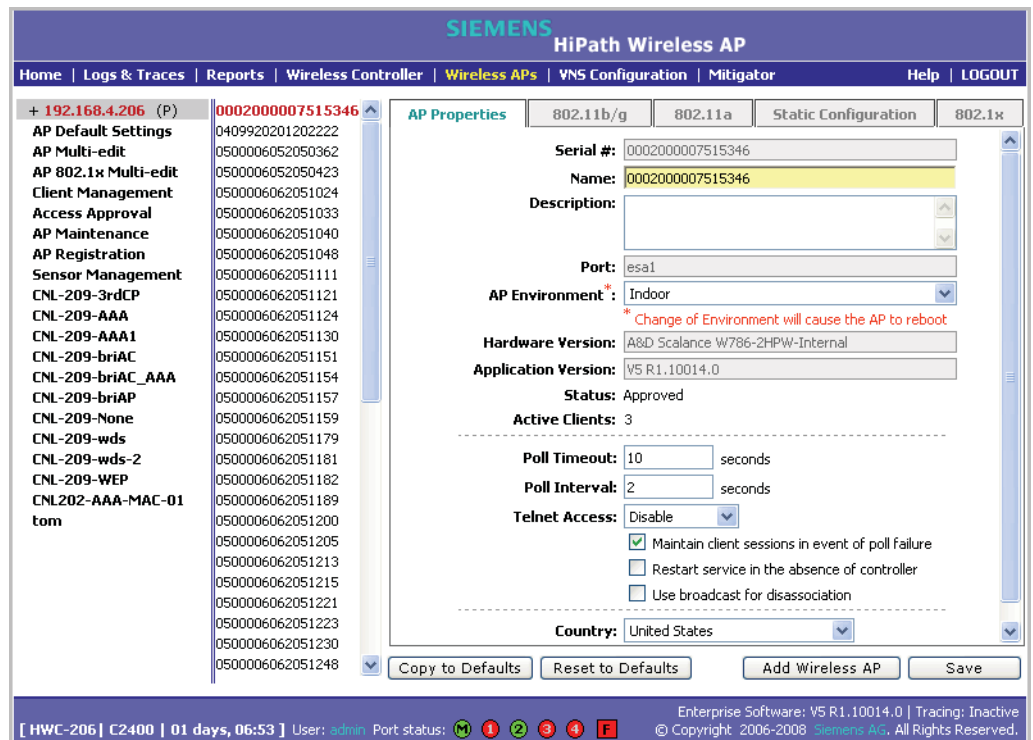
Once a Wireless AP has successfully registered, you can then modify its properties. Modifying an AP’s properties can include modifying properties on the following tabs:

- **AP properties**
- **802.11b/g/n**
- **802.11a/n**
- **Static Configuration**
- **802.1x**

You can modify a Wireless AP’s properties based on its role either as an access point or as a sensor. For more information, see [Section 4.9, “Configuring an AP as a sensor”](#), on page 141.

**To modify a Wireless AP's properties as an access point:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the **Wireless AP** list, click the Wireless AP whose properties you want to modify. The **AP Properties** tab displays Wireless AP information.



3. Modify the Wireless AP's information:

- **Name** – Type a unique name for the Wireless AP that identifies the AP. The default value is the Wireless AP's serial number.
- **Description** – Type comments for the Wireless AP.
- **AP Environment** – Click the Wireless AP's environment — **Indoor** or **Outdoor**.

---

**Note:** The **AP Environment** drop-down is displayed on the **AP Properties** tab only if the selected Wireless AP is the HiPath Outdoor Wireless AP. Since the HiPath Outdoor Wireless AP can be deployed in both indoor and outdoor environments, the **AP Properties** page enables you to specify the environment.

---

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Role** – Click the role for the Wireless AP, either **Access Point** or **Sensor**. Once the Wireless AP is configured as **Sensor**, it no longer performs RF services, and is no longer managed by the HiPath Wireless Controller.

---

**Note:** The **Role** drop-down is displayed on the **AP Properties** page only if the selected Wireless AP is the HiPath Wireless AP 2610/2620.

Since only the HiPath Wireless AP can perform the role of a sensor, the **AP Properties** tab enables you to specify the Wireless AP's role.

If the selected Wireless AP is the HiPath Outdoor Wireless AP or the Wireless 802.11n AP, the **AP Properties** tab will not display the **Role** drop-down; the HiPath Outdoor Wireless AP and Wireless 802.11n AP cannot perform the role of a sensor.

---

- **Poll Timeout** – Type the timeout value, in seconds, for the Wireless AP to re-establish the link with the HiPath Wireless Controller if it (Wireless AP) does not get an answer to its polling. The default value is 15 seconds.
- **Poll Interval** – Type the interval value, in seconds, for polling the controller. The default value is 2 seconds.
- **Telnet Access** – Click to enable or disable Telnet Access to the Wireless AP.
- **Maintain client session in event of poll failure** – Select this option (if using a bridged at AP VNS) if the AP should remain active if a link loss with the controller occurs. This option is enabled by default.
- **Restart service in the absence of controller** – Select this option (if using a bridged at AP VNS) to ensure the Wireless APs' radios continue providing service if the Wireless AP's connection to the HiPath Wireless Controller is lost. If this option is enabled, it allows the Wireless AP to start a bridged at AP VNS even in the absence of a HiPath Wireless Controller.
- **Use broadcast for disassociation** – Select if you want the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This will affect the behavior of the AP under the following conditions:
  - If the Wireless AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection).
  - If a BSSID is deactivated or removed on the Wireless AP.

This option is disabled by default.

---

**Note:** The **Maintain client session in event of poll failure**, the **Restart service in the absence of controller**, and the **Use broadcast for disassociation** options are not displayed on the **AP Properties** page if the selected Wireless AP is a Wireless 802.11n AP (AP3610/AP3620).

---

- **Country** – Click the country of operation. This option is only available with some licenses.

The following on the **AP Properties** tab are view only:

- **Serial #** – Displays a unique identifier that is assigned during the manufacturing process.
- **Port** – Displays the Ethernet port of the HiPath Wireless Controller the Wireless AP is connected to.
- **Hardware Version** – Displays the current version of the Wireless AP hardware.
- **Application Version** – Displays the current version of the Wireless AP software.
- **Status:**
  - **Approved** – Indicates that the Wireless AP has received its binding key from the HiPath Wireless Controller after the discovery process.
  - **Pending** – Indicates that the Wireless AP has not yet successfully been approved for access with the secure controller.

You can modify the status of a Wireless AP on the **Access Approval** page. For more information, see [Section 4.5.1, “Modifying a Wireless AP’s status”](#), on page 88

- **Active Clients** – Displays the number of wireless devices currently active on the Wireless AP.

4. To save your changes, click **Save**.

**To modify a Wireless AP’s properties as a sensor:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the **Wireless AP** list, click the Wireless AP whose properties you want to modify. The **AP Properties** tab displays Wireless AP information.

## Configuring the Wireless AP

### Configuring Wireless AP settings

The screenshot shows the Siemens HiPath Wireless AP configuration interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar lists various configuration options, with 'AP Properties' selected. The main content area displays the 'AP Properties' form for a specific AP. The form includes the following fields:

- Serial #:** 0500006092051170
- Name:** 0500006092051170
- Description:** 0500006092051170
- Hardware Version:** Siemens Wireless AP 2610 internal
- Role:** Sensor

At the bottom of the form, there are four buttons: 'Copy to Defaults', 'Reset to Defaults', 'Add Wireless AP', and 'Save'. The status bar at the bottom of the interface shows 'Enterprise Software: V5 R1.10014.0 | Tracing: Inactive' and '© Copyright 2006-2008 Siemens AG. All Rights Reserved.'.

#### 3. Modify the Wireless AP's information:

- **Name** – Type a unique name for the Wireless AP that identifies the AP. The default value is the Wireless AP's serial number.
- **Description** – Type comments for the Wireless AP.
- **Role** – Click the role for the AP, either **Access Point** or **Sensor**. Once the AP is configured as a **Sensor**, the AP no longer performs RF services and is no longer managed by the HiPath Wireless Controller. For more information, see [Section 4.9, "Configuring an AP as a sensor"](#), on page 141.

#### 4. To save your changes, click **Save**.

### 4.5.3 Modifying Wireless AP radio properties

Most properties of the Wireless AP radios can be modified without requiring a reboot of the Wireless AP. However, if the modification of a Wireless AP property does trigger a reboot, the Wireless AP property is identified with a red asterisk in the HiPath Wireless Assistant.

---

**Note:** Modifying Wireless AP radio properties can vary significantly depending on the model of the Wireless AP you are configuring:

- For specific information on modifying a Wireless 802.11n AP, see [Section 4.5.3.1, “Modifying Wireless 802.11n AP 3610/3620 radio properties”](#), on page 96.
  - For specific information on modifying a Wireless AP 2610/2620 or HiPath Wireless Outdoor AP, see [Section 4.5.3.2, “Modifying Wireless AP 2610/2620 radio properties”](#), on page 106.
- 

#### **Dynamic Radio Management (DRM)**

When you modify a Wireless AP’s radio properties, the Dynamic Radio Management (DRM) functionality of the HiPath Wireless Controller is used to help establish the optimum radio configuration for your Wireless APs. DRM is enabled by default. The HiPath Wireless Controller’s DRM:

- Adjusts transmit power levels to balance coverage between Wireless APs assigned to the same RF domain and operating on the same channel.
  - Scans and coordinates with other Wireless APs to select an optimal operating channel.
- 

**Note:** The Wireless 802.11n AP does not support the DRM functionality of the HiPath Wireless Controller.

---

The DRM feature is comprised of two functions:

- **Auto Channel Selection (ACS)** – ACS provides an easy way to optimize channel arrangement based on the current situation in the field. ACS provides an optimal solution only if it is triggered on all Wireless APs in a deployment. Triggering ACS on a single Wireless AP or on a subset of Wireless APs provides a useful but suboptimal solution. Also, ACS only relies on the information observed at the time it is triggered. Once a Wireless AP has selected a channel, it will remain operating on that channel until the user changes the channel or triggers ACS. ACS can be triggered by one of the following events:
  - A new Wireless AP registers with the HiPath Wireless Controller and the **AP Default Settings** channel is **Auto**.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- A user selects the **Auto** channel from the Wireless AP's radio configuration tabs.
- A user selects the **Auto** channel from the **AP Multi-edit** page.
- A Wireless AP detects radar on its current operating channel and it employs ACS to select a new channel
- **Auto Tx Power Control (ATPC)** – ATPC guarantees your LAN a stable RF environment by automatically adapting transmission power signals according to the coverage provided by the Wireless APs. ATPC can be either enabled or disabled.

#### Wireless APs and the sensor role

When an Wireless AP is assigned to the sensor role, its configuration data is preserved on the HiPath Wireless Controller. The configuration data can only be modified when the Wireless AP is switched back to the Wireless AP role.

In addition, if a Wireless AP is assigned to the sensor role, the **802.11b/g**, **802.11a**, and **Static Configuration** tabs are not visible.

---

**Note:** The HiPath Wireless Outdoor AP and the Wireless 802.11n AP cannot work as a sensor; you cannot assign the sensor role to the HiPath Wireless Outdoor AP or the Wireless 802.11n AP.

---

#### 4.5.3.1 Modifying Wireless 802.11n AP 3610/3620 radio properties

The Wireless 802.11n AP 3610/3620 is a 802.11n (draft)-compliant access point. The following section discusses how to modify a Wireless 802.11n AP.

For information on how to modify a Wireless AP 2610/2620 or the HiPath Wireless Outdoor AP, see [Section 4.5.3.2, “Modifying Wireless AP 2610/2620 radio properties”](#), on page 106.

#### Channel bonding

Channel bonding improves the effective throughput of the wireless LAN. In contrast to the Wireless AP 26xx which uses radio channel spacings that are only 20MHz wide, the Wireless 802.11n AP can use two channels at the same time to create a 40MHz wide channel. To achieve a 40MHz channel width, the Wireless 802.11n AP employs channel bonding — two 20MHz channels at the same time.

The 40MHz channel width is achieved by bonding the primary channel (20MHz) with an extension channel that is either 20MHz above (bonding up) or 20MHz below (bonding down) of the primary channel.

Depending on the radio protocols, channel bonding can be predefined:



- **802.11b/g/n** – Any channel can bond up or down as long as the band edge is not exceeded.
- **802.11a/n** – Bonding pairs are predefined.

Channel bonding is enabled by selecting the **Channel Width** on the **802.11b/g/n** and **802.11a/n** tabs. When selecting **Channel Width**, the following options are available:

- **20MHz** – Channel bonding is not enabled:
  - 802.11n clients use the primary channel (20MHz)
  - Non-802.11n clients, beacons, and multicasts use the 802.11a/b/g radio protocols.
- **40MHz** – Channel bonding is enabled:
  - 802.11n clients that support the 40MHz frequency can use 40MHz, 20MHz, or the 802.11a/b/g radio protocols.
  - 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11a/b/g radio protocols.
  - Non-802.11n clients, beacons, and multicasts use the 802.11a/b/g radio protocols.
  - If the primary channel allows for both bonding types (up and down), you can click the channel bond type from the **Channel Bonding** drop-down list.
  - If the primary channel allows for one of the bonding types (up or down), the channel bond type is displayed in the **Channel Bonding** drop-down list.
- **Auto** – Channel bonding is automatically enabled or disabled, switching between 20MHz and 40MHz, depending on how busy the extension channel is. If the extension channel is busy above a prescribed threshold percentage, which is defined in the **40MHz Channel Busy Threshold** box, channel bonding is disabled.

#### **Channel selection — primary and extension**

The primary channel of the Wireless 802.11n AP is selected from the **Request New Channel** drop-down list. If **auto** is selected, the ACS feature selects the primary channel. Depending on the primary channel that is selected, channel bonding may be allowed: up, down, both, or neither.

#### **Guard interval**

The guard intervals ensure that individual transmissions do not interfere with one another. The Wireless 802.11n AP provides a shorter guard interval that increases the channel throughput. When a 40MHz channel is used, you can

## Configuring the Wireless AP

### Configuring Wireless AP settings

select the guard interval to improve the channel efficiency. The guard interval is selected from the **Guard Interval** drop-down list. Longer guard periods reduce the channel efficiency.

### Aggregate MSDU and MPDU

The Wireless 802.11n AP provides aggregate Mac Service Data Unit (MSDU) and aggregate Mac Protocol Data Unit (MPDU) functionality, which combines multiple frames together into one larger frame for a single delivery. This aggregation reduces the overhead of the transmission and results in increased throughput. The aggregate methods are enabled and defined selected from the **Aggregate MSDUs** and **Aggregate MPDUs** drop-down lists.

### To modify Wireless 802.11n AP radio properties:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. Click the appropriate Wireless 802.11n AP in the list.
3. If applicable, click the **802.11b/g/n** tab to modify the radio properties:

Each tab displays the radio settings for each radio on the Wireless AP. If the radio has been assigned to a VNS, the VNS names and MAC addresses are displayed in the **Base Settings** section. The HiPath Wireless Controller can support the following:

- C2400 – Up to 64 VNSs

- C20 – Up to 8 VNSs

The Wireless 802.11n AP radios can be assigned to each of the configured VNSs in a system. Each radio can be the subject of 8 VNS assignments (corresponding to the number of SSIDs it can support). Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

The **BSS Info** section is view only. After VNS configuration, the **Basic Service Set (BSS)** section displays the MAC address on the Wireless AP for each VNS and the SSIDs of the VNSs to which this radio has been assigned.

4. In the **Base Settings** section, do the following:

- **Radio Mode** – Click one of the following radio options:
  - **b** – Click to select the 802.11b-only mode of the 802.11b/g/n radio. If selected, the AP will use only 11b (CCK) rates with all associated clients.
  - **b/g** – Click to select both the 802.11g mode and the 802.11b mode of the 802.11b/g/n radio. If selected, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients. The AP will not transmit or receive 11n rates.
  - **b/g/n** – Click to select b/g/n modes of the 802.11b/g/n radio. If selected, the AP will use all available 11b, 11g, and 11n rates.
  - **off** – Click to disable the 802.11b/g/n radio.

---

**Note:** Depending on the radio options you select, some of the radio settings may not be available for configuration.

---

- **Channel Width** – Click the channel width for the radio:
  - **20MHz** – Click to allow 802.11n clients to use the primary channel (20MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11b/g radio protocols.
  - **40MHz** – Click to allow 802.11n clients that support the 40MHz frequency to use 40MHz, 20MHz, or the 802.11b/g radio protocols. 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11b/g radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11b/g radio protocols.
  - **Auto** – Click to automatically switch between 20MHz and 40MHz channel widths, depending on how busy the extension channel is.
- **DTIM Period** – Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is 5.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Beacon Period** – Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
  - **RTS/CTS Threshold** – Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
  - **Frag. Threshold** – Type the fragment size threshold, in bytes, above which the packets will be fragmented by the Wireless 802.11n AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
5. In the **Basic Radio Settings** section, do the following:

- **Request New Channel** – Click the wireless channel you want the Wireless 802.11n AP to use to communicate with wireless devices.

Click **Auto** to request the ACS to search for a new channel for the Wireless 802.11n AP, using a channel selection algorithm. This forces the Wireless 802.11n AP to go through the auto-channel selection process again.

Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see [Appendix B, “Regulatory information”](#).

- **Channel Bonding** – Click the bonding method, **Up** or **Down**. The primary channel (20MHz) is bonded with an extension channel that is either 20MHz above (bonding up) or 20MHz below (bonding down) of the primary channel. Depending on the channel that is selected in the **Request New Channel** drop-down list, you may be prevented from bonding **Up** or **Down** in the **Channel Bonding** drop-down list.
- **Guard Interval** – Click a guard interval, **Long** or **Short**, when a 40MHz channel is used. It is recommended to use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).
- **Max Tx Power** – Click the maximum Tx power level that the range of transmit power can be adjusted: **0** to **17** dBm. It is recommended to use **17 dBm** to not limit the potential Tx power level range that can be used.
- **Current Channel** – This field is view only. It displays the actual channel the ACS has assigned to the Wireless 802.11n AP radio. The **Current Channel** value and the **Last Requested Channel** value may be different because the ACS automatically assigns the best available channel to the Wireless 802.11n AP, ensuring that a Wireless 802.11n AP's radio is always operating on the best available channel.

- **Last Requested Channel** – This field is view only. This field displays the last wireless channel that you had selected for the Wireless AP to communicate with the wireless devices.
  - **Auto Tx Power Ctrl (ATPC)** – The Wireless 802.11n AP does not support the DRM functionality of the HiPath Wireless Controller and its related ATPC feature.
  - **Current Tx Power Level** – This field is view only. It displays the actual Tx power level assigned to the Wireless 802.11n AP radio.
6. In the **11b Settings** section, do the following:
- **Preamble** – Click a preamble type for 11b-specific (CCK) rates: **Short** or **Long**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this Wireless 802.11n AP. Click **Long** if compatibility with pre-11b clients is required.
7. In the **11g Settings** section, do the following:
- **Protection Mode** – Click a protection mode: **None** or **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
  - **Protection Type** – Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

---

**Note:** The overall throughput is reduced when **Protection Mode** is enabled, due to the additional overhead caused by the RTS/CTS. The overhead is minimized by setting **Protection Type** to **CTS Only**. Although, the overhead causes the overall throughput to be sometimes lower than if just 11b mode is used. If there are many 11b clients, it is recommended to disable 11g support (11g clients are backward compatible with 11b APs).

An alternate approach, although a more expensive method, is to dedicate all APs on a channel for 11b (for example, disable 11g on these APs) and disable 11b on all other APs. The difficulty with this method is that the number of APs must be increased to ensure coverage separately for 11b and 11g clients.

---

8. In the **11n Settings** section, do the following:
- **Protection Mode** – Click a protection mode: **Enabled** or **Disabled**. This protects high throughput transmissions on primary channels from non-11n APs and clients. Click **Disabled** if non-11n APs and clients are not expected. Click **Enabled** if you expect many non-11n APs and clients. The overall throughput is reduced when **Protection Mode** is enabled.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **40MHz Protection Mode** – Click a protection type, **CTS Only** or **RTS-CTS**, or **None**, when a 40MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
  - **40MHz Prot. Channel Offset** – Select a 20MHz channel offset if the deployment is using channels that are 20MHz apart (for example, using channels **1, 5, 9, and 13**) or a 25MHz channel offset if the deployment is using channels that are 25MHz apart (for example, using channels **1, 6, and 11**).
  - **40MHz Channel Busy Threshold** – Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40MHz).
  - **Aggregate MSDUs** – Click an aggregate MSDU mode: **Enabled** or **Disabled**. Aggregate MSDU increases the maximum frame transmission size.
  - **Aggregate MSDU Max Length** – Type the maximum length of the aggregate MSDU. The value range is 2290-4096 bytes.
  - **Aggregate MPDUs** – Click an aggregate MPDU mode: **Enabled** or **Disabled**. Aggregate MPDU provides a significant improvement in throughput .
  - **Aggregate MPDU Max Length** – Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
  - **Agg. MPDU Max # of Sub-frames** – Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
  - **ADDBA Support** – Click an ADDBA support mode: **Enabled** or **Disabled**. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. **ADDBA Support** must be enabled if **Aggregate APDU** is enable.
9. If applicable, click the **802.11a/n** tab to modify the radio properties:

## Configuring the Wireless AP

### Configuring Wireless AP settings

10. In the **Base Settings** section, do the following:

- **Radio Mode** – Click one of the following radio options:
  - **a** – Click to enable only the 802.11a mode of the 802.11a/n radio. If disabled, the Wireless 802.11n AP will not accept associations from 11a clients.
  - **a/n** – Click to enable both the 802.11a mode and the 802.11n mode of the 802.11ba/n radio.
  - **off** – Click to disable the 802.11a/n radio.

---

**Note:** Depending on the radio options you select, some of the radio settings may not be available for configuration.

---

- **Channel Width** – Click the channel width for the radio:
  - **20MHz** – Click to allow 802.11n clients to use the primary channel (20MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11a radio protocols.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **40MHz** – Click to allow 802.11n clients that support the 40MHz frequency to use 40MHz, 20MHz, or the 802.11a radio protocols. 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11a radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11a radio protocols.
- **Auto** – Click to automatically switch between 20MHz and 40MHz channel widths, depending on how busy the extension channel is.
- **DTIM Period** – Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** – Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS Threshold** – Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** – Type the fragment size threshold, in bytes, above which the packets will be fragmented by the Wireless 802.11n AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.

11. In the **Basic Radio Settings** section, do the following:

- **Request New Channel** – Click the wireless channel you want the Wireless 802.11n AP to use to communicate with wireless devices.

Click **Auto** to request the ACS to search for a new channel for the Wireless AP, using a channel selection algorithm. This forces the Wireless 802.11n AP to go through the auto-channel selection process again.

Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see [Appendix B, “Regulatory information”](#).

- **Guard Interval** – Click a guard interval, **Long** or **Short**, when a 40MHz channel is used. It is recommended to use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).
- **Max Tx Power** – Click the maximum Tx power level that the range of transmit power can be adjusted: **0** to **22** dBm. It is recommended to use **22 dBm** to not limit the potential Tx power level range that can be used.



- **Current Channel** – This field is view only. It displays the actual channel the ACS has assigned to the Wireless 802.11n AP radio. The **Current Channel** value and the **Request New Channel** value may be different because the ACS automatically assigns the best available channel to the Wireless 802.11n AP, ensuring that a Wireless 802.11n AP's radio is always operating on the best available channel.
- **Last Requested Channel** – This field displays the last wireless channel that you had selected for the Wireless 802.11n AP to communicate with the wireless devices.
- **Auto Tx Power Ctrl (ATPC)** – The Wireless 802.11n AP does not support the DRM functionality of the HiPath Wireless Controller and its related ATPC feature.
- **Current Tx Power Level** – This field is view only. It displays the actual Tx power level assigned to the Wireless 802.11n AP radio.

12. In the **11n Settings** section, do the following:

- **Protection Mode** – Click a protection mode: **Enabled** or **Disabled**. This protects high throughput transmissions on primary channels from non-11n APs and clients. Click **Disabled** if non-11n APs and clients are not expected. Click **Enabled** if you expect many non-11n APs and clients. The overall throughput is reduced when **Protection Mode** is enabled.
- **40MHz Protection Mode** – Click a protection type, **CTS Only** or **RTS-CTS**, or **None**, when a 40MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
- **40MHz Prot. Channel Offset** – Select a 20MHz channel offset if the deployment is using channels that are 20MHz apart (for example, using channels **1, 5, 9, and 13**) or a 25MHz channel offset if the deployment is using channels that are 25MHz apart (for example, using channels **1, 6, and 11**).
- **40MHz Channel Busy Threshold** – Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40MHz).
- **Aggregate MSDUs** – Click an aggregate MSDU mode: **Enabled** or **Disabled**. Aggregate MSDU increases the maximum frame transmission size.
- **Aggregate MSDU Max Length** – Type the maximum length of the aggregate MSDU. The value range is 2290-4096 bytes.
- **Aggregate MPDUs** – Click an aggregate MPDU mode: **Enabled** or **Disabled**. Aggregate MPDU provides a significant improvement in throughput .

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Aggregate MPDU Max Length** – Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
- **Agg. MPDU Max # of Sub-frames** – Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
- **ADDBA Support** – Click an ADDBA support mode: **Enabled** or **Disabled**. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. **ADDBA Support** must be enabled if **Aggregate APDU** is enable.

13. To save your changes, click **Save**.

### 4.5.3.2 Modifying Wireless AP 2610/2620 radio properties

The following section discusses how to modify a Wireless AP 2610/2620 and the HiPath Wireless Outdoor AP. For information on how to modify a Wireless 802.11n AP 3610/3620, see [Section 4.5.3.1, “Modifying Wireless 802.11n AP 3610/3620 radio properties”](#), on page 96.

#### To modify the Wireless AP’s radio properties:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. Click the appropriate Wireless AP in the list.
3. Click the radio tab you want to modify.

Each tab displays the radio settings for each radio on the Wireless AP. If the radio has been assigned to a VNS, the VNS names and MAC addresses appear in the **Base Settings** section. The HiPath Wireless Controller can support the following:

- C2400 – Up to 64 VNSs
- C20 – Up to 8 VNSs

The Wireless AP radios can be assigned to each of the configured VNSs in a system. Each radio can be the subject of 8 VNS assignments (corresponding to the number of SSIDs it can support). Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

The **BSS Info** section is view only. After VNS configuration, the **Basic Service Set (BSS)** section displays the MAC address on the Wireless AP for each VNS and the SSIDs of the VNSs to which this radio has been assigned.

4. If applicable, click the **802.11b/g** tab to modify the radio properties:

## Configuring the Wireless AP

### Configuring Wireless AP settings

5. In the **Base Settings** section, do the following:

- **Radio Mode** – Click one of the following radio options:
  - **b** – Click to select the 802.11b-only mode of the 802.11b/g radio. If selected, the AP will use only 11b (CCK) rates with all associated clients. The AP will not transmit or receive 11g rates.
  - **g** – Click to select the 802.11g-only mode of the 802.11b/g radio. If selected, the AP will not accept associations from 11b clients, but it will still use all CCK and OFDM 11g rates with its associated clients. To disable CCK rates, use the **Min/Max Basic Rate** and **Max Operation Rate** controls to select OFDM-only rates.
  - **b/g** – Click to enable both the 802.11g mode and the 802.11b mode of the 802.11b/g radio. If selected, the AP will accept associations from all clients and use all available 11b and 11g rates.
  - **off** – Click to disable the 802.11b/g radio.
- **DTIM Period** – Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is 5.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Beacon Period** – Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
  - **RTS/CTS Threshold** – Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
  - **Frag. Threshold** – Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
6. In the **Basic Radio Settings** section, do the following:
- **RF Domain** – Type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 15 characters. The RF Domain is used to identify a group of Wireless APs.
  - **Request New Channel** – Click the wireless channel you want the Wireless AP to use to communicate with wireless devices.

Click **Auto** to request the ACS to search for a new channel for the Wireless AP, using a channel selection algorithm. This forces the AP to go through the auto-channel selection process again.

Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see [Appendix B, “Regulatory information”](#).

- **Current Channel** – This field is view only. It displays the actual channel the ACS has assigned to the Wireless AP radio. The Current Channel value and the Requested Channel value may be different because the ACS automatically assigns the best available channel to the Wireless AP, ensuring that a Wireless AP's radio is always operating on the best available channel.
- **Last Requested Channel** – This field is view only. This field displays the last wireless channel that you had selected for the Wireless AP to communicate with the wireless devices.
- **Auto Tx Power Ctrl (ATPC)** – Click to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Wireless APs. After a period of time, the system will stabilize itself based on the RF coverage of your Wireless APs.
- **Current Tx Power Level** – This field is view only. It displays the actual Tx power level assigned to the Wireless AP radio.

- **Max Tx Power** – Click the maximum Tx power level that the range of transmit power can be adjusted: **8, 9, 10, 11, 12, 13, 14, 15, 16, 17,** and **18** dBm. It is recommended to use **18 dBm** to not limit the potential Tx power level range that can be used.
- **Min Tx Power** – If ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted: **8, 9, 10, 11, 12, 13, 14, 15, 16, 17,** and **18** dBm. It is recommended to click **8 dBm** to not limit the potential Tx power level range that can be used.
- **Auto Tx Power Ctrl Adjust** – If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to click **0 dBm** during your initial configuration. If you have an RF plan that recommended Tx power levels for each Wireless AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Rx Diversity** – Click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** – Click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Best** that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Best**. Under those circumstances, it is recommended to use either **Left** or **Right** for Tx Diversity. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Min Basic Rate** – Click the minimum data rate that must be supported by all stations in a BSS: **1, 2, 5.5,** or **11** Mbps for 11b and 11b+11g modes. Click **1, 2, 5.5, 6, 11, 12,** or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6, 12,** or **24** Mbps) all basic rates will be 11g-specific.
- **Max Basic Rate** – Click the maximum data rate that must be supported by all stations in a BSS: **1, 2, 5.5,** or **11** Mbps for 11b and 11b+11g modes. Click **1, 2, 5.5, 6, 11, 12,** or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6, 12,** or **24** Mbps) all basic rates will be 11g-specific.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Max Operational Rate** – Click the maximum data rate that clients can operate at while associated with the AP: **1, 2, 5.5,** or **11** Mbps for 11b-only mode. Click **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 28,** or **54** Mbps for 11b+11g or 11g-only modes. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
  - **No of Retries for Background BK** – Click the number of retries for the Background transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
  - **No of Retries for Best Effort BE** – Click the number of retries for the Best Effort transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
  - **No of Retries for Video VI** – Click the number of retries for the Video transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
  - **No of Retries for Voice VO** – Click the number of retries for the Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
  - **No of Retries for Turbo Voice TVO** – Click the number of retries for the Turbo Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
7. In the **11b Settings** section, do the following:
- **Preamble** – Click a preamble type for 11b-specific (CCK) rates: **Short** or **Long**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Click **Long** if compatibility with pre-11b clients is required.
8. In the **11g Settings** section, do the following:
- **Protection Mode** – Click a protection mode: **None, Auto,** or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
  - **Protection Rate** – Click a protection rate: **1, 2, 5.5,** or **11** Mbps. The default and recommended setting is **11**. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than **11** Mbps are required to ensure coverage.

- **Protection Type** – Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

**Note:** The overall throughput is reduced when **Protection Mode** is enabled, due to the additional overhead caused by the RTS/CTS. The overhead is minimized by setting **Protection Type** to **CTS Only** and **Protection Rate** to **11 Mbps**. Although, the overhead causes the overall throughput to be sometimes lower than if just 11b mode is used. If there are many 11b clients, it is recommended to disable 11g support (11g clients are backward compatible with 11b APs).

An alternate approach, although a more expensive method, is to dedicate all APs on a channel for 11b (for example, disable 11g on these APs) and disable 11b on all other APs. The difficulty with this method is that the number of APs must be increased to ensure coverage separately for 11b and 11g clients.

9. If applicable, click the **802.11a** tab to modify the radio properties:

10. In the **Base Settings** section, do the following:

- **Radio Mode** – Click one of the following radio options:
  - **a** – Click to enable the 802.11a radio.
  - **off** – Click to disable the 802.11a radio.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **DTIM Period** – Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** – Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS Threshold** – Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** – Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.

11. In the **Basic Radio Settings** section, do the following:

- **RF Domain** – Type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 15 characters. The RF Domain is used to identify a group of Wireless APs.
- **Current Channel** – This field is view only. It displays the actual channel the ACS has assigned to the Wireless AP radio. The Current Channel value and the Requested Channel value may be different because the ACS automatically assigns the best available channel to the Wireless AP, ensuring that a Wireless AP's radio is always operating on the best available channel.
- **Last Requested Channel** – This field displays the last wireless channel that you had selected for the Wireless AP to communicate with the wireless devices.
- **Requested New Channel** – Click the wireless channel you want the Wireless AP to use to communicate with wireless devices.

Click **Auto** to request the ACS to search for a new channel for the Wireless APs, using a channel selection algorithm. This forces the APs to go through the auto-channel selection process again.

Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see [Appendix B, "Regulatory information"](#).



- **Auto Tx Power Ctrl (ATPC)** – Click to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Wireless APs. After a period of time, the system will stabilize itself based on the RF coverage of your Wireless APs.
- **Current Tx Power Level** – This field is view only. It displays the actual Tx power level assigned to the Wireless AP radio.
- **Max Tx Power** – Click the maximum Tx power level that the range of transmit power can be adjusted: **0** to **18** dBm. It is recommended to use **18 dBm** to not limit the potential Tx power level range that can be used.
- **Min Tx Power** – If ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted: **0** to **18** dBm. It is recommended to use **0 dBm** to not limit the potential Tx power level range that can be used.
- **Auto Tx Power Ctrl Adjust** – If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use **0 dBm** during your initial configuration. If you have an RF plan that recommended Tx power levels for each Wireless AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Rx Diversity** – Click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** – Click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Best** that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Best**. Under those circumstances, it is recommended to use either **Left** or **Right** for Tx Diversity. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Min Basic Rate** – Click the minimum data rate that must be supported by all stations in a BSS: **6**, **12**, or **24** Mbps. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **Max Basic Rate** – Click the maximum data rate that must be supported by all stations in a BSS: **6**, **12**, or **24** Mbps. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Max Operational Rate** – Click the maximum data rate that clients can operate at while associated with the AP: **6, 9, 12, 18, 24, 36, 48, or 54** Mbps. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Max Basic Rate**.

---

**Note:** Radio channels 100 to 140 occupy the 5470-5725 MHz band in the regulatory domains of the European Union and European Union free trade countries.

Radio B/G Channels 12 and 13 are not available in North America. Radio B/G channel 14 is only available in Japan.

---

- **No of Retries for Background BK** – Click the number of retries for the Background transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Best Effort BE** – Click the number of retries for the Best Effort transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Video VI** – Click the number of retries for the Video transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Voice VO** – Click the number of retries for the Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Turbo Voice TVO** – Click the number of retries for the Turbo Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.

12. To save your changes, click **Save**.

### 4.5.4 Setting up the Wireless AP using static configuration

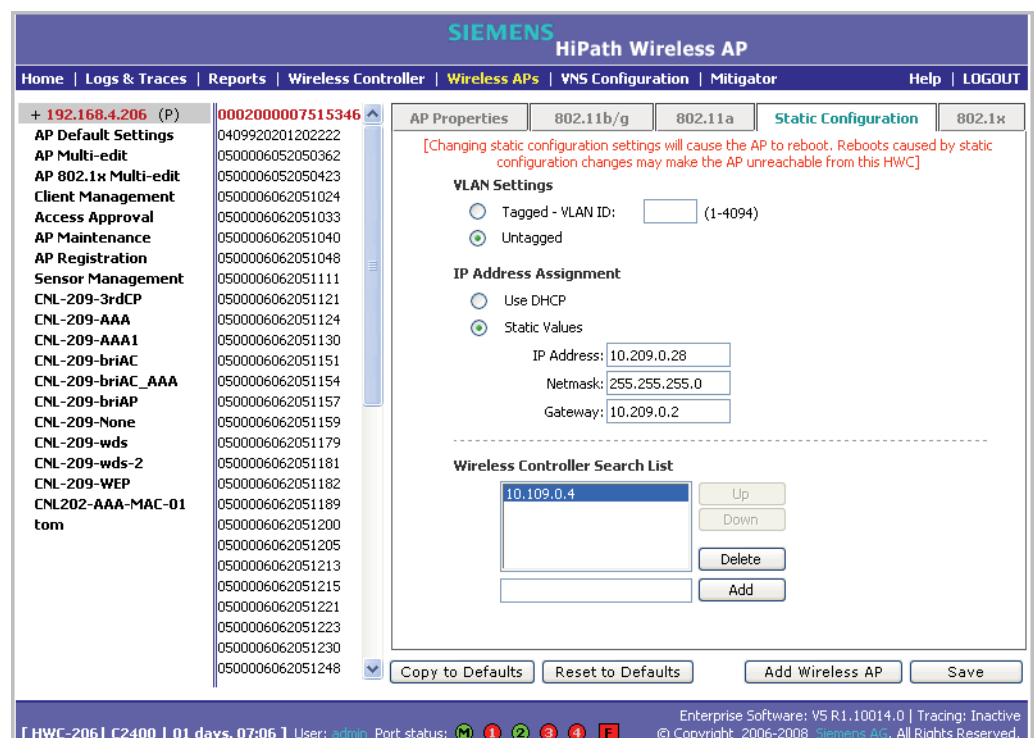
The Wireless AP static configuration feature provides the HiPath Wireless Controller, Access Points and Convergence Software solution with the capability for a network with either a central office or a branch office model. The static configuration settings assist in the setup of branch office support. These settings are not dependent of branch topology, but instead can be employed at any time if required. In the branch office model, Wireless APs are installed in remote sites,

while the HiPath Wireless Controller is in the central office. The Wireless APs require the capability to interact in both the local site network and the central network. To achieve this model, a static configuration is used.

**Note:** If a Wireless AP with a statically configured IP address (without a statically configured Wireless Controller Search List) cannot register with the HiPath Wireless Controller within the specified number of retries, the Wireless AP will use SLP, DNS, and SLP multicast as a backup mechanism.

**To set up a Wireless AP using static configuration:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. Click the appropriate Wireless AP in the list.
3. Click the **Static Configuration** tab.



4. Select one of the VLAN settings for the Wireless AP:

**Note:** The Wireless 802.11n AP does not support VLAN tagging.

- **Tagged - VLAN ID** – Select if you want to assign this AP to a specific VLAN and type the value in the box.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Untagged** – Select if you want this AP to be untagged. This option is selected by default.

---

**Caution:** Caution should be exercised when using this feature. If a VLAN tag is not configured properly, the connectivity with the AP will be lost. To configure the AP VLAN, do the following:

- Connect the AP to the HiPath Wireless Controller or to the network point that does not require AP VLAN tagging.
- Use Static Configuration to enable VLAN and define the VLAN ID.
- Save the configuration on the AP. The AP reboots and loses connectivity to the HiPath Wireless Controller.
- Disconnect the AP and attach it to its final network location.

If the VLAN settings match the network configuration, the AP registers with the HiPath Wireless Controller successfully. If the AP VLAN is not configured properly (wrong tag), connecting to the AP may not be possible. To recover from this situation, you will need to reset the AP to its factory default settings. For more information, see [Section 11.2, “Resetting the Wireless APs to their factory default settings”](#), on page 313.

---

5. Select one of the two methods of IP address assignment for the Wireless AP:

- **Use DHCP** – Select this option to enable Dynamic Host Configuration Protocol (DHCP). This option is enabled by default.
- **Static Values** – Select this option to specify the IP address of the Wireless AP.
  - **IP Address** – Type the IP address of the AP.
  - **Subnet Mask** – Type the appropriate subnet mask to separate the network portion from the host portion of the address.
  - **Gateway** – Type the default gateway of the network.

---

**Note:** For the initial configuration of a Wireless AP to use a static IP address assignment, the following is recommended:

- Allow the Wireless AP to first obtain an IP address using DHCP. By default, Wireless APs are configured to use the DHCP IP address configuration method.
- Allow the Wireless AP to connect to the HiPath Wireless Controller using the DHCP assigned IP address.
- After the Wireless AP has successfully registered to the HiPath Wireless Controller, use the **Static Configuration** tab to configure a static IP address for the Wireless AP, and then save the configuration.
- Once the static IP address has been configured on the Wireless AP, the Wireless AP can then be moved to its target location, if applicable. (A branch office scenario is an example of a setup that may require static IP

assignment.) If the Wireless AP IP address is not configured properly, connecting to the Wireless AP may not be possible. To recover from this situation, you will need to reset the Wireless AP to its factory default settings. For more information, see [Section 11.2, “Resetting the Wireless APs to their factory default settings”](#), on page 313.

---

6. In the **Add** box, type the IP address of the HiPath Wireless Controller that will control this Wireless AP.
7. Click **Add**. The IP address is added to the list.
8. Repeat steps 5 and 6 to add additional HiPath Wireless Controllers.
9. Click **Up** and **Down** to modify the order of the HiPath Wireless Controllers. The maximum is three controllers.

The Wireless AP attempts to connect to the IP addresses in the order in which they are listed. The Wireless AP is successful when it finds a HiPath Wireless Controller that will allow it to register.

This feature allows the Wireless AP to bypass the discovery process. If the **Wireless Controller Search List** box is not populated, the Wireless AP will use SLP to discover a HiPath Wireless Controller.

For the initial Wireless AP deployment, it is necessary to use one of the described options in [Section 4.2, “Discovery and registration overview”](#), on page 71.

10. To save your changes, click **Save**.

### **4.5.5 Setting up 802.1x authentication for a Wireless AP**

802.1x is an authentication standard for wired and wireless LANs. The 802.1x standard can be used to authenticate access points to the LAN to which they are connected. 802.1x support provides security for network deployments where access points are placed in public spaces.

---

**Note:** The Wireless 802.11n AP does not support 802.1x authentication.

---

To successfully set up 802.1x authentication of a Wireless AP, the Wireless AP must be configured for 802.1x authentication before the Wireless AP is connected to a 802.1x enabled switch port.

---

**Caution:** If the switch port, to which the Wireless AP is connected to, is not 802.1x enabled, the 802.1x authentication will not take effect.

---

## Configuring the Wireless AP

### Configuring Wireless AP settings

802.1x authentication credentials can be updated at any time, whether or not the Wireless AP is connected with an active session. If the Wireless AP is connected, the new credentials are sent immediately. If the Wireless AP is not connected, the new credentials are delivered the next time the Wireless AP connects to the HiPath Wireless Controller.

There are two main aspects to the 802.1x feature:

- Credential management – The HiPath Wireless Controller and the Wireless AP are responsible for the requesting, creating, deleting, or invalidating the credentials used in the authentication process.
- Authentication – The Wireless AP is responsible for the actual execution of the EAP-TLS or PEAP protocol.

802.1x authentication can be configured on a per access point basis. For example, 802.1x authentication can be applied to specific Wireless APs individually or with a multi-edit function.

The 802.1x authentication supports two authentication methods:

- PEAP (Protected Extensible Authentication Protocol)
  - Is the recommended 802.1x authentication method
  - Requires minimal configuration effort and provides equal authentication protection to EAP-TLS
  - Uses user ID and passwords for authentication of access points
- EAP-TLS
  - Requires more configuration effort
  - Requires the use of a third-party Certificate Authentication application
  - Uses certificates for authentication of access points
  - HiPath Wireless Controller can operate in either proxy mode or pass through mode.
    - Proxy mode – The HiPath Wireless Controller generates the public and private key pair used in the certificate.
    - Pass through mode – The certificate and private key is created by the third-party Certificate Authentication application.

---

**Note:** Although a Wireless AP can support using both PEAP and EAP-TLS credentials simultaneously, it is not recommended to do so. Instead, it is recommended that only one type of authentication be used, and that only credentials for that type of authentication get installed on the Wireless AP.

---

### 4.5.5.1 Configuring 802.1x PEAP authentication

PEAP authentication uses user ID and passwords for authentication. To successfully configure 802.1x authentication of a Wireless AP, the Wireless AP must first be configured for 802.1x authentication before the Wireless AP is deployed on a 802.1x enabled switch port.

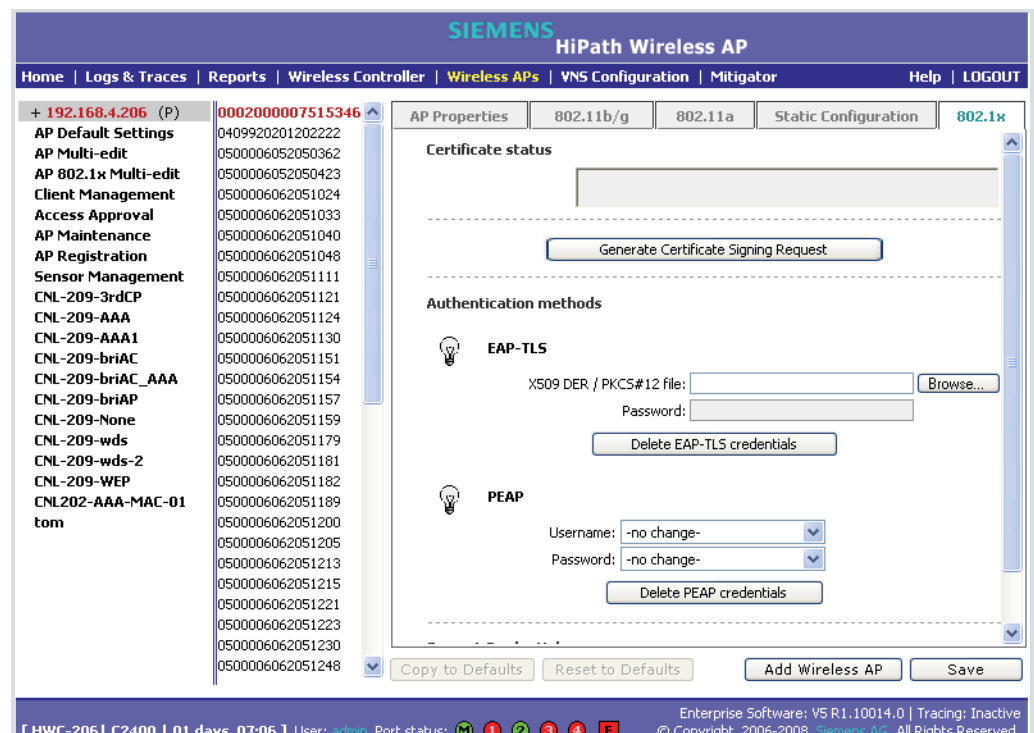
---

**Note:** Usernames and passwords for PEAP authentication credentials each have a maximum length of 128 characters.

---

**To configure 802.1x PEAP authentication:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the Wireless AP list, click the Wireless AP for which you want to configure 802.1x PEAP authentication.
3. Click the **802.1x** tab.



4. In the **Username** drop-down list, click the value you want to assign as the username credential:

- **Name** – The name of the Wireless AP, which is assigned on the **AP Properties** tab. The Wireless AP name can be edited.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Serial** – The serial number of the Wireless AP. The Wireless AP serial number cannot be edited.
  - **MAC** – The MAC address of the Wireless AP. The Wireless AP MAC address cannot be edited.
  - **Other** – Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the username credential.
5. In the **Password** drop-down list, click the value you want to assign as the password credential:
- **Name** – The name of the Wireless AP, which is assigned on the **AP Properties** tab. The Wireless AP name can be edited.
  - **Serial** – The serial number of the Wireless AP. The Wireless AP serial number cannot be edited.
  - **MAC** – The MAC address of the Wireless AP. The Wireless AP MAC address cannot be edited.
  - **Other** – Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the password credential.
6. To save your changes, click **Save**.

The 802.1x PEAP authentication configuration is assigned to the Wireless AP. The Wireless AP can now be deployed to a 802.1x enabled switch port.

#### 4.5.5.2 Configuring 802.1x EAP-TLS authentication

EAP-TLS authentication uses certificates for authentication. A third-party Certificate Authentication application is required to configure EAP-TLS authentication. Certificates can be overwritten with new ones at any time.

With EAP-TLS authentication, the HiPath Wireless Controller can operate in either proxy mode or pass through mode.

---

**Note:** When a Wireless AP configured with 802.1x EAP-TLS authentication is connected to a HiPath Wireless Controller, the Wireless AP begins submitting logs to the HiPath Wireless Controller 30 days before the certificate expires to provide administrators with a warning of the impending expiry date.

---

##### Proxy mode

In proxy mode, HiPath Wireless Controller generates the public and private key pair used in the certificate. You can specify the criteria used to create the Certificate Request. The Certificate Request that is generated by the HiPath Wireless Controller is then used by the third-party Certificate Authentication application to create the certificate used for authentication of the Wireless AP. To



successfully configure 802.1x authentication of a Wireless AP, the Wireless AP must first be configured for 802.1x authentication before the Wireless AP is deployed on a 802.1x enabled switch port.

**To configure 802.1x EAP-TLS authentication in proxy mode:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the Wireless AP list, click the Wireless AP for which you want to configure 802.1x EAP-TLS authentication.
3. Click the **802.1x** tab.
4. Click **Generate certificate request**. The **Generate Certificate Request** window is displayed.

The screenshot shows a web-based form titled "Generate Certificate Signing Request" with the Siemens logo. The form is titled "Enter required information" and contains several input fields: "Country name:", "State or Province name:", "Locality name (city):", "Organization name:", "Organizational Unit name:", "Common name:" (with a dropdown menu showing "Name: 0002000007515346"), and "Email address:". At the bottom of the form are two buttons: "Generate Certificate Signing Request" and "Close".

5. Type the criteria to be used to create the certificate request. All fields are required:
  - **Country name** – The two-letter ISO abbreviation of the name of the country
  - **State or Province name** – The name of the State/Province
  - **Locality name (city)** – The name of the city
  - **Organization name** – The name of the organization
  - **Organizational Unit name** – The name of the unit within the organization
  - **Common name** – Click the value you want to assign as the common name of the Wireless AP:

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Name** – The name of the Wireless AP, which is assigned on the **AP Properties** tab. The Wireless AP name can be edited.
  - **Serial** – The serial number of the Wireless AP. The Wireless AP serial number cannot be edited.
  - **MAC** – The MAC address of the Wireless AP. The Wireless AP MAC address cannot be edited.
  - **Other** – Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the common name of the Wireless AP.
  - **Email address** – The email address of the organization
6. Click **Generate certificate request**. A certificate request file is generated (.csr file extension). The name of the file is the Wireless AP serial number. The **File Download** dialog is displayed.
  7. Click **Save**. The **Save as** window is displayed.
  8. Navigate to the location on your computer that you want to save the generated certificate request file, and then click **Save**.
  9. In the third-party Certificate Authentication application, use the content of the generated certificate request file to generate the certificate file (.cer file extension).
  10. On the **802.1x** tab, click **Browse**. The **Choose file** window is displayed.
  11. Navigate to the location of the certificate file, and click **Open**. The name of the certificate file is displayed in the **X509 DER / PKCS#12 file** box.
  12. To save your changes, click **Save**.

The 802.1x EAP-TLS (certificate and private key) authentication in proxy mode is assigned to the Wireless AP. The Wireless AP can now be deployed to a 802.1x enabled switch port.

#### Pass through mode

In pass through mode, the certificate and private key is created by the third-party Certificate Authentication application. To successfully configure 802.1x authentication of a Wireless AP, the Wireless AP must first be configured for 802.1x authentication before the Wireless AP is deployed on a 802.1x enabled switch port.

Before you configure 802.1x using EAP-TLS authentication in pass through mode, you must first create a certificate using the third-party Certificate Authentication application and save the certificate file in PKCS #12 file format (.pfx file extension ) on your system.

**To configure 802.1x EAP-TLS authentication in pass through mode:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the Wireless AP list, click the Wireless AP for which you want to configure 802.1x EAP-TLS authentication.
3. Click the **802.1x** tab.
4. Click **Browse**. The **Choose file** window is displayed.
5. Navigate to the location of the certificate file (.pfx) and click **Open**. The name of the certificate file is displayed in the **X509 DER / PKCS#12 file** box.
6. In the **Password** box, type the password that was used to protect the private key.

---

**Note:** The password that was used to protect the private key must be a maximum of 31 characters long.

---

7. To save your changes, click **Save**.

The 802.1x EAP-TLS authentication in pass through mode is assigned to the Wireless AP. The Wireless AP can now be deployed to a 802.1x enabled switch port.

### **4.5.5.3 Viewing 802.1x credentials**

When 802.1x authentication is configured on a Wireless AP, the light bulb icon on the **802.1x** tab for the configured Wireless AP is lit to indicate which 802.1x authentication method is used. A Wireless AP can be configured to use both EAP-TLS and PEAP authentication methods. For example, when both EAP-TLS and PEAP authentication methods are configured for the Wireless AP, both light bulb icons on the **802.1x** tab are lit.

---

**Note:** You can only view the 802.1x credentials of Wireless APs that have an active session with the HiPath Wireless Controller. If you attempt to view the credentials of a Wireless AP that does not have an active session, the Wireless AP Credentials window displays the following message:

**Unable to query Wireless AP: not connected.**

---

## Configuring the Wireless AP

### Configuring Wireless AP settings

#### To view current 802.1x credentials:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the Wireless AP list, click the Wireless AP for which you want to view its current 802.1x credentials.
3. In the **Current Credentials** section, click **Get additional Certificate info**. The Wireless AP Credentials window is displayed.



The screenshot shows a window titled "SIEMENS Wireless AP Credentials". Inside the window, under the heading "Current credentials in use by Wireless AP", the following information is displayed:

Username:	0409920201201774
Password:	*****
Certificate serial number:	149ACC5C0000000008B
Certificate expiry date:	Wednesday April 23rd 2008 04:13:25 PM
Certificate issued on:	Tuesday April 24th 2007 04:13:26 PM
Certificate issued by:	CN=testvpc, DC=com, DC=Siemenswifi
Subject alternative name:	Principal Name=0409920201201774@Siemenswifi.com
Full distinguished name:	CN=Users, CN=0409920201201774, DC=com, DC=Siemenswifi

At the bottom of the window is a "Close" button.

#### 4.5.5.4 Deleting 802.1x credentials

---

**Caution:** Exercise caution when deleting 802.1x credentials. For example, deleting 802.1x credentials may prevent the Wireless AP from being authenticated or to lose its connection with the HiPath Wireless Controller.

---

#### To delete current 802.1x credentials:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the Wireless AP list, click the Wireless AP for which you want to delete its current 802.1x credentials.
3. Do the following:
  - To delete EAP-TLS credentials, click **Delete EAP-TLS** credentials.
  - To delete PEAP credentials, click **Delete PEAP** credentials.

The credentials are deleted and the Wireless AP settings are updated.

**Note:** If you attempt to delete the 802.1x credentials of a Wireless AP that currently does not have an active session with the HiPath Wireless Controller, the credentials are only deleted after the Wireless AP connects with the HiPath Wireless Controller.

## 4.5.6 Setting up 802.1x authentication for Wireless APs using Multi-edit

In addition to configuring Wireless APs individually, you can also configure 802.1x authentication for multiple Wireless APs simultaneously by using the AP 802.1x Multi-edit feature.

To configure 802.1x PEAP authentication using Multi-edit:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **AP 802.1x Multi-edit**.
3. In the **Wireless APs** list, click one or more APs to edit. To select multiple APs, click the APs from the list while pressing the CTRL key.

The screenshot displays the Siemens HiPath Wireless AP configuration interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar shows a tree view with 'AP 802.1x Multi-edit' selected. The main content area is divided into two panes. The left pane, titled 'Wireless APs', shows a list of APs with their MAC addresses. The right pane, titled '802.1x Authentication', contains three sections: 'Certificate Signing Request' with fields for Country name, State or Province name, Locality name (city), Organization name, Organizational Unit name, Common name (set to MAC), and Email address; 'Bulk Certificate Upload' with fields for ZIP Archive and Password; and 'PEAP Authentication' with fields for Username and Password (both set to MAC). A status bar at the bottom indicates 'Enterprise Software: V5 R1.10014.0 | Tracing: Inactive' and '© Copyright 2006-2008 Siemens AG. All Rights Reserved.'

## Configuring the Wireless AP

### Configuring Wireless AP settings

4. In the **PEAP Authentication** section, do the following:
  - In the **Username** drop-down list, click the value you want to assign as the username credential:
    - **Name** – The name of the Wireless AP, which is assigned on the **AP Properties** tab. The Wireless AP name can be edited.
    - **Serial** – The serial number of the Wireless AP. The Wireless AP serial number cannot be edited.
    - **MAC** – The MAC address of the Wireless AP. The Wireless AP MAC address cannot be edited.
  - In the **Password** drop-down list, click the value you want to assign as the password credential:
    - **Name** – The name of the Wireless AP, which is assigned on the **AP Properties** tab. The Wireless AP name can be edited.
    - **Serial** – The serial number of the Wireless AP. The Wireless AP serial number cannot be edited.
    - **MAC** – The MAC address of the Wireless AP. The Wireless AP MAC address cannot be edited.
5. Click **Set PEAP credentials**. The **AP 802.1x Multi-edit progress** window is displayed, which provides the status of the configuration process. Once complete, the **Settings updated** message is displayed in the footer of the HiPath Wireless Assistant.

The 802.1x PEAP authentication configuration is assigned to the Wireless APs. The Wireless APs can now be deployed to 802.1x enabled switch ports.

#### To configure 802.1x EAP-TLS authentication in proxy mode using multi-edit:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **AP 802.1x Multi-edit**.
3. In the **Wireless APs** list, click one or more Wireless APs to configure. To click multiple Wireless APs, click the Wireless APs from the list while pressing the CTRL key.
4. In the **Certificate request** section, type the following:
  - **Country name** – The two-letter ISO abbreviation of the name of the country
  - **State or Province name** – The name of the State/Province
  - **Locality name (city)** – The name of the city
  - **Organization name** – The name of the organization

- **Organizational Unit name** – The name of the unit within the organization
  - **Common name** – Click the value you want to assign as the common name of the Wireless AP:
    - **Name** – The name of the Wireless AP, which is assigned on the **AP Properties** tab. The Wireless AP name can be edited.
    - **Serial** – The serial number of the Wireless AP. The Wireless AP serial number cannot be edited.
    - **MAC** – The MAC address of the Wireless AP. The Wireless AP MAC address cannot be edited.
  - **Email address** – The email address of the organization
5. Click **Generate Certificates**. The **AP 802.1x Multi-edit progress** window is displayed, which provides the status of the configuration process. Once complete, the **File Download** dialog is displayed.
  6. Click **Save**. The **Save as** window is displayed.
  7. Navigate to the location on your computer that you want to save the generated **certificate\_requests.tar** file, and then click **Save**.

The **certificate\_requests.tar** file contains a certificate request (.csr) file for each Wireless AP. For each certificate request, generate a certificate using the third-party Certificate Authentication application. Once complete, zip all the certificates files (.cer) into one .zip file.
  8. In the **Bulk Certificate Upload** section, click **Browse**. The **Choose file** window is displayed.
  9. Navigate to the location of the zipped certificates file, and then click **Open**. The name of the zipped certificates file is displayed in the **ZIP Archive** box.
  10. Click **Upload and Set certificates**. Once complete, the **Settings updated** message is displayed in the footer of the HiPath Wireless Assistant.

**Configuring 802.1x EAP-TLS authentication in pass through mode using Multi-edit:**

Before you configure 802.1x EAP-TLS authentication in pass through mode using Multi-edit, the following prerequisites are required:

- You must first generate a certificate for each Wireless AP using the third-party Certificate Authentication application.
- When generating the certificates:
  - Use the Common name value (either Name, Serial, or MAC) of the Wireless AP to name each generated certificate.
  - Use a common password for each generated certificate.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- All .pfx files created by the the third-party Certificate Authentication application must be zipped into one file.

#### To configure 802.1x EAP-TLS authentication in pass through mode using Multi-edit:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **AP 802.1x Multi-edit**.
3. In the **Wireless APs** list, click one or more Wireless APs to configure. To click multiple Wireless APs, click the Wireless APs from the list while pressing the CTRL key.
4. In the **Bulk Certificate Upload** section, click **Browse**. The **Choose file** window is displayed.
5. Navigate to the location of the zipped certificates file, and then click **Open**. The name of the zipped certificates file is displayed in the **ZIP Archive** box.
6. In the **Password** box, type the password used during the certificates generation process.
7. Click **Upload and Set certificates**. Once complete, the **Settings updated** message is displayed in the footer of the HiPath Wireless Assistant.

---

**Note:** Only APs that are in Pending state can be approved as a sensor or as an access point. To change the role of an approved AP, use the **Role** drop-down list on the **AP Properties** tab or the **AP Multi-edit** page.

Only the HiPath Wireless AP 2610/2620 can be approved as a sensor. The HiPath Wireless Outdoor AP and Wireless 802.11n AP 3610/3620 cannot work as sensors.

---

## 4.5.7 Configuring the default Wireless AP settings

Wireless APs are added with default settings. You can modify the system's Wireless AP default settings, and then use these default settings to configure newly added Wireless APs. In addition, you can base the system's Wireless AP default settings on an existing Wireless AP configuration or have configured Wireless APs inherit the properties of the default Wireless AP configuration when they register with the system.

The process of configuring the default Wireless AP settings is divided into three tabs:



## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Common Configuration** – Configure common configuration, such as VNS assignments and static configuration options for all Wireless APs including, the Wireless AP 2610/2620, the Wireless 802.11n AP 3610/3620, and the HiPath Wireless Outdoor AP 2650/2660.
- **Standard AP Defaults** – Configure the default Wireless AP settings for only the Wireless AP 2610/2620 and HiPath Wireless Outdoor AP 2650/2660.
- **11n AP Defaults** – Configure the default Wireless AP settings for only the Wireless 802.11n AP 3610/3620.

#### To configure the default AP settings:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **AP Default Settings**.

The screenshot shows the Siemens HiPath Wireless AP configuration page. The left sidebar lists various configuration options, with 'AP Default Settings' highlighted. The main area is divided into three tabs: 'Common Configuration', 'Standard AP Defaults', and '11n AP Defaults'. The 'Common Configuration' tab is active, showing 'Static Configuration' and 'VNS Assignments' sections. The 'VNS Assignments' section includes a table for associating radios with VNS, b/g, and a.

Associate radios:	VNS	b/g	a
bridgedAC2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-3rdCP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-AAA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CNL-209-AAA1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-briAC1_AAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-briAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-CP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL-209-WEP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNL202-AAA-MAC-01	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Modify the following Wireless AP default settings as required:

- Static Configuration
- VNS Assignments
- AP Properties
- Radio Settings

## Configuring the Wireless AP

### Configuring Wireless AP settings

4. To configure common configuration applicable to all Wireless APs, click the **Common Configuration** tab.
5. In the **Static Configuration** section, do one of the following:
  - To allow each Wireless AP to provide its own HWC Search List, select the **Learn HWC Search List from AP** checkbox.
  - To specify a common HWC Search List for all Wireless APs, clear the **Learn HWC Search List from AP** checkbox, and then do the following:
    - a) In the **Add** box, type the IP address of the HiPath Wireless Controller that will control this Wireless AP.
    - b) Click **Add**. The IP address is added to the list.
    - c) Repeat steps **a** and **b** to add additional HiPath Wireless Controllers.
    - d) Click **Up** and **Down** to modify the order of the HiPath Wireless Controllers. The maximum is three controllers.

The Wireless AP attempts to connect to the IP addresses in the order in which they are listed. The Wireless AP is successful when it finds a HiPath Wireless Controller that will allow it to register.

This feature allows the Wireless AP to bypass the discovery process. If the **Wireless Controller Search List** box is not populated, the Wireless AP will use SLP to discover a HiPath Wireless Controller.

The DHCP function for wireless clients must be provided locally by a local DHCP server, unless each wireless client has a static IP address.

For the initial Wireless AP deployment, it is necessary to use one of the described options in [Section 4.2, "Discovery and registration overview"](#), on page 71.

6. In the **VNS Assignments** section, assign the radios for each VNS in the list by selecting or clearing the options.
7. To configure default Wireless AP settings for only the Wireless AP 2610/2620 and HiPath Wireless Outdoor AP, click the **Standard AP Defaults** tab.

## Configuring the Wireless AP

### Configuring Wireless AP settings

8. In the **AP Properties** section, do the following:

- **Role** – Click the role for the Wireless AP, either **Access Point** or **Sensor**. Once the Wireless AP is configured as **Sensor**, it no longer performs RF services, and is no longer managed by the HiPath Wireless Controller.
- **Poll Timeout** – Type the timeout value, in seconds. The Wireless AP uses this value to trigger re-establishing the link with the HiPath Wireless Controller if it (Wireless AP) does not get an answer to its polling. The default value is 10 seconds.
- **Poll Interval** – Type the interval value, in seconds, for polling the controller. The default value is 2 seconds.
- **Telnet Access** – Click whether Telnet Access to the Wireless AP is enabled or disabled.
- **Maintain client session in event of poll failure** – Select this option (if using a bridged at AP VNS) if the AP should remain active if a link loss with the controller occurs. This option is enabled by default.
- **Restart service in the absence of controller** – Select this option (if using a bridged at AP VNS) to ensure the Wireless APs' radios continue providing service if the Wireless AP's connection to the HiPath Wireless Controller is lost. If this option is enabled, it allows the Wireless AP to start a bridged at AP VNS even in the absence of a HiPath Wireless Controller.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Use broadcast for disassociation** – Select if you want the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This will affect the behavior of the AP under the following conditions:
  - If the Wireless AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection).
  - If a BSSID is deactivated or removed on the Wireless AP.

This option is enabled by default.

- **Country** – Click the country of operation. This option is only available with some licenses.

9. In the **Radio Settings** section, do the following:

- **Radio mode** – Click the radios you want to enable.
- **DTIM** – Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** – For each radio, type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS** – For each radio, type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** – For each radio, type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **RF Domain** – For each radio, type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 15 characters. The RF Domain is used to identify a group of Wireless APs.
- **Channel** – For each radio, click the wireless channel you want the Wireless APs to use to communicate with wireless devices. Click **Auto** to request the ACS to search for a new channel for the Wireless APs, using a channel selection algorithm. This forces the APs to go through the auto-channel selection process again. If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm.

Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see [Appendix B, "Regulatory information"](#).

- **Auto Tx Power Ctrl** – For each radio, click to either enable or disable ATPC from the **Auto Tx Power Ctrl** drop-down list. ATPC automatically adapts transmission power signals according to the coverage provided by the Wireless APs. After a period of time, the system will stabilize itself based on the RF coverage of your Wireless APs.
- **Max Tx Power** – For each radio, click the appropriate Tx power level from the **Max TX Power** drop-down list. The values in the **Max TX Power** drop-down is in dBm (dBm is an abbreviation for the power ratio in decibel (dB) of the measured power referenced to one milliwatt).
- **Min Tx Power** – For each radio, if ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted: **0 to 18** dBm. It is recommended to use **0 dBm** to not limit the potential Tx power level range that can be used.
- **Auto Tx Power Ctrl Adjust** – For each radio, if ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use **0 dBm** during your initial configuration. If you have an RF plan that recommended Tx power levels for each Wireless AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Rx Diversity** – For each radio, click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity receiving antennas. The default and recommended selection is **Best**. If only one antenna is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** – For each radio, click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity receiving antennas. The default selection is **Best** that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Best**. Under those circumstances, it is recommended to use either **Left** or **Right** for Tx Diversity. If only one antenna is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Preamble** – Click a preamble type for 11b-specific (CCK) rates: **Short**, **Long**, or **Auto**. The recommended value is **Auto**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Click **Long** if compatibility with pre-11b clients is required.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Protection Mode** – Click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **Protection Rate** – Click a protection rate: **1**, **2**, **5.5**, or **11** Mbps. The default and recommended setting is **11**. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than **11** Mbps are required to ensure coverage.
- **Protection Type** – Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.
- **Min Basic Rate** – For each radio, click the minimum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Click **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. Click **6**, **12**, or **24** Mbps for 11a mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Basic Rate** – For each radio, click the maximum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Click **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. Click **6**, **12**, or **24** Mbps for 11a mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Operational Rate** – For each radio, click the maximum data rate that clients can operate at while associated with the AP: **1**, **2**, **5.5**, or **11** Mbps for 11b-only mode. Click **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **28**, or **54** Mbps for 11b+11g or 11g-only modes. Click **6**, **9**, **12**, **18**, **24**, **36**, **48**, or **54** Mbps for 11a mode. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **Background BK** – For each radio, click the number of retries for the Background transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Best Effort BE** – For each radio, click the number of retries for the Best Effort transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Video VI** – For each radio, click the number of retries for the Video transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Voice VO** – For each radio, click the number of retries for the Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Turbo Voice TVO** – For each radio, click the number of retries for the Turbo Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.

10. To configure default Wireless AP settings for only the Wireless 802.11n AP 3610/3620, click the **11n AP Defaults** tab.

The screenshot displays the Siemens HiPath Wireless AP configuration interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar shows a tree view of configuration options, with 'AP Default Settings' selected. The main content area is divided into three tabs: 'Common Configuration', 'Standard AP Defaults', and '11n AP Defaults'. The '11n AP Defaults' tab is active, showing the 'AP Properties' and 'Radio Settings' sections. The 'AP Properties' section includes fields for 'Poll Timeout' (10), 'Poll Interval' (2), 'Telnet Access' (Disabled), and 'Country' (United States). The 'Radio Settings' section is split into two columns for '802.11b/g/n' and '802.11a/n'. The '802.11b/g/n' settings include 'Radio Mode' (b/g/n), 'Channel Width' (20MHz), 'DTIM' (10), 'Beacon Period' (100), 'RTS/CTS' (2346), 'Frag. Threshold' (2346), 'Channel' (auto), 'Channel Bonding' (Up), 'Guard Interval' (Long), 'Max Tx Power' (18 dBm), and 'Preamble' (Short). The '802.11a/n' settings include 'Radio Mode' (a/n), 'Channel Width' (20MHz), 'DTIM' (10), 'Beacon Period' (100), 'RTS/CTS' (2346), 'Frag. Threshold' (2346), 'Channel' (auto), 'Channel Bonding' (Up), 'Guard Interval' (Long), 'Max Tx Power' (18 dBm), and 'Preamble' (Short). A 'Save Settings' button is located at the bottom right of the configuration area. The bottom status bar shows system information: '[ HWC-206 | C2400 | 05 days, 06:50 ] User: admin Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] [ F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright. 2006-2008 Siemens AG. All Rights Reserved.'

11. In the **AP Properties** section, do the following:

- **Poll Timeout** – Type the timeout value, in seconds. The Wireless AP uses this value to trigger re-establishing the link with the HiPath Wireless Controller if it (Wireless AP) does not get an answer to its polling. The default value is 10 seconds.
- **Poll Interval** – Type the interval value, in seconds, for polling the controller. The default value is 2 seconds.
- **Telnet Access** – Click whether Telnet Access to the Wireless AP is enabled or disabled.

## Configuring the Wireless AP

### Configuring Wireless AP settings

- **Country** – Click the country of operation. This option is only available with some licenses.

12. In the **Radio Settings** section, do the following:

- **Radio Mode** – Click the radios you want to enable.
- **Channel Width** – Click the channel width for the radio:
  - **20MHz** – Click to allow 802.11n clients to use the primary channel (20MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11b/g radio protocols.
  - **40MHz** – Click to allow 802.11n clients that support the 40MHz frequency to use 40MHz, 20MHz, or the 802.11b/g radio protocols. 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11b/g radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11b/g radio protocols.
  - **Auto** – Click to automatically switch between 20MHz and 40MHz channel widths, depending on how busy the extension channel is.
- **DTIM** – Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** – For each radio, type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS** – For each radio, type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** – For each radio, type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **Channel** – For each radio, click the wireless channel you want the Wireless APs to use to communicate with wireless devices. Click **Auto** to request the ACS to search for a new channel for the Wireless APs, using a channel selection algorithm. This forces the APs to go through the auto-channel selection process again. If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm. Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see [Appendix B, “Regulatory information”](#).



- **Channel Bonding** – Click the bonding method, **Up** or **Down**. The primary channel (20MHz) is bonded with an extension channel that is either 20MHz above (bonding up) or 20MHz below (bonding down) of the primary channel. Depending on the channel that is selected in the **Request New Channel** drop-down list, you may be prevented from bonding **Up** or **Down** in the **Channel Bonding** drop-down list.
- **Guard Interval** – Click a guard interval, **Long** or **Short**, when a 40MHz channel is used. It is recommended to use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).
- **Max Tx Power** – For each radio, click the appropriate Tx power level from the **Max TX Power** drop-down list. The values in the **Max TX Power** drop-down is in dBm (dBm is an abbreviation for the power ratio in decibel (dB) of the measured power referenced to one milliwatt).
- **Preamble** – Click a preamble type for 11b-specific (CCK) rates: **Short**, **Long**, or **Auto**. The recommended value is **Auto**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Click **Long** if compatibility with pre-11b clients is required.
- **Protection Mode** – Click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **Protection Type** – Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

13. In the **11n Settings** section, do the following:

- **Protection Mode** – For each radio, click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **40MHz Protection Mode** – Click a protection type, **CTS Only** or **RTS-CTS**, or **None**, when a 40MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
- **40MHz Prot. Channel Offset** – Select a 20MHz channel offset if the deployment is using channels that are 20MHz apart (for example, using channels **1**, **5**, **9**, and **13**) or a 25MHz channel offset if the deployment is using channels that are 25MHz apart (for example, using channels **1**, **6**, and **11**).

## Configuring the Wireless AP

*Modifying a Wireless AP's properties based on a default AP configuration*

- **40MHz Channel Busy Threshold** – Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40MHz).
  - **Aggregate MSDUs** – Click an aggregate MSDU mode: **Enabled** or **Disabled**. Aggregate MSDU increases the maximum frame transmission size.
  - **Aggregate MSDU Max Length** – Type the maximum length of the aggregate MSDU. The value range is 2290-4096 bytes.
  - **Aggregate MPDUs** – Click an aggregate MPDU mode: **Enabled** or **Disabled**. Aggregate MPDU provides a significant improvement in throughput .
  - **Aggregate MPDU Max Length** – Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
  - **Agg. MPDU Max # of Sub-frames** – Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
14. **ADDBA Support** – Click an ADDBA support mode: **Enabled** or **Disabled**. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. **ADDBA Support** must be enabled if **Aggregate APDU** is enable.
15. To save your changes, click **Save Settings**.

## 4.6 Modifying a Wireless AP's properties based on a default AP configuration

If you have a Wireless AP that is already configured with its own settings, but would like the Wireless AP to be reset to use the system's default AP settings, use the **Reset to Defaults** feature on the **AP Properties** tab.

**To configure a Wireless AP with the system's default AP settings:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the **Wireless AP** list, click the Wireless AP whose properties you want to modify. The **AP Properties** tab displays Wireless AP information.
3. To have the Wireless AP inherit the system's default AP settings, click **Reset to Defaults**. A pop-up window asking you to confirm the configuration change is displayed.
4. To confirm resetting the AP to the default settings, click **OK**.

## 4.7 Modifying the Wireless AP's default setting using the Copy to Defaults feature

You can modify the system's default AP settings by using the **Copy to Defaults** feature on the **AP Properties** tab. This feature allows the properties of an already configured AP to become the system's default AP settings.

### **To modify the system's default AP settings based on an already configured AP:**

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the **Wireless AP** list, click the Wireless AP whose properties you want to become the system's default AP settings. The **AP Properties** tab displays Wireless AP information.
3. If applicable, modify the Wireless AP's properties. For more information, see [Section 4.5.2, "Modifying a Wireless AP's properties"](#), on page 90.
4. To make this AP's configuration be the system's default AP settings, click **Copy to Defaults**. A pop-up window asking you to confirm the configuration change is displayed.
5. To confirm resetting the system's default AP settings, click **OK**.

## 4.8 Configuring Wireless APs simultaneously

In addition to configuring Wireless APs individually, you can also configure multiple Wireless APs simultaneously by using the **AP Multi-edit** functionality. Configuring Wireless APs simultaneously is similar to modifying the system's default AP settings or individual Wireless APs.

When selecting the Wireless APs to simultaneously configure, you can use the following criteria:

- Select the Wireless APs by hardware type
- Select the Wireless APs individually

You can select multiple hardware types and individual Wireless APs by pressing the Ctrl key and selecting the hardware types and specific Wireless APs.

---

**Note:** Only settings and options supported by all of the selected hardware types are available for configuring.

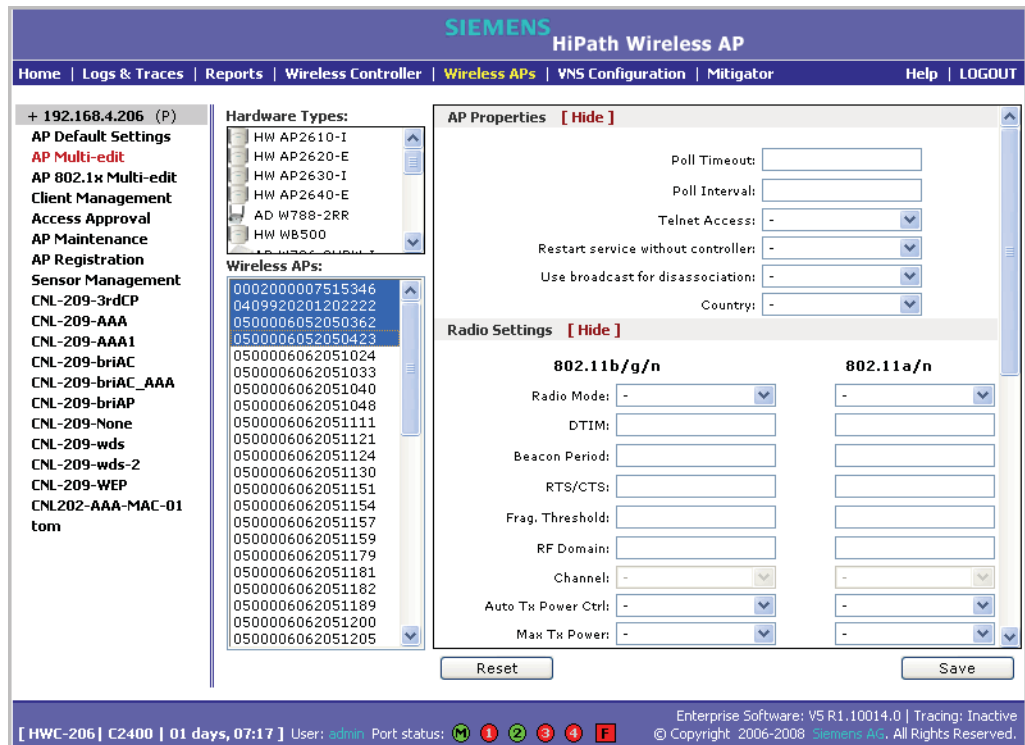
---

## Configuring the Wireless AP

### Configuring Wireless APs simultaneously

#### To configure Wireless APs simultaneously:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **AP Multi-edit**.



#### 3. Do the following:

- In the **Hardware Types** list, click one or more Wireless AP hardware types.
- In the **Wireless APs** list, click one or more Wireless APs to edit. To click multiple Wireless APs, click the APs from the list while pressing the CTRL key.

**Note:** When using multi-edit configuration, any box or option that is not explicitly modified will not be changed by the update.

The Wireless APs shown in the **Wireless APs** list can be from any version of the software. Attributes that are common between software versions are set on all Wireless APs. Attributes that are not common, are only sent to the AP versions to which the attributes apply. Attempting to set an attribute that does not apply for an AP will not abort the multi-edit operation.

#### 4. Modify the configuration of the selected Wireless APs:

- **AP Properties** – For more information, see Section 4.5.2, “Modifying a Wireless AP’s properties”, on page 90.
  - **Radio Settings** – For more information, see Section 4.5.3, “Modifying Wireless AP radio properties”, on page 95.
  - **Static Configuration** – For more information, see Section 4.5.4, “Setting up the Wireless AP using static configuration”, on page 114.
5. In the **AP Properties**, **Radio Settings**, and **Static Configuration** sections of the page, select and type the attributes you want to edit for all selected APs.

---

**Note:** Only settings and options supported by all of the currently selected hardware types are available for configuring.

---

6. To save your changes, click **Save**.

## 4.9 Configuring an AP as a sensor

---

**Note:** Only the HiPath Wireless AP 2610/2620 can be configured as a sensor. The HiPath Wireless Outdoor AP and the Wireless 802.11n AP cannot perform a sensor’s role; it cannot be configured as a sensor.

---

An AP that is configured as a sensor performs scanning services and relays information to the HWMA (HiPath Wireless Manager Advanced). When an AP is **Approved as Sensor**, the AP does the following:

- Connection to the HiPath Wireless Controller is severed
- AP registers with the HWMA
- The AP performs scanning services (the AP no longer performs RF services for the HiPath Wireless Controller)

When an AP is operating as a sensor, it has no interaction with the HiPath Wireless Controller, and it does not perform like an AP: it does not allow devices to associate to it and traffic is not forwarded through it. An AP operating as a sensor is managed by the HWMA. The HWMA’s sensor domain license (SDL) limit governs the number of sensors the customer can have.

When an AP is configured as a sensor, the AP’s current configuration data is retained in the controller database. If the sensor is later configured back to perform RF services, its previous configuration data is reassigned to it. For more information, see the *HiPath Wireless Manager User Guide*.

In order for APs configured as sensors to connect with the HWMA, you must configure the Sensor Management values for the HiPath Wireless Controller:

## Configuring the Wireless AP

### Performing Wireless AP software maintenance

- TFTP server IP address
- Path to sensor image

#### To configure Sensor Management values for the HiPath Wireless Controller:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** page is displayed.
2. In the left pane, click **Sensor Management**. The **Wireless AP Sensor Management** page is displayed.

The screenshot displays the Siemens HiPath Wireless AP configuration web interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The main content area is titled 'Wireless AP Sensor Management' and contains two input fields: 'TFTP Server:' and 'Path to Image:'. A 'Save' button is located to the right of these fields. The left sidebar shows a tree view of configuration options, with 'Sensor Management' highlighted in red. The status bar at the bottom indicates the user is 'admin', the port status is 'M 1 2 3 4 F', and the software version is 'V5 R1.10014.0'.

3. Type the following:
  - **TFTP Server** – The IP of the TFTP server the AP is to retrieve the sensor image file from.
  - **Path to Image** – The filename and location of the sensor image.
4. To save your changes, click **Save**.

## 4.10 Performing Wireless AP software maintenance

Periodically, the software used by the Wireless APs is altered for reasons of upgrade or security. The new version of the AP software is installed from the HiPath Wireless Controller.

The software for each Wireless AP can be uploaded either immediately, or the next time the Wireless AP connects. Part of the Wireless AP boot sequence is to seek and install its software from the HiPath Wireless Controller.

Most of the properties of each radio on a Wireless AP can be modified without requiring a reboot of the AP.

The Wireless AP keeps a backup copy of its software image. When a software upgrade is sent to the Wireless AP, the upgrade becomes the Wireless AP's current image and the previous image becomes the backup. In the event of failure of the current image, the Wireless AP will run the backup image.

---

**Note:** The HiPath Wireless Controller does not ship with sensor software. Sensor software must be installed on a TFTP server.

---

#### To maintain the list of current Wireless AP software images:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** page is displayed.
2. From the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.

The screenshot shows the Siemens HiPath Wireless AP configuration interface. The main content area is titled 'AP Software Maintenance' and contains the following sections:

- AP Images for Platform:** A drop-down menu is set to 'AP2600'. Below it, a list of images is shown, with 'AP200-V5R1.10014.0.img (Default)' selected. There are 'Set as default' and 'Delete' buttons below the list.
- Download AP Images:** Fields for 'FTP Server', 'User ID', 'Password', 'Confirm', 'Directory', and 'Filename'. A 'Platform' drop-down menu is set to 'AP2600'. A 'Download' button is at the bottom right of this section.
- Upgrade Behavior:** Two radio buttons: 'Upgrade when AP connects using settings from Controlled Upgrade' (selected) and 'Always upgrade AP to default image (overrides Controlled Upgrade settings)'. A 'Save' button is at the bottom right.
- Disk space left for images:** 107 MB.

The footer of the interface displays: [ HWC-206 | C2400 | 01 days, 07:20 ] User: admin Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] [ F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved.

3. In the **AP Images for Platform** drop-down list, click the appropriate platform.

## Configuring the Wireless AP

### Performing Wireless AP software maintenance

4. To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.
5. In the **Upgrade Behavior** section, select one of the following:
  - **Upgrade when AP connects using settings from Controlled Upgrade** – The **Controlled Upgrade** tab is displayed. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
  - **Always upgrade AP to default image (overrides Controlled Upgrade settings)** – Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.
6. To save your changes, click **Save**.

#### To delete a Wireless AP software image:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** page is displayed.
2. From the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
3. In the **AP Images for Platform** drop-down list, click the appropriate platform.
4. In the **AP Images** list, click the image you want to delete.
5. Click **Delete**. The image is deleted.

#### To download a new Wireless AP software image:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** page is displayed.
2. From the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
3. In the **Download AP Images** list, type the following:
  - **FTP Server** – The IP of the FTP server to retrieve the image file from.
  - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.



- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
  - **Filename** – The name of the image file to retrieve.
  - **Platform** – The AP hardware type to which the image applies. There are several types of AP and they require different images.
4. Click **Download**. The new software image is downloaded.

#### To define parameters for a Wireless AP controlled software upgrade:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** page is displayed.
2. From the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
3. Click the **Controlled Upgrade** tab.

The screenshot shows the Siemens HiPath Wireless AP software maintenance interface. The left navigation pane includes the following items: + 192.168.4.56 (P), AP Default Settings, AP Multi-edit, AP 802.1x Multi-edit, Client Management, Access Approval, AP Maintenance (highlighted), AP Registration, Sensor Management, CNL-209-AAA, CNL-209-briAP, CNL-209-briAP\_AAA, and CNL-209-CP. The main content area is titled 'AP Software Maintenance' and 'Controlled Upgrade'. It contains the following steps:

Step 1: Select AP Platform: AP2600

Step 2: Select an image to use: AP200-V4R1.5.9.img

Step 3: Apply the AP image from Step 2 to the selected APs below:

	Wireless APs	Current version	Upgrade to
<input type="checkbox"/>	0409920201201282	5.0.1	

Buttons: Select All, Clear All, Apply AP image version, Save for later, Upgrade Now

Step 4: Repeat Steps 1 - 3 as necessary  
 Step 5: Save this upgrade strategy for later, or upgrade the APs now:

**Note:** The **Controlled Upgrade** tab will appear only when the **Upgrade Behavior** is set to **Upgrade when AP connects using settings from Controlled Upgrade** on the **AP Software Maintenance** tab.

4. In the **Select AP Platform** drop-down list, click the type of AP you want to upgrade.
5. In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.

## Configuring the Wireless AP

### *Performing Wireless AP software maintenance*

6. In the list of registered **Wireless APs**, select the checkbox for each Wireless AP to be upgraded with the selected software image.
7. Click **Apply AP image version**. The selected software image is displayed in the **Upgrade To** column of the list.
8. To save the software upgrade strategy to be run later, click **Save for later**.
9. To run the software upgrade immediately, click **Upgrade Now**. The selected Wireless AP reboots, and the new software version is loaded.

---

**Note:** The **Always upgrade AP to default image** checkbox on the **AP Software Maintenance** tab overrides the **Controlled Upgrade** settings.

---

## 5 Virtual Network Services

This chapter describes Virtual Network Services (VNS) concepts, including:

- [VNS overview](#)
- [Setting up a VNS checklist](#)
- [Topology of a VNS](#)
- [RF assignment for a VNS](#)
- [Authentication for a VNS](#)
- [Filtering for a VNS](#)
- [Data protection on a VNS—WEP and WPA](#)
- [VNS global settings](#)
- [Setting up a new VNS](#)

### 5.1 VNS overview

A VNS is an IP subnet designed to enable Wireless APs to interact with wireless devices. A VNS is similar to a regular IP subnet. A VNS has the following properties:

- Each VNS is assigned a unique identifier.
- Each VNS is assigned a Service Set Identifier (SSID). The SSID does not have to be unique.
- Each VNS is assigned a range of IP addresses for wireless devices. All of the wireless devices share the same IP address prefix—the part of the IP address that identifies the network and subnet.

The IP addresses of the wireless devices are assigned dynamically by the HiPath Wireless Controller's Dynamic Host Configuration Protocol (DHCP) server within the assigned range.

---

**Note:** If the VNS is in branch mode, the HiPath Wireless Controller's DHCP server will not assign IP addresses to the wireless devices. For a routed VNS, you can allow the enterprise network's DHCP server to provide the IP addresses for the VNS by enabling DHCP Relay.

The assigned addresses must be within range of the VNS definition and the controller must be defined in the network as the path for traffic delivery to the mobile units. For more information, see [Section 6.3.1.8, "Using a DHCP relay for the VNS"](#), on page 172.

---

## Virtual Network Services

### Setting up a VNS checklist

These IP addresses are not virtual IP addresses. They are regular IP addresses and are unique over the network. These IP addresses are advertised to other hosts on the network to exchange traffic with the wireless devices in the VNS.

- A single overall filtering policy applies to all the wireless devices within the VNS. Additional filtering can be applied when the wireless user is authenticated by the Remote Authentication Dial-In User Service (RADIUS) server. This does not apply for a bridged VNS.
- When the HiPath Wireless Controller creates a VNS, it also creates a virtual IP subnet for that VNS. This does not apply for a bridged VNS.
- Each VNS represents a mobility group that, when configured, can be carried across multiple HiPath Wireless Controllers. This does not apply for a bridged VNS.
- Each VNS also offers unique Authentication, Authorization and Accounting (AAA) services.

## 5.2 Setting up a VNS checklist

VNS provides a versatile means of mapping wireless networks to the topology of an existing wired network. When you set up a VNS on the HiPath Wireless Controller, you are defining a subnet for a group of wireless device users. The VNS definition creates a virtual IP subnet where the HiPath Wireless Controller acts as a default gateway to wireless devices.

In addition you can determine if the VNS is to apply for traffic bridging at the AP. This type of VNS requires specification of RF parameters and authentication parameters (if AAA type), although filtering specifications and topology specifications do not apply.

The HiPath Wireless Controller C20/C2400 provides the option to define a VNS as locally bridged to a VLAN at the controller. To support that configuration, you must define which VLAN the VNS should bridge to. With this configuration, it is possible that the controller is not involved in the IP address assignment for user addresses. Instead, the IP addresses for users are assigned directly by the DHCP infrastructure that services the VLAN.

---

**Note:** In a VLAN-bridged VNS, the default configuration dictates that the controller is not the DHCP server for that segment. However, DHCP services can selectively be enabled, including DHCP Relay, allowing you to use the controller to become the default DHCP server for the VLAN, if applicable.

---

Before defining a VNS, the following properties must be determined:

- A user access plan for both individual users and user groups
- The RADIUS attribute values that support the user access plan
- The location and identity of the Wireless APs that will be used on the VNS
- The routing mechanism to be used on the VNS
- For tunneled configurations mostly, the network addresses that the VNS will use
- A VLAN bridged VNS (at the controller) requires the specification of the IP address for the controller's own interface point (Port) on that VLAN. In addition, if you elect to have the controller operate as the default DHCP server for the VLAN, the corresponding IP topology for that subnet must also be specified.
- The type of authentication for wireless device users on the VNS
- The specific filters to be applied to the defined users and user groups to control network access
- The quality of service (QoS) requirements
- What privacy mechanisms should be employed between the Wireless APs and the wireless devices
- Classification list for traffic priority. For example, whether the VNS is to be used for voice traffic and if voice traffic is to be given priority.
- Whether the VNS traffic is to be bridged directly to the network at the AP or tunneled to the controller for forwarding. Bridging at the AP is useful in branch office deployments in which APs must provide service even when the connection to the controller is unavailable.

#### User access plan

The user access plan should analyze the enterprise network and identify which users should have access to which areas of the network. What areas of the network should be separated? Which users can go out to the World Wide Web?

The Controller, Access Points and Convergence Software system relies on authenticating users via a RADIUS server (or other authentication server). To make use of this feature, an authentication server on the network is required. Make sure that the server's database of registered users, with login identification and passwords, is current.

In the case of certificate-based installations, you must ensure that the proper user certificate profiles are setup on the RADIUS server.

---

**Note:** To deploy Controller, Access Points and Convergence Software without a RADIUS server (and without authentication of users on the network), click **SSID** for network assignment (on the **Topology** tab). On the **Authentication** -

**Configure Captive Portal** page, select the **No Captive Portal** option. There will be no authentication of users, but the Controller, Access Points and Convergence Software is otherwise operational.

---

The user access plan should also identify the user groups in your enterprise, and the business structure of the enterprise network, such as:

- Department (such as Engineering, Sales, Finance)
- Role (such as student, teacher, library user)
- Status (such as guest, administration, technician)

For each user group, you should set up a filter ID attribute in the RADIUS server, and then associate each user in the RADIUS server to at least one filter ID name. You can define specific filtering rules, by filter ID attribute, that will be applied to user groups to control network access. Filtering is applied by the controller. Filter ID assignments is a configuration option, and not a requirement to setup per user filter ID definitions. If a filter is not returned by the Access-Accept confirmation for a particular user, the controller uses the default filter profile for the VNS as the applicable filter set.

## 5.3 Topology of a VNS

Before you decide if a VNS will participate in a VLAN and configure a VNS, define the global settings that will apply to all VNS definitions. For example, global settings can include identifying the location of the RADIUS servers and enabling priority traffic handling for voice-over-internet traffic and dynamic authorization server support.

The type of network assignment determines all the other factors of the VNS. There are two options for network assignment:

- **SSID:**
  - Has Captive Portal authentication, or no authentication
  - Requires restricted filtering rules before authentication
  - Requires filtering rules for group filter IDs after authentication. A default filter applies if a more specific filter is not indicated by the RADIUS Access-Accept response.
  - Used for a VNS supporting wireless voice traffic (QoS)
  - Used for a VNS supporting third-party APs
  - Has WEP and WPA-PSK privacy
- **AAA:**

- Has 802.1x authentication
- Requires filtering rules for group filter IDs and default filter. A definition of group filter IDs is optional. If a filter is not specified or not returned by the Access-Accept response, the default filter group is applied.
- Has WEP and WPA privacy
- HiPath Wireless Controller is involved in authenticating users. 802.1x packets for AAA assignment are forwarded by the Wireless AP to the HiPath Wireless Controller through to the RADIUS server.

### Traffic behavior types

There are 4 traffic types available when setting up your VNS:

- Tunneled to controller
- Bridged at AP
- Bridged to VLAN at controller
- Wireless Distribution System (WDS)

The Wireless APs are assigned to the VNS by radios. A Wireless AP radio is available for VNS assignment until it has been assigned to a maximum eight VNSs with the exception of WDS VNS that can handle maximum of seven VNSs. For more information, see [Section 6.17, “Wireless Distribution System”](#), on page 229.

The HiPath Wireless Controller can support the following:

- C2400 – Up to 64 VNSs
- C20 – Up to 8 VNSs

Once a VNS definition is saved, the HiPath Wireless Controller updates this information on the Wireless AP. The VNS broadcasts the updates during beacon transmission, unless the SSID beacon is suppressed on the **Topology** tab.

The **Wireless AP Configuration** page lists defined VNSs and which radio each has been assigned to.

On the **Topology** tab, define parameters for DHCP for IP address assignment. DHCP IP assignment is not applicable to Bridged at AP mode. DHCP assignment is disabled by default for Bridged to VLAN mode. However, you can enable DHCP server/relay functionality to have the controller service the IP addresses for the VLAN (and wireless users).

You can also configure this VNS for management traffic or for third-party APs.

## 5.4 RF assignment for a VNS

The second step in setting up a VNS is to configure the RF assignment for the VNS. From the **RF** tab you assign APs to a VNS and SSID definitions.

## 5.5 Authentication for a VNS

The third step in setting up a VNS is to configure the authentication mechanism for the VNS. The authentication mechanism depends on the network assignment. In addition, all VNS definitions can include authentication by Media Access Control (MAC) address. Authentication by MAC address provides a method of access control for a user as it associates with the AP based on the device's MAC address.

### 5.5.1 Authentication with SSID network assignment

If network assignment is SSID, there are two authentication options:

- **None** – This authentication method is the default for a new SSID assignment VNS. Authentication VNS, unless MAC-based authorization is used, the default filter is applied, not the non-authentication filter. For more information, see [Section 5.6, “Filtering for a VNS”, on page 154](#).
- **Captive Portal** – This authentication method employs a Web redirection which directs a user's Web session to an authentication server. Typically, the user must provide their credentials (userID, password) to be authenticated. The Captive Portal redirection operation will redirect any Web page requests corresponding to targets not explicitly allowed by the non-authenticated filter. The redirection will instruct the user's Web page to contact the defined authentication Web server. You must ensure that the authentication Web server is explicitly listed as an allow destination in order for traffic to access it.

The HiPath Wireless Controller supports two modes of Captive Portal authentication:

- **Internal Captive Portal** – The controller's own Captive Portal authentication page (configured as an editable form) is used to request user credentials.
- **External Captive Portal** – An entity outside of the HiPath Wireless Controller is responsible for handling the user authentication process, presenting the credentials request forms and performing user authentication procedures. The controller is then informed of the authentication results via its Business Ecosystem's interfaces.

Four authentication types are supported for Captive Portal authentication:



- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Windows-specific version of CHAP (MS CHAP)
- MS CHAP v2 (Windows-specific version of CHAP, version 2)

For Captive Portal authentication, the RADIUS server must support the selected authentication type: PAP, CHAP (RFC2484), MS-CHAP (RFC2433), or MS-CHAPv2 (RFC2759).

## 5.5.2 Authentication with AAA (802.1x) network assignment

If network assignment is AAA with 802.1x authentication, the wireless device user requesting network access must first be authenticated. The wireless device's client utility must support 802.1x. The user's request for network access along with login identification or a user profile is forwarded by the HiPath Wireless Controller to a RADIUS server. The HiPath Wireless Controller, Access Points and Convergence Software system supports the following authentication types:

- **Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)** – Relies on client-side and server-side certificates to perform authentication. Can be used to dynamically generate a Pairwise Master Key for encryption.
- **Extensible Authentication Protocol with Tunneled Transport Layer Security (EAP-TTLS)** – Relies on mutual authentication of client and server through an encrypted tunnel. Unlike EAP-TLS, it requires only server-side certificates. The client uses PAP, CHAP, or MS-CHAPv2 for authentication.
- **Protected Extensible Authentication Protocol (PEAP)** – Is an authentication protocol similar to TTLS in its use of server side certificates for server authentication and privacy and its support for a variety of user authentication mechanisms.

For 802.1x, the RADIUS server must support RADIUS extensions (RFC2869).

Until the access-accept is received from the RADIUS server for a specific user, the user is kept in an unauthenticated state. 802.1x rules dictate no other packets other than EAP are allowed to traverse between the AP and the HiPath Wireless Controller until authentication completes. Once authentication is completed (access-accept is received), the user's client is then allowed to proceed with IP services, which typically implies the request of an IP address via DHCP.

In addition, the definition of a specific filter ID is optional configuration. If a specific filter ID is not defined or returned by the access-accept operation, the HiPath Wireless Controller assigns the VNS' default filter for authenticated users.

---

**Note:** The HiPath Wireless Controller only assigns the device's IP after the client requests one.

---

Both Captive Portal and AAA (802.1x) authentication mechanisms in Controller, Access Points and Convergence Software rely on a RADIUS server on the enterprise network. You can identify and prioritize up to three RADIUS servers on the HiPath Wireless Controller—in the event of a failover of the active RADIUS server, the HiPath Wireless Controller will poll the other servers in the list for a response. Once an alternate RADIUS server is found, it becomes the active RADIUS server, until it either also fails, or the administrator redefines another.

## 5.6 Filtering for a VNS

The VNS capability provides a technique to apply policy, to allow different network access to different groups of users. This is accomplished by packet filtering.

After setting authentication, define the filtering rules for the filters that apply to your network and the VNS you are setting up. Several filter types are applied by the HiPath Wireless Controller:

- **Exception filter** – Protect access to a system's own interfaces, including the VNS' own interface. VNS exception filters are applied to user traffic intended for the HiPath Wireless Controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
- **Non-authenticated filter with filtering rules that apply before authentication** – Controls network access and to direct users to a Captive Portal Web page for login.
- **Group filters, by filter ID, for designated user groups** – Controls access to certain areas of the network, with values that match the values defined for the RADIUS filter ID attribute.
- **Default filter** – Controls access if there is no matching filter ID for a user.

Within each type of filter, define a sequence of filtering rules. The filtering rule sequence must be arranged in the order that you want them to take effect. Each rule is defined to allow or deny traffic in either direction:

- **In** – From a wireless device in to the network
- **Out** – From the network out to a wireless device

## 5.6.1 Final filter rule

The final rule in any filter should act as a catch-all for any traffic that did not match a filter. This final rule should either allow all or deny all traffic, depending on the requirements for network access. For example, the final rule in a non-authenticated filter for Captive Portal is typically deny all. A final allow all rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found.

A default rule of deny all is automatically created by the system for initial filter definitions. The administrator can change the action to allow all. However, a default filter rule cannot be removed. Since a default filter rule provides a catch-all default behavior for packet handling, all applicable user defined filter rules must be defined prior to this rule.

Each rule can be based on any one of the following:

- Destination IP address or any IP address within a specified range that is on the network subnet (as a wildcard)
- Destination ports, by number and range
- Protocols (UDP, TCP, etc.)

## 5.6.2 Filtering sequence

The filtering sequence depends on the type of authentication used:

- **No authentication (network assignment by SSID)**

Only the default filter will apply. Specific network access can be defined.

- **Authentication by captive portal (network assignment by SSID)**

The non-authenticated filter will apply before authentication. Specific network access can be defined. The filter should also include a rule to allow all users to get as far as the Captive Portal Web page where the user can enter login identification for authentication. When authentication is returned, the filter ID group filters are applied. If no filter ID matches are found, then the default filter is applied. The filter ID group is an optional behavior specification. If a filter ID is not returned, or an invalid one is returned, the default filter group is applied.

- **Authentication by AAA (802.1x)**

AAA assignment requires that user authentication is completed using the 802.1x/EAP protocol before a user is granted access to a network resource. Therefore, the enforcement of non-authenticated traffic rules is not applicable. When authentication is returned, then the filter ID group filters are applied. A VNS can have a subgroup with Login-LAT-Group ID that has its own filtering rules. The Login-LAT-Group indicates that a user session should be associated with a more specific VNS (a child VNS). The sub-VNS provides a

## Virtual Network Services

### Data protection on a VNS—WEP and WPA

different topology definition than the parent VNS, as well as having its own set of filter definitions. Filter IDs returned in association with a Login-LAT-Group definition are applied to the user, in relation to the sub-VNS indicated by the Login-LAT-Group specification. If no filter ID matches are found, then the default filter is applied.

The following is a high-level description of how HiPath Wireless Controller filters traffic:

**Step One** – The HiPath Wireless Controller attempts to match each packet of a VNS to the filtering rules that apply to the wireless device user.

**Step Two** – If a filtering rule is matched, the operation to allow or deny is executed.

**Step Three** – The next packet is fetched for filtering.

## 5.7 Data protection on a VNS—WEP and WPA

On wireless and wired networks, data is protected by encryption techniques. The type of data protection that is available depends on the VNS assignment mode:

- **SSID** – Only WEP and WPA (1 or 2)-PSK privacy types are available
- **AAA** – WEP, Dynamic WEP, and WPA (1 or 2) privacy types are available

### Data protection encryption techniques

- **Wired Equivalent Privacy (WEP)** – WEP encrypts data sent between wireless nodes. Each node must use the same encryption key.
- **Wi-Fi Protected Access Privacy (WPA v.1 and v.2)** – Encryption is by Advanced Encryption Standard (AES) or by Temporal Key Integrity Protocol (TKIP). Two modes are available:
  - **Enterprise** – Specifies 802.1x authentication and requires an authentication server
  - **Pre-Shared Key (PSK)** – Relies on a shared secret. The PSK is a shared secret (pass-phrase) that must be entered in both the Wireless AP or router and the WPA clients.

---

**Note:** The Wireless 802.11n AP does not support WPA v.1 and v.2 encryption. For more information, see [Section 6.11, “Configuring privacy for a VNS”](#), on page 208.

---

## 5.8 VNS global settings

Before defining a specific VNS, define the global settings that will apply to all VNS definitions. These global settings include:

- Identify the location and password of RADIUS servers on the enterprise network. The defined servers appear as available choices when you set up the authentication mechanism for each VNS.
- Define the shared secret used to encrypt the Pairwise Master Key (PMK) for WPA2 v.2 pre-authentication between HiPath Wireless Controllers on the network.
- Enable Dynamic Authorization Server (DAS) configuration support.
- Adjust admission control thresholds. Admission control thresholds protect admitted traffic against overloads, provides distinct thresholds for VO and VI, and distinct thresholds for roaming and new streams.

---

**Note:** The Wireless 802.11n AP does not support admission control thresholds.

---

### To define RADIUS servers for VNS global settings:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network** list is displayed.
2. In the left pane, click **Global Settings**. The **Authentication** tab is displayed.

## Virtual Network Services

### VNS global settings

The screenshot displays the Siemens HiPath Virtual Network Configuration web interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The main content area is titled 'Global Settings' and features a left-hand sidebar with a tree view of 'Virtual Networks' including items like 'bridgedAC2', 'CNL-209-3rdCP', 'CNL-209-AAA', 'AAA\_vns1', 'AAA\_vns2 \*', 'CNL-209-AAA1', 'CNL-209-briAC1\_AAA', 'briAC\_Child1', 'CNL-209-briAP', 'CNL-209-CP', 'vns1 \*', 'vns2 \*', 'CNL-209-None', 'CNL-209-Test', 'CNL-209-wds', 'CNL-209-wds-2', and 'CNL-209-WEP'. Below the sidebar are buttons for 'Add subnet', 'Rename subnet', and 'Delete subnet'. The main panel is titled 'Authentication' and contains tabs for 'DAS', 'Wireless QoS', and 'General'. The 'RADIUS Servers' section shows a list of servers with 'freeradius209' and 'JASPER' selected. To the right of the list are input fields for 'Server Name' (freeradius209), 'Server Address' (192.168.4.21), and 'Shared Secret' (masked with dots). There are 'Unmask' and 'Add Server' buttons. A note states: '\* RADIUS servers which are currently associated with VNS(s) cannot be removed'. A 'Remove selected server' button is located below the list. A 'Save' button is at the bottom right. The footer contains system information: '[ HWC-206 | C2400 | 01 days, 07:23 ] User: admin Port status: [ M 1 2 3 4 F ] Enterprise Software: V5 R1.10014.0 | Trading: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved.'

3. To define a RADIUS server available on the network, do the following:

- In the **Server Name** box, type a name.
- In the **Server Address** box, type the IP address.
- In the **Shared Secret** box, type the password that is required in both directions. This password is used to validate the connection between controller and the RADIUS server.

4. In order to proofread your password before saving the configuration, click **Unmask**. The password is displayed. To mask the password, click **Mask**.

This precautionary step is highly recommended in order to avoid an error, later, when the HiPath Wireless Controller attempts to communicate with the RADIUS server.

5. To add the server to the list, click **Add**.

6. To remove a server, click the server in the list, and then click **Remove selected server**.

7. To save your changes, click **Save**.

**To define admission control thresholds for VNS global settings:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network** list is displayed.
2. In the left pane, click **Global Settings**. The **Authentication** tab is displayed.
3. Click the **Wireless QoS** tab.

The screenshot shows the Siemens HiPath Virtual Network Configuration web interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', and 'Mitigator'. The 'VNS Configuration' tab is active. On the left, the 'Global Settings' section is expanded, showing a list of Virtual Networks. The main content area is titled 'Admission Control Thresholds' and contains four settings, each with a percentage value in a drop-down menu:

- Max Voice (VO) BW for roaming streams: 80%
- Max Voice (VO) BW for new streams: 60%
- Max Video (VI) BW for roaming streams: 60%
- Max Video (VI) BW for new streams: 40%

A note below the settings states: 'Note: Settings only apply on APs serving QoS-enabled VNS with Admission Control enabled'. A 'Save' button is located at the bottom right of the settings area. The status bar at the bottom shows system information: '[ HWC-206 ] C2400 | 01 days, 07:24 | User: admin Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] [ F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved.'

4. Using the percentage drop-down lists, define the thresholds for the following:
  - **Max Voice (VO) BW for roaming streams** – The maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.
  - **Max Voice (VO) BW for new streams** – The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.
  - **Max Video (VI) BW for roaming streams** – The maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.
  - **Max Video (VI) BW for new streams** – The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.

## Virtual Network Services

### VNS global settings

These global QoS settings apply to all APs that serve QoS enabled VNSs with admission control.

---

**Note:** The Wireless 802.11n AP does not support admission control thresholds.

---

5. To save your changes, click **Save**.

#### To define inter-HiPath Wireless Controller shared secret for VNS global settings:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network** list is displayed.
2. In the left pane, click **Global Settings**.
3. Click the **General** tab.

4. In the **Inter-HWC Shared Secret** box, type a password between 8 and 63 characters long, to be used between HiPath Wireless Controllers. The shared secret is to encrypt pre-shared keys that have to be moved between controllers for mobility. The same shared secret must also be defined on the other HiPath Wireless Controllers on the network.
5. In order to proofread your password before saving the configuration, click **Unmask**. The password is displayed. To mask the password, click **Mask**.



This precautionary step is highly recommended in order to avoid an error, later, when the HiPath Wireless Controller attempts to communicate with the RADIUS server.

6. To save your changes, click **Save**.

## **5.9 Setting up a new VNS**

Now that you are familiar with the VNS concepts, you can now set up a new VNS. Setting up a new VNS involves the following general steps:

- Step one – Create a VNS name
- Step two – Define the topology parameters
- Step three – Configure the VNS

For information on setting up a new VNS, see [Chapter 6](#), “Virtual Network configuration”.

## **Virtual Network Services**

*Setting up a new VNS*

## 6 Virtual Network configuration

This chapter discusses VNS (Virtual Network Services) configuration, including:

- Topology for a VNS
- Assigning Wireless AP radios to a VNS
- Authentication for a VNS
- Defining accounting methods for a VNS
- Defining RADIUS filter policy for VNSs and VNS groups
- Configuring filtering rules for a VNS
- Enabling multicast for a VNS
- Configuring privacy for a VNS
- Defining a VNS with no authentication
- Defining priority level and service class for VNS traffic
- Working with Quality of Service (QoS)
- Configuring the QoS policy on a VNS
- Bridging traffic locally
- Wireless Distribution System

Setting up a VNS defines a virtual IP subnet for a group of wireless device users, where the HiPath Wireless Controller acts as a default gateway to wireless devices. For each VNS, you define its topology, authentication, accounting, RADIUS servers, filtering, multicast parameters, privacy and policy mechanism. When you set up a new VNS, additional tabs appear only after you save the topology.

### 6.1 VNS Types

The VNS topologies are classified on the basis of the following VNS types:

- **Routed VNS** – User traffic is tunneled to the HiPath Wireless Controller. (This is the default setup.)
- **Bridged at the AP VNS** – User traffic is directly bridged to a VLAN at the AP network point of access (switch port).
- **VLAN bridged VNS** – User traffic is tunneled to the HiPath Wireless Controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet.

## Virtual Network configuration

### Creating a new VNS name

- **Wireless Distribution System (WDS)** – User traffic plies over a wireless network that uses multiple access points interconnected via wireless links. For more information, see [Section 6.17.7, “Deploying the WDS system”](#), on page 238.

---

**Note:** The bridged at the controller, routed and bridged at the AP VNSs are the network VNSs and they are used to service the client devices. The WDS VNS is used for establishing WDS links between WDS Wireless APs.

---

## 6.2 Creating a new VNS name

Setting up a new VNS involves the following general steps:

- Step one – Create a VNS name:
- Step two – Defining the topology parameters
- Step three – Configuring the VNS

Before you can define the VNS topology parameters and configure the VNS, you must first create a new VNS name.

### To create a new VNS name:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane, type a name that will identify the new VNS in the **Add subnet** box.
3. Click **Add subnet**. The name is displayed in the **Virtual Networks** list. The **Topology** tab is displayed.

The following sections describe in detail how to define the VNS topology parameters and configure the VNS.

## 6.3 Topology for a VNS

On the **Topology** tab, the key choice for a VNS is the type of network assignment, which determines all the other factors of the VNS. When you have completed defining the topology for your VNS, save the topology settings. Once your topology is saved, you can then access the remaining VNS tabs and continue configuring your VNS.

There are two options for network assignment:

- **SSID** – The SSID determines the VNS to which a user profile will be assigned (user topology/IP, filters):
  - Has Captive Portal authentication, or no authentication (as well as MAC-based authentication).
  - Requires restricted filtering rules before authentication and, after authentication, filtering rules for group filter IDs.
  - Is used for a VNS supporting wireless voice traffic (QoS).
  - Is used for a VNS supporting third-party APs.
  - Has WEP and WPA-PSK privacy.
- **AAA** (Authentication, Authorization and Accounting):
  - has 802.1x authentication (as well as MAC-based authentication).
  - requires filtering rules for group filter IDs and default filter.
  - has Dynamic WEP and WPA (WPA v.1 and WPA v.2) privacy.

### **6.3.1 Configuring topology for a VNS for Captive Portal**

The section describes how to set up a VNS for Captive Portal. The **RF** tab, where you assign APs to VNSs, is not accessible until the topology for the VNS has been configured and saved.

## Virtual Network configuration

### Topology for a VNS

#### To create an SSID for Captive Portal VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to create an SSID for. The **Topology** tab is displayed.
3. From the **Assignment by** drop-down list, click **SSID**.

#### 6.3.1.1 Defining session timeout parameters

The HiPath Wireless Controller allows a client to associate to the AP and exist on the network without having authentication. Every associated user has a user session tracked by the HiPath Wireless Controller from the time of association with the AP. Users can be temporarily (or longer for SSID assigned VNSs) be in the non-authenticated state. Pre timeout is the maximum amount of time allowed to elapse from the last time any traffic was received by the system for an unauthenticated user. For example, a user may have disconnected from the system (shutdown the device, moved out of range, etc.). A pre timeout expires and cleans up the session.

The post timeout is the max amount of time that is allowed to elapse from the last time any traffic was received for an authenticated user. For example, a user may have disconnected from the system and is no longer be connected. A post timeout expires and cleans up the session.

A client that exceeds either the pre or post timeout value will be forced to disassociate.

The session timer defines the maximum amount of time a session is allowed to be connected to the system. The session timer is particularly useful in pay-per-use models. When the lifetime of the session reaches the defined limit, the session is expired and cleaned up. A user would have to re-authenticate with the system to continue to receive network services.

---

**Note:** The VNS timeout parameters define the default timers applicable to session management within the VNS. However, RADIUS authentication (access-accept) may return specific timers applicable to the particular user. A RADIUS returned value overwrites the VNS default values for the specific user.

In addition, a zero (0) value for any of the timers indicates a non-applicable value. Therefor, the corresponding timer is not enforced.

---

#### **To define the session timeout parameters for a VNS:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define the session timeout parameters for. The **Topology** tab is displayed.
3. In the **Idle (pre)** box, type the number of minutes that a client is allowed to be idle on the VNS before authentication.
4. In the **Idle (post)** box, type the number of minutes that a client is allowed to be idle on the VNS after authentication.
5. In the **Session** box, type the maximum time limit of a session. If you do not provide a Session value, there is no time limit.

#### **6.3.1.2 Enabling management traffic**

If management traffic is enabled for a VNS, it overrides the built-in exception filters that prohibit traffic on the HiPath Wireless Controller data interfaces. For more information, see [Section 6.9, "Configuring filtering rules for a VNS"](#), on page 194.

## Virtual Network configuration

### Topology for a VNS

#### To enable management traffic on a VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to enable management traffic for. The **Topology** tab is displayed.
3. Select the **Allow mgmt traffic** checkbox.

#### 6.3.1.3 Enabling third-party APs on a VNS

Configuring a VNS for third-party APs is only available with SSID network assignment. Use this function as part of the process defined in [Chapter 8, “Working with third-party APs”](#).

A third-party AP VNS allows for the specification of a segregated subnet by which non-HiPath Wireless APs are used to provide RF services to users while still utilizing the HiPath Wireless Controller for user authentication and user policy enforcement.

---

**Note:** Third-party AP devices are not fully integrated with the system and therefore must be managed individually to provide the correct user access characteristics. Also, third-party AP devices must be defined in bridge mode so that user traffic is directly transposed to the third-party AP subnet and picked up by the HiPath Wireless Controller for forwarding and policy enforcement.

---

#### To enable third-party APs on a VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to enable third-party APs for. The **Topology** tab is displayed.
3. Select the **Use 3rd Party AP** checkbox.

The definition of third-party AP identification parameters allows the system to be able to differentiate the third-party AP device (and corresponding traffic) from user devices on that segment. Devices identified as third-party APs are considered pre-authenticated, and are not required to complete the corresponding authentication verification stages defined for users in that segment (typically Captive Portal enforcement).

In addition, third-party APs have a specific set of filters (third-party) applied to them by default, which allows the administrator to provide different traffic access restrictions to the third-party AP devices for the users that use those resources. The third-party filters could be used to allow access to third-party APs management operations (for example, HTTP, SNMP).



4. To save your changes, click **Save**.

#### 6.3.1.4 Defining a next hop route and OSPF advertisement for a VNS

The next hop definition allows the administrator to define a specific host as the target for all non-VNS targeted traffic for users in a VNS. The next hop IP identifies the target device to which all VNS (user traffic) will be forwarded to. Next-hop definition supersedes any other possible definition in the routing table.

If the traffic destination from a wireless device on a VNS is outside of the VNS, it is forwarded to the next hop IP address, where this router applies policy and forwards the traffic. This feature applies to unicast traffic only. In addition, you can also modify the Open Shortest Path First (OSPF) route cost.

OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place.

##### To define a next hop route and OSPF advertisement:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define a next-hop route for. The **Topology** tab is displayed.
3. In the **Next Hop Address** box, type the IP address of the next hop router on the network through which you wish all traffic on this VNS to be directed.
4. In the **OSPF Route Cost** box, type the OSPF cost of reaching the VNS subnet.

The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the controller as a better fit or lowest cost path to reach devices in a particular network. The higher the cost, the less likely of the possibility that the controller will be chosen as a route for traffic, unless that controller is the only possible route for that traffic.

5. To disable OSPF advertisement on this VNS, select the **disable OSPF Advertisement** checkbox.

#### 6.3.1.5 Defining the IP address for the VNS (for the DHCP server on the controller)

Bridged at the AP VNSs do not require the definition of a corresponding IP address definition for the VNS since all traffic for users in that VNS will be directly bridged by the AP at the local network point of attachment (VLAN at AP port).

The IP address definition is only required for a routed VNS or VLAN bridged VNS.

##### To define the IP address for the VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define the IP address for. The **Topology** tab is displayed.
3. In the **Gateway** box, type the HiPath Wireless Controller's own IP address in that VNS.

This IP address is the default gateway for the VNS. The HiPath Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to MUs (in the VNS) as the default gateway for the VNS subnet. (MUs target the HiPath Wireless Controller's interface in their effort to route packets to an external host).

For a VLAN bridged VNS, the IP address corresponds to the HiPath Wireless Controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.

---

**Note:** If you are configuring Bridged at Controller VNS, the Gateway field appears as Interface **IP Addr** on the user interface.

---

4. In the **Mask** box, type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).

The following values to DHCP configuration are only applicable for configurations if the controller is the DHCP server for users in the VNS—a routed VNS or a VLAN bridged VNS with DHCP enabled (by default, DHCP is disabled). These values are not visible for a bridged at AP VNS or a VLAN bridged VNS with DHCP disabled (by default, DHCP is disabled).

The **Address Range** boxes (from and to) populate automatically with the range of IP addresses to be assigned to wireless devices using this VNS, based on the IP address you provided.

- To modify the address in the **Address Range from** box, type the first available address.

- To modify the address in the **Address Range to** box, type the last available address.
- If there are specific IP addresses to be excluded from this range, click **Exclusion(s)**. The DHCP Address Exclusion window is displayed.

- In the DHCP Address Exclusion window, do one of the following:
    - To specify an IP range, type the first available address in the **From** box and type the last available address in the **to** box. Click **Add** for each IP range you provide.
    - To specify a IP address, select the **Single Address** option and type the IP address in the box. Click **Add** for each IP address you provide.
  - To save your changes, click **Save**. The DHCP Address Exclusion window closes.
5. The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the VNS.
  6. In the **Domain Name** box, type the external enterprise domain name.

### 6.3.1.6 Modifying time limits for IP assignments

The following procedure is only applicable for configurations if the controller is the DHCP server for users in the VNS—a routed VNS or a VLAN bridged VNS with DHCP enabled (by default, DHCP is local). These values are not visible for a bridged at AP VNS or a VLAN bridged VNS with DHCP disabled (by default, DHCP is disabled).

Time limits for IP assignments dictate the default and the maximum time limits a wireless device can keep the DHCP server-assigned IP address.

## Virtual Network configuration

### *Topology for a VNS*

#### **To modify time limits for IP assignments:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to set time limits for. The **Topology** tab is displayed.
3. In the **Lease default** box, type the default time limit. The default time limit dictates how long a wireless device can keep the DHCP server assigned IP address. The default value is 36000 seconds (10 hours).
4. In the **Lease max** box, type the maximum time limit. The default time limit is 2539000 seconds (approximately 705 hours or 29 days).

#### **6.3.1.7 Setting the name server configuration**

Although this procedure could also apply to any VNS type, normally these settings are defined in the context of DHCP definitions and therefore these values are not available for configurations if DHCP service is not defined.

A VLAN bridged VNS has an option to define the DHCP behavior for the VNS. By default, the DHCP service is disabled although the administrator can elect to have the controller's VNS interface on the VLAN become either the actual DHCP server (enable DHCP) or become the relay agent for DHCP requests.

#### **To set the name server configuration:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to set the name server configuration for. The **Topology** tab is displayed.
3. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
4. If applicable, in the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

#### **6.3.1.8 Using a DHCP relay for the VNS**

Although this procedure could also apply to any VNS type, normally these settings are defined in the context of DHCP definitions and therefore these values are not available for configurations if DHCP service is not defined.

Using a DHCP relay forces the HiPath Wireless Controller to forward DHCP requests to an external DHCP server on the enterprise network. This function bypasses the local DHCP server for the HiPath Wireless Controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.

The range of IP addresses assigned to the wireless device users on this VNS should also be designated on the external DHCP server.

**To use an external DHCP server for the VNS:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to use DHCP relay for. The **Topology** tab is displayed.
3. From the **DHCP Option** drop-down list, click **Use DHCP Relay**.
4. In the **Gateway** box, type the IP address for the VNS.
5. In the **Mask** box, type the appropriate subnet mask for this IP address.
6. In the **DHCP Server** box, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. In the case of relay, the HiPath Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

---

**Note:** The DHCP Server must be configured to match the VNS settings. In particular for Routed VNS', the DHCP server must identify the HiPath Wireless Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)

---

### 6.3.2 Configuring topology for a VNS for AAA

The following sections describe how to configure the topology for a VNS for AAA.

**To create an AAA topology:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to create an AAA topology for. The **Topology** tab is displayed.
3. From the **Assignment by** drop-down list, click **AAA**.

## Virtual Network configuration

### Assigning Wireless AP radios to a VNS

SIEMENS HiPath Virtual Network Configuration

Home | Logs & Traces | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator | Help | LOGOUT

Global Settings

Virtual Networks

- bridgedAC2
- CNL-209-3rdCP
- CNL-209-AAA
  - AAA\_vns1
  - AAA\_vns2 \*
- CNL-209-AAA1
- CNL-209-briAC
  - 1\_AAA
  - briAC\_Child
    - 1
- CNL-209-briAP
- CNL-209-CP
  - vns1 \*
  - vns2 \*
- CNL-209-None
- CNL-209-Test
- CNL-209-wds
- CNL-209-wds-2
- CNL-209-WEP

Trial

Add subnet

Rename subnet

Delete subnet

Topology

Topology settings required before other attributes can be configured

VNS Mode: Routed

DHCP Option: Local DHCP Server

Gateway:

Mask:

Address Range: from: to:

B'cast Address:

Domain Name:

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

Network Assignment:

Assignment by: AAA

Allow mgmt traffic

Timeout:

Idle: (pre) 5 minutes

(post) 30 minutes

Session: 0 minutes

Next Hop Routing:

Next Hop Address:

OSPF Route Cost: 50000

\* routing table/default cost used if not specified

Disable OSPF Advertisement

Save Cancel

VNS has been created

[ HWC-206 ] C2400 | 01 days, 07:27 ] User: admin Port status: M 1 2 3 4 F

Enterprise Software: V5 R1.10014.0 | Tracing: Inactive

© Copyright: 2006-2008 Siemens AG. All Rights Reserved.

4. Configure the topology for your VNS accordingly. For more information, see Section 6.3, “Topology for a VNS”, on page 164.
5. To save your changes, click **Save**.

### 6.3.3 Saving your topology properties

Once your topology is defined, you can then save your topology properties to continue configuring your VNS. To save your topology properties, click **Save**.

## 6.4 Assigning Wireless AP radios to a VNS

If two HiPath Wireless Controllers have been paired for availability (for more information, see Section 7.1, “Availability overview”, on page 251), each HiPath Wireless Controller's registered Wireless APs will appear as foreign in the list of available Wireless APs on the other HiPath Wireless Controller.

Once you have assigned a Wireless AP radio to eight VNSs, it will not appear in the list for another VNS setup. Each radio can support up to eight SSIDs (16 per AP). Each AP can be assigned to any of the VNSs defined within the system. The HiPath Wireless Controller can support the following:

- C2400 – Up to 64 VNSs

- C20 – Up to 8 VNSs

---

**Note:** You can assign the radios of all three Wireless AP variants — HiPath Wireless AP, HiPath Wireless Outdoor AP, and Wireless 802.11n AP — to any VNS.

---

**To assign Wireless APs to a VNS:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to assign Wireless APs to. The **Topology** tab is displayed.
3. Click the **RF** tab.
4. In the **SSID** box, type the SSID that wireless devices will use to access the Wireless AP.
5. In the **Advanced RF Settings**, select the following:
  - **Suppress SSID** – Select to prevent this SSID from appearing in the beacon message sent by the Wireless AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
  - **Enable proprietary IE** – Select to enable radio channel reports to be sent to the Wireless AP for improving roaming time and reliability, as well as improving client power consumption. The AP channel report lists all channels on which the VNS can be found—all channels used by all APs that have been assigned to the VNS. The AP will provide this list in a proprietary information element to be included in Beacon and Probe response packets. By default this option is disabled. It is recommended to enable this option.
  - **Enable 11h support** – Select to enable TPC (Transmission Power Control) reports. By default this option is disabled. It is recommended to enable this option.
    - **Apply power back-off** – Select to enable the AP to use reduced power (as does the 11h client). By default this option is disabled. It is recommended to enable this option.
  - **Process client IE requests** – Select to enable the AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IE's in the corresponding Probe Response frames. By default this option is disabled. It is recommended to enable this option.

## Virtual Network configuration

### Deleting a VNS

6. From the **Wireless APs** list, click the APs and their radios that you want to assign to the VNS. You can also use the **Select APs** list, to select APs and their radios by grouping:
  - **All radios** – Click to assign all of the APs' radios.
  - **a radios** – Click to assign only the APs' a radios.
  - **b/g radios** – Click to assign only the APs' b/g radios.
  - **local APs - all radios** – Click to assign only the local APs.
  - **local APs - a radios** – Click to assign only the local APs' a radios.
  - **local APs - b/g radios** – Click to assign only the local APs' b/g radios.
  - **foreign APs - all radios** – Click to assign only the foreign APs.
  - **foreign APs - a radios** – Click to assign only the foreign APs' a radios.
  - **foreign APs - b/g radios** – Click to assign only the foreign APs' b/g radios.
  - **clear all selections** – Click to clear all of the AP radio assignments.
  - **original selections** – Click to return to the AP radio selections prior to the most recent save.
7. To save your changes, click **Save**.

You can view the VNSs that each radio is assigned to by clicking the radio tabs from the **Wireless AP Configuration** page.

## 6.5 Deleting a VNS

You can delete the VNSs that are not in use.

### To delete the VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. From the list of **Virtual Networks**, click the VNS.
3. To delete the VNS, click **Delete subnet**.

## 6.6 Authentication for a VNS

The next step in configuring a VNS is to set up the authentication mechanism. There are various authentication combinations available:



- If network assignment is by SSID, authentication can be:
  - none
  - by Captive Portal using internal Captive Portal
  - by Captive Portal using external Captive Portal
  - by MAC-based authentication
- If network assignment is by AAA (802.1x), authentication can be:
  - by 802.1x authentication, the wireless device user must be authenticated before gaining network access
  - by MAC-based authentication

The first step for any type of authentication is to select RADIUS servers for:

- Authentication
- Accounting
- MAC-based authentication

MAC-based authentication enables network access to be restricted to specific devices by MAC address. In addition to the other types of authentication, when MAC-based authentication is employed the HiPath Wireless Controller queries a RADIUS server to determine if the wireless client's MAC address is authorized to access the network.

### 6.6.1 Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Controller, Access Points and Convergence Software authentication mechanism provides six VSAs for RADIUS and other authentication mechanisms.

Attribute Name	ID	Type	Messages	Description
Siemens-URL-Redirection	1	string	Returned from RADIUS server	A URL that can be returned to redirect a session to a specific Web page.
Siemens-AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign policy based on AP name or location.
Siemens-AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.

Table 14 Vendor Specific Attributes

## Virtual Network configuration

### Authentication for a VNS

Attribute Name	ID	Type	Messages	Description
Siemens-VNS-Name	4	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning policy and billing options, based on service selection.
Siemens-SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning policy and billing options, based on service selection.
Siemens-BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning policy and billing options, based on service selection and location.

Table 14 Vendor Specific Attributes

The first five of these VSAs provide information on the identity of the specific Wireless AP that is handling the wireless device, enabling the provision of location-based services.

The RADIUS message also includes RADIUS attributes Called-Station-Id and Calling-Station-Id in order to include the MAC address of the wireless device.

---

**Note:** Siemens-URL-Redirection is supported by MAC-based authentication.

---

## 6.6.2 Defining authentication for a VNS for Captive Portal

For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the non-authenticated filter. For more information, see [Section 6.9.2, “Defining non-authenticated filters”, on page 197](#). One of these destinations should be a server, either internal or external, which presents a Web login page — the Captive Portal. The wireless device user must input an ID and a password. This request for authentication is sent by the HiPath Wireless Controller to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the HiPath Wireless Controller implements policy and allows the appropriate network access.

Captive Portal authentication relies on a RADIUS server on the enterprise network. There are three mechanisms by which Captive Portal authentication can be carried out:

- **Internal Captive Portal** – The HiPath Wireless Controller displays the Captive Portal Web page, carries out the authentication, and implements policy.

- **External Captive Portal** – After an external server displays the Captive Portal Web page and carries out the authentication, the HiPath Wireless Controller implements policy.
- **External Captive Portal with internal authentication** – After an external server displays the Captive Portal Web page, the HiPath Wireless Controller carries out the authentication and implements policy.

#### To define authentication by Captive Portal:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to set up authentication by Captive Portal for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:
  - **Auth** – Use to define authentication servers.
  - **MAC** – Use to define servers for MAC-based authentication.
  - **Acct** – Use to define accounting servers.

4. Click **Auth**. The Authentication fields are displayed.
5. From the **RADIUS** drop-down list, click the server you want to use for Captive Portal authentication, and then click **Use**. The server's default information is displayed.

## Virtual Network configuration

### Authentication for a VNS

The RADIUS servers are defined on the **Global Settings** page. For more information, see Section 5.8, “VNS global settings”, on page 157.

The screenshot shows the Siemens HiPath Virtual Network Configuration interface. The main window is titled "CNL-209-AAA" and has tabs for Topology, RF, Auth & Acct (selected), RAD Policy, Filtering, Multicast, Privacy, and QoS Policy. The "Auth & Acct" tab is active, showing the RADIUS configuration. The "RADIUS" section includes a dropdown menu for the selected server (JASPER) and a "Use" button. Below it is a "Config'd Servers" list with "freeradius209" selected and "Up" and "Down" buttons. There are also "Reset to primary", "Test", and "View Summary" buttons. The "Auth \*" section has a checked "Use server for Authentication" checkbox. The "MAC" and "Acct" sections are visible. The "Auth" section includes fields for Port (1812), Total # of Tries (3), Timeout (5) seconds, NAS IP Address (172.29.30.1), NAS identifier (CNL-209-AAA), and NAS port type (Wireless IEEE 802.11). There is a checked "Set as primary server" checkbox. The "RADIUS Accounting" section has an "Interim Interval" of 30 minutes and a checkbox for "Collect Accounting Information of Wireless Controller". The "Incl. VSA Attb.:" section has checkboxes for AP's, VNS's, and SSID. The bottom status bar shows "Enterprise Software: V5 R1.10014.0 | Trading: Inactive" and "© Copyright. 2006-2008 Siemens AG. All Rights Reserved."

The selected server is no longer available in the **RADIUS** drop-down list.

The server name is now displayed in the list of configured servers, next to the **Up** and **Down** buttons, where it can be prioritized for RADIUS redundancy. The server can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk is displayed next to **Auth**, indicating that a server has been assigned.

6. In the **Port** box, type the port used to access the RADIUS server. The default is 1812.
7. In the **# of Retries** box, type the number of times the HiPath Wireless Controller will attempt to access the RADIUS server.
8. In the **Timeout** box, type the maximum time that a HiPath Wireless Controller will wait for a response from the RADIUS server before attempting again.
9. In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

10. In the **Auth. Type** drop-down list, click the authentication protocol to be used by the RADIUS server to authenticate the wireless device users. The authentication protocol applies to a VNS with Captive Portal authentication:

- **PAP** – Password Authentication Protocol
- **CHAP** – Challenge Handshake Authentication Protocol
- **MS-CHAP** – Windows-specific version of CHAP
- **MS-CHAP2** – Windows-specific version of CHAP, version 2

11. In the **Include VSA Attributes** section, click the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:

- **AP's**
- **VNS's**
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

12. If appropriate, select the **Reset to Primary** checkbox. This checkbox is visible when a RADIUS server has not yet been selected as a primary server, or if the server you are configuring has already been selected as the primary server, the **Reset to Primary** checkbox is selected.

RADIUS redundancy defines additional backup RADIUS servers that the system will attempt to communicate with in case a connection with the identified primary server fails. If connection to an active primary server fails, the system automatically attempts to connect to one of the alternate servers in sequence. If the system succeeds in registering with a defined alternate server, it becomes the active primary server, which is identified by the A on the list. You can subsequently reset or change the identification of the primary server by selecting the applicable **Reset to Primary** checkbox.

13. To save your changes, click **Save**.

---

**Note:** If you have already assigned a server to either MAC-based authentication or accounting, and you want to use it again for authentication, highlight its name in the list next to the **Up** and **Down** buttons and select the **Use server for Authentication** checkbox. The server's default information is displayed.

---

### 6.6.2.1 Defining the RADIUS server priority for RADIUS redundancy

If more than one server has been defined for any type of authentication, you can define the priority of the servers in the case of failover.

## Virtual Network configuration

### Authentication for a VNS

In the event of a failover of the main RADIUS server—if there is no response after the set number of retries—then the other servers in the list will be polled on a round-robin basis until a server responds.

If one of the other servers becomes the active server during a failover, when the new active server properties are displayed the **Set as primary server** checkbox is selected.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

#### To define the RADIUS server priority for RADIUS redundancy:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define the RADIUS server priority for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab.
4. From the drop-down list, click the servers group you want to prioritize:
  - Configured Servers
  - Authentication Servers
  - MAC Servers
  - Accounting Servers
5. In the server list, click the RADIUS server and then click **Up** or **Down** to arrange the order. The first server in the list is the active one.
6. To test the HiPath Wireless Controller's connection to all configured RADIUS servers, click **Test**. The Test RADIUS servers page displays the message transaction with the RADIUS server, which allows you to visually verify the state of the server connection and user authentication.

The RADIUS test is a test of connectivity to the RADIUS server, not of full RADIUS functionality. AAA VNSs use EAP over RADIUS for authentication. The HiPath Wireless Controller's EAP RADIUS connectivity test initiates an Access-Request, to which the RADIUS server will respond with a challenge. If the challenge is received then the test is deemed to have succeeded. If the challenge is not received then the test is deemed to have failed. In either case, the test ends at this point; for AAA VNSs, there is no need for a client password below.
7. In the **User ID** box, type the user ID that you know can be authenticated.
8. In the **Password** box, type the corresponding password.
9. Click **Test**. The **Test Result** page is displayed.

10. To view a summary of the RADIUS configuration, click **View Summary**. The **RADIUS summary** page is displayed.
11. To save your changes, click **Save**.

### 6.6.2.2 Configuring Captive Portal for internal or external authentication

There are three Captive Portal options:

- **No Captive Portal Support**
- **Internal Captive Portal** – Define the parameters of the internal Captive Portal page displayed by the HiPath Wireless Controller, and the authentication request from the HiPath Wireless Controller to the RADIUS server.
- **External Captive Portal** – Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the HiPath Wireless Controller request to a RADIUS server.

For more information, see Section 6.6.2.2, “To configure the Captive Portal settings for internal Captive Portal:”, on page 184 or Section 6.6.2.2, “To configure the Captive Portal Settings for external Captive Portal:”, on page 185.

**SIEMENS** Captive Portal Settings

**No Captive Portal Support**

**Internal Captive Portal**

Login Label:  Header and footer width is 790 pixels. Extra contents will be cropped out. Please keep them in reasonable heights.

Password Label:

Header URL:

Footer URL:

Message:

Replace Gateway IP with FQDN:

Default Redirection URL:

Specific Message URL:

Include Attributes	Header	Footer
AP Serial	<input type="checkbox"/>	<input type="checkbox"/>
AP Name	<input type="checkbox"/>	<input type="checkbox"/>
VNS Name	<input type="checkbox"/>	<input type="checkbox"/>
SSID	<input type="checkbox"/>	<input type="checkbox"/>
MAC Address	<input type="checkbox"/>	<input type="checkbox"/>

**Provide button for users:**

Logoff

Status check

**External Captive Portal**

HWC Connection:  :

External authentication server access. Port range: 32768 - 65535

Shared Secret:

Shared secret should be between 16 - 64 characters

Redirection URL:

Note: token=<integer\_val>&dest=<original\_target\_url> will be APPENDED to the redirection URL

## Virtual Network configuration

### Authentication for a VNS

#### To configure the Captive Portal settings for internal Captive Portal:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to configure the Captive Portal settings for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab.
4. Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** page is displayed.
5. Select the **Internal Captive Portal** option.
6. In the **Login Label** box, type the text that will appear as a label for the user login field.
7. In the **Password Label** box, type the text that will appear as a label for the user password field.
8. In the **Header URL** box, type the location of the file to be displayed in the Header portion of the Captive Portal page. This page can be customized to suit your organization, with logos or other graphics.

---

**Caution:** If you use logos or graphics, ensure that the graphics or logos are appropriately sized. Large graphics or logos may force the login section out of view.

---

9. In the **Footer URL** box, type the location of the file to be displayed in the Footer portion of the Captive Portal page.
10. In the **Message** box, type the message that will appear above the Login box to greet the user. For example, the message could explain why the Captive Portal page is appearing, and instructions for the user.
11. In the **Replace Gateway IP with FQDN** box, type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.
12. In the **Default Redirection URL** box, type the URL to which the wireless device user will be directed to after authentication.
13. In the **Specific Message URL** box, type the URL of a document that will be displayed in a text frame on the Captive Portal login page. This text frame can be used to display lengthier messages, such as terms and conditions of use for users who have not yet logged in.
14. In the right pane, select the appropriate checkboxes to include the following VSA Attributes in the message to the authentication server:
  - AP Serial number
  - AP Name



- VNS Name
  - SSID
  - MAC Address
15. In the right pane, select whether these VSA attributes apply to the header or footer of the Captive Portal page.

The selections influence what URL is returned in either section. For example, wireless users can be identified by which Wireless AP or which VNS they are associated with, and can be presented with a Captive Portal Web page that is customized for those identifiers.
  16. To provide users with a logoff button, select **Logoff**. The Logoff button launches a pop-up logoff page, allowing users to control their logoff.
  17. To provide users with a status check button, select **Status check**. The Status check button launches a pop-up window, which allows users to monitor session statistics such as system usage and time left in a session.
  18. To save your changes, click **Save**.
  19. To see how the Captive Portal page you have designed will look, click **View Sample Portal Page**.

---

**Caution:** In order for Captive Portal authentication to be successful, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the non-authenticated filter. For more information, see [Section 6.9.2, "Defining non-authenticated filters"](#), on page 197.

---

#### To configure the Captive Portal Settings for external Captive Portal:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to configure the Captive Portal settings for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab.
4. Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** page is displayed.
5. Select the **External Captive Portal** option.
6. In the **HWC Connection** drop-down list, click the IP address.
7. Type the port of the HiPath Wireless Controller.

## Virtual Network configuration

### Authentication for a VNS

If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the HiPath Wireless Controller to allow the HiPath Wireless Controller to continue with the RADIUS authentication and filtering.

In the **Shared Secret** box, type the password common to both the HiPath Wireless Controller and the external Web server if you want to encrypt the information passed between the HiPath Wireless Controller and the external Web server.

8. In the **Redirection URL** box, type the URL to which the wireless device user will be directed to after authentication.
9. To save your changes, click **Save**.

---

**Note:** You must add a filtering rule to the non-authenticated filter that allows access to the External Captive Portal site. For more information, see [Section 5.6, "Filtering for a VNS", on page 154](#).

---

### 6.6.3 Defining authentication for a VNS for AAA

If network assignment is AAA with 802.1x authentication, the wireless device must successfully complete the user authentication verification prior to being granted network access. This enforcement is performed by both the user's client and the AP. The wireless device's client utility must support 802.1x. The user's EAP packets request for network access along with login identification or a user profile is forwarded by the HiPath Wireless Controller to a RADIUS server.

---

**Note:** In order to use WPA with 802.1x authentication, network assignment must be AAA.

---

#### To define authentication by AAA (802.1x):

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to set up authentication by AAA for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:
  - **Auth** – Use to define authentication servers.
  - **MAC** – Use to define servers for MAC-based authentication.
  - **Acct** – Use to define accounting servers.

## Virtual Network configuration

### Authentication for a VNS

The screenshot displays the Siemens HiPath Virtual Network Configuration interface. The main window is titled "CNL-209-AAA" and has several tabs: Topology, RF, Auth & Acct (selected), RAD Policy, Filtering, Multicast, Privacy, and QoS Policy. The "Auth & Acct" tab is active, showing the RADIUS configuration. On the left, there is a "Virtual Networks" sidebar with a list of networks, including "CNL-209-AAA" which is highlighted. Below the sidebar are buttons for "Add subnet", "Rename subnet", and "Delete subnet". The RADIUS configuration area includes a "RADIUS" section with a "Config'd Servers" dropdown menu showing "freeradius209" selected. To the right of this dropdown are "Up" and "Down" buttons, and a "Reset to primary" button. Below these are "Test" and "View Summary" buttons. The "Auth \*" section is expanded, showing a "Use server for Authentication" checkbox which is checked. Below this are fields for "Port: 1812", "Total # of Tries: 3", "Timeout: 5 seconds", "NAS IP Address: 172.29.30.1", "NAS identifier: CNL-209-AAA", and "NAS port type: Wireless IEEE 802.11". There is also a "Set as primary server" checkbox which is checked. Below the "Auth \*" section is a "RADIUS Accounting" section with an "Interim Interval: 30 minutes" field and a "Collect Accounting Information of Wireless Controller" checkbox. At the bottom right of the configuration area are "Save" and "Cancel" buttons. The status bar at the bottom of the interface shows "[ HWC-206 | C2400 | 01 days, 07:32 ] User: admin Port status: M 1 2 3 4 F" and "Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved."

4. Click **Auth**. The Authentication fields are displayed.
5. From the **RADIUS** drop-down list, click the server you want to use for Captive Portal authentication, and then click **Use**. The server's default information is displayed.

The RADIUS servers are defined on the **Global Settings** page. For more information, see Section 5.8, "VNS global settings", on page 157.

## Virtual Network configuration

### Authentication for a VNS

The screenshot shows the Siemens HiPath Virtual Network Configuration interface. The main window is titled "CNL-209-AAA" and has tabs for "Topology", "RF", "Auth & Acct", "RAD Policy", "Filtering", "Multicast", "Privacy", and "QoS Policy". The "Auth & Acct" tab is selected. The "RADIUS" section is active, showing a "JASPER" server selected in a dropdown menu. Below this is a "Config'd Servers" list with "freeradius209" listed, and "Up" and "Down" buttons. There are also "Reset to primary", "Test", and "View Summary" buttons. The "Auth \*" section is checked, and "Use server for Authentication" is checked. The "MAC \*" and "Acct" sections are unchecked. The "Port" is set to 1812, "Total # of Tries" is 3, and "Timeout" is 5 seconds. The "NAS IP Address" is 172.29.30.1, and the "NAS identifier" is CNL-209-AAA. The "NAS port type" is "Wireless IEEE 802.11". The "Set as primary server" checkbox is checked. The "Incl. VSA Attrib.:" section has checkboxes for "AP's", "VNS's", and "SSID", all of which are unchecked. The "RADIUS Accounting" section has an "Interim Interval" of 30 minutes and a checkbox for "Collect Accounting Information of Wireless Controller" which is unchecked. At the bottom right, there are "Save" and "Cancel" buttons. The status bar at the bottom shows "Enterprise Software: V5 R1.10014.0 | Tracing: Inactive" and "© Copyright: 2006-2008 Siemens AG, All Rights Reserved."

The selected server is no longer available in the **RADIUS** drop-down list.

The server name is now displayed in the list of configured servers, next to the **Up** and **Down** buttons, where it can be prioritized for RADIUS redundancy. The server can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk is displayed next to **Auth**, indicating that a server has been assigned.

6. In the **Port** box, type the port used to access the RADIUS server. The default is 1812.
7. In the **# of Retries** box, type the number of times the HiPath Wireless Controller will attempt to access the RADIUS server.
8. In the **Timeout** box, type the maximum time that a HiPath Wireless Controller will wait for a response from the RADIUS server before attempting again.
9. In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.
10. In the **Include VSA Attributes** section, select the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:
  - **AP's**

- **VNS's**
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

11. If applicable, select the **Set as primary server** checkbox.

12. To save your changes, click **Save**.

---

**Note:** If you have already assigned a server to either MAC-based authentication or accounting, and you want to use it again for authentication, highlight its name in the list next to the **Up** and **Down** buttons and select the **Use server for Authentication** checkbox. The server's default information is displayed.

---

## 6.6.4 Defining MAC-based authentication for a VNS

MAC-based authentication enables network access to be restricted to specific devices by MAC address. The HiPath Wireless Controller queries a RADIUS server for a MAC address when a wireless client attempts to connect to the network.

MAC-based authentication can be set up on any type of VNS, in addition to the Captive Portal or AAA authentication. To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC (or a password defined by the administrator) for each user. Specifying a MAC address format and policy depends on which RADIUS server is being used.

If MAC-based authentication is to be used in conjunction with the 802.1x or Captive Portal authentication, an additional account with a real UserID and Password must also be set up on the RADIUS server.

MAC-based authentication responses may indicate to the HiPath Wireless Controller what VNS a user should be assigned to. Authentication (if enabled) can apply on every roam.

### To define MAC-based authentication for a VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to set up MAC-based authentication for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:
  - **Auth** – Use to define authentication servers.

## Virtual Network configuration

### Authentication for a VNS

- **MAC** – Use to define servers for MAC-based authentication.
  - **Acct** – Use to define accounting servers.
4. Click **MAC**. The MAC fields are displayed.
  5. From the **RADIUS** drop-down list, click the server you want to use for MAC authentication, and then click **Use**. The server's default information is displayed and a red asterisk is displayed next to **MAC**, indicating that a server has been assigned.

The RADIUS servers are defined on the **Global Settings** page. For more information, see Section 5.8, "VNS global settings", on page 157.

The screenshot displays the Siemens HiPath Virtual Network Configuration web interface. The main content area is titled "CNL-209-AAA" and shows the "Auth & Acct" configuration page. The "RADIUS" section is active, showing a dropdown menu with "JASPER" selected and a "Use" button. Below this, a "Config'd Servers" list shows "freeradius209" selected. To the right, the "Auth \*" section is expanded, showing "Use server for MAC Authorization" checked. The "MAC \*" section is also expanded, showing fields for "Port: 1812", "Total # of Tries: 3", "Timeout: 5 seconds", "NAS IP Address: 172.29.30.1", "NAS identifier: CNL-209-AAA", "Auth. type:" (dropdown), and "Password:" (text input with "Unmask" button). The "Acct" section is also visible. At the bottom, the "RADIUS Accounting" section shows "Interim Interval: 30 minutes" and a checkbox for "Collect Accounting Information of Wireless Controller". The interface includes a left sidebar with "Global Settings" and "Virtual Networks" lists, and a top navigation bar with "Home", "Logs & Traces", "Reports", "Wireless Controller", "Wireless APs", "VNS Configuration", "Mitigator", "Help", and "LOGOUT".

6. If applicable, to use a server that has already been used for another type of authentication or accounting, click the server you want to use for MAC authentication, and then select **User server for MAC Authentication**.
7. In the **Port** box, type the port used to access the RADIUS server. The default is 1812.
8. In the **# of Retries** box, type the number of times the HiPath Wireless Controller will attempt to access the RADIUS server.
9. In the **Timeout** box, type the maximum time, in seconds, that a HiPath Wireless Controller will wait for a response from the RADIUS server before attempting again.

10. In the **NAS IP Address** box, type the Network Access Server (NAS) IP address.
11. In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.
12. In the **Auth. Type** field, click the authentication protocol to be used by the RADIUS server to authenticate the wireless device users for a Captive Portal VNS.
13. In the **Password** box, type the password you want to use for MAC-based authentication requests. The password is forwarded by the HiPath Wireless Controller to the authentication server. If the **Password** box is left empty, the MAC address will act as the default password.  
  
Toggle between **Mask/Unmask** to view and hide the defined password.
14. If applicable, select **Set as primary server**.
15. To enable MAC-based authentication on roam, select the **MAC-based authentication on roam** checkbox.

---

**Note:** Only select this checkbox if you are using MAC based authentication and if you want your clients to be authorized every time they roam to another AP. If this feature is not enabled, and MAC-based authentication is in use, the client is authenticated only at the start of a session.

---

16. To save your changes, click **Save**.

## 6.7 Defining accounting methods for a VNS

The next step in configuring a VNS is to define the methods of accounting. Accounting tracks the activity of a wireless device users. There are two types of accounting available:

- **HiPath Wireless Controller accounting** – Enables the HiPath Wireless Controller to generate Call Data Records (CDRs) in a flat file on the HiPath Wireless Controller.
- **RADIUS accounting** – Enables the HiPath Wireless Controller to generate an accounting request packet with an accounting start record after successful login by the wireless device user, and an accounting stop record based on session termination. The HiPath Wireless Controller sends the accounting requests to a remote RADIUS server.

## Virtual Network configuration

### *Defining accounting methods for a VNS*

HiPath Wireless Controller accounting creates Call Data Records (CDRs) in a standard format of authenticated user sessions, such as start time and duration of session. The CDRs are stored in flat files that can be downloaded via the Command Line Interface (CLI).

If RADIUS accounting is enabled, a RADIUS accounting server needs to be specified.

#### **To define accounting methods for a VNS:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define accounting methods for. The **Topology** tab is displayed.
3. Click the **Auth & Acct** tab.
4. To enable HiPath Wireless Controller accounting, select **Collect Accounting Information of Wireless Controller**.
5. From the **RADIUS** drop-down list, click the server you want to use for RADIUS accounting, and then click **Use**. The server's default information is displayed and a red asterisk is displayed next to **Acct**, indicating that a server has been assigned.

The RADIUS servers are defined on the **Global Settings** page. For more information, see [Section 5.8, "VNS global settings"](#), on page 157.

6. Select **Use server for RADIUS Accounting**.
7. In the **Port** box, type the port used to access the RADIUS server. The default is 1812.
8. In the **# of Retries** box, type the number of times the HiPath Wireless Controller will attempt to access the RADIUS server.
9. In the **Timeout** box, type the maximum time that a HiPath Wireless Controller will wait for a response from the RADIUS server before attempting again.
10. In the **Interim Interval** box, type the time interval when accounting records are sent. Interim accounting records are sent if the interim time interval is reached before the session ends. The default is 60 minutes.
11. To save your changes, click **Save**.



## 6.8 Defining RADIUS filter policy for VNSs and VNS groups

The next step in configuring a VNS is to define the filter ID values for a VNS. These filter ID values must match those set up on the RADIUS servers.

---

**Note:** This configuration step is optional. If filter ID values are not defined, the system uses the default filter as the applicable filter group for authenticated users within a VNS. However, if more user-specific filter definitions are required, for example filters based on a user's department, then the filter ID configuration is used to overwrite the default assignment.

---

In addition to the filter ID values, you can also set up a group ID for a VNS with AAA authentication. You can set up a group within a VNS that relies on the RADIUS attribute Login-LAT-Group (RFC2865). For each group, you can define filtering rules to control access to the network.

If you define a group within an AAA VNS, the group (or child) definition acquires the same authentication and privacy parameters as the parent VNS. However, you need to define a different topology and filtering rules for this group.

All the filters are exposed. For the Assignment by SSID with no authentication, the filter that is applied to the client session is the default filter.

### **To define the filter ID values on a VNS:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define filter ID values for. The **Topology** tab is displayed.
3. Click the **RAD Policy** tab.

## Virtual Network configuration

### Configuring filtering rules for a VNS

4. In the **Filter ID Values** box, type the name of a group that you want to define specific filtering rules for to control network access.
5. Click the corresponding **Add** button. The filter ID value is displayed in the list. These filter ID values will appear in the **Filter ID** list on the **Filtering** tab. These filter ID values must match those set up for the filter ID attribute in the RADIUS server.
6. If applicable, repeat steps 4 and 5 to add additional filtering ID values.
7. In the **VNS Group Name** box, type the name of a VNS group you want to create and define within the selected parent VNS.
8. Click the corresponding **Add** button. The Group Name will appear as a child of the parent VNS in the left pane **Virtual Networks** list.
9. To your changes, click **Save**.

## 6.9 Configuring filtering rules for a VNS

The next step in configuring a VNS is to configure the filtering rules for a VNS.

In an AAA VNS, a non-authenticated filter is unnecessary because users have already been authenticated. When authentication is returned, the filter ID group filters are applied. For AAA, a VNS can have a sub-group with Login-LAT-group

ID that has its own filtering rules. If no filter ID matches are found, then the default filter is applied. VNS Policy is also applicable for Captive Portal and MAC-based authorization.

### **6.9.1 Filtering rules for an exception filter**

The exception filter provides a set of rules aimed at restricting the type of traffic that is delivered to the controller. By default, your system is shipped with a set of restrictive filtering rules that help control access through the interfaces to only absolutely necessary services.

By configuring to allow management on an interface, an additional set of rules is added to the shipped filter rules that provide access to the system's management configuration framework (SSH, HTTPS, SNMPAgent). Most of this functionality is handled directly behind the scenes by the system, rolling and un-rolling canned filters as the system's topology and defined access privileges for an interface change.

---

**Note:** An interface for which **Allow Management** is enabled, can be reached by any other interface. By default, **Allow Management** is disabled and shipped interface filters will only permit the interface to be visible directly from its own subnet.

---

The visible exception filters definitions, both in physical ports and VNS definitions, allow administrators to define a set of rules to be prepended to the system's dynamically updated exception filter protection rules. Rule evaluation is performed top to bottom, until an exact match is determined. Therefore, these user-defined rules are evaluated before the system's own generated rules. As such, these user-defined rules may inadvertently create security lapses in the system's protection mechanism or create a scenario that filters out packets that are required by the system.

---

**Note:** Use exception filters only if absolutely necessary. It is recommended to avoid defining general allow all or deny all rule definitions since those definitions can easily be too liberal or too restrictive to all types of traffic.

---

The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the filter rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number for the applicable service running on the controller's management plane.

The exception filter on an VNS applies only to the destination portion of the packet. Traffic to a specified IP address and IP port is either allowed or denied. Adding exception filtering rules allows network administrators to either tighten or

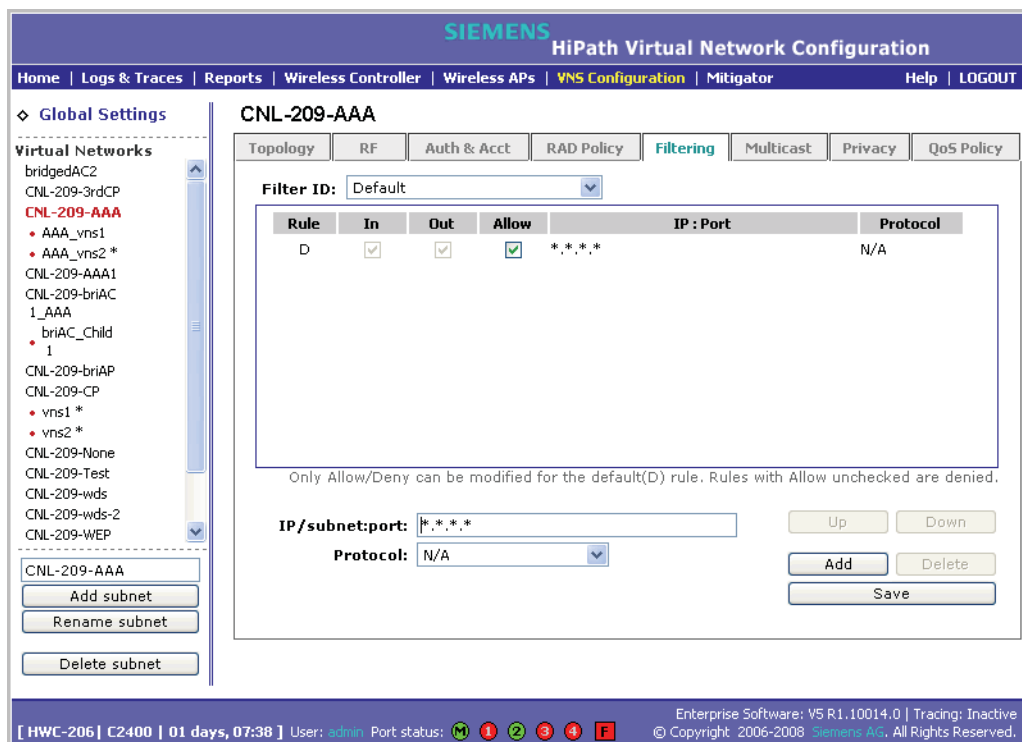
## Virtual Network configuration

### Configuring filtering rules for a VNS

relax the built-in filtering that automatically drops packets not specifically allowed by filtering rule definitions. The exception filtering rules can deny access in the event of a DoS attack, or can allow certain types of management traffic that would otherwise be denied. Typically, **Allow Management** is enabled

#### To define filtering rules for an exception filter:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define filter ID values for. The **Topology** tab is displayed.
3. Click the **Filtering** tab.
4. From the **Filter ID** drop-down list, click **Exception**.



5. For each filtering rule you are defining, do the following:
  - In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
  - In the **Protocol** drop-down list, click the applicable protocol. The default is N/A.
6. Define a rule to allow access to the default gateway for this VNS:
  - Select **IP/Port**.

- Type the default gateway IP address (VNS' IP address) that you defined on the **Topology** tab for this VNS.
7. Click **Add**. The information is displayed in the **Filter Rules** section of the tab.
  8. Click the new filter, then select the **Allow** checkbox applicable to the rule you defined.
  9. To edit the order of filters, click the filter, and then click the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.
  10. To save your changes, click **Save**.

---

**Note:** For external Captive Portal, you need to add an external server to a non-authentication filter.

---

## 6.9.2 Defining non-authenticated filters

Defining non-authenticated filters allows administrators to identify destinations to which a user is allowed to access without incurring an authentication redirection. Typically, the recommended default rule is to deny all. Administrators should define a rule set that will permit users to access essential services:

- DNS (IP of DNS server)
- Default Gateway (VNS Interface IP)

Any HTTP streams requested by the client for denied targets will be redirected to the specified location.

The non-authenticated filter should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. This filter should also allow network access to the IP address of the DNS server and to the network address—the gateway of the VNS. The VNS gateway is used as the IP for an internal Captive Portal page. An external Captive Portal will provide a specific IP definition of a server outside the HiPath Wireless Controller.

## Virtual Network configuration

### Configuring filtering rules for a VNS

Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach Websites other than those specifically allowed in the non-authenticated filter will be redirected to the allowed destinations. Most HTTP traffic outside of those defined in the non-authenticated filter will be redirected.

---

**Note:** Although non-authenticated filters definitions are used to assist in the redirection of HTTP traffic for restricted or denied destinations, the non-authenticated filter is not restricted to HTTP operations. The filter definition is general. Any traffic other than HTTP that the filter does not explicitly allow will be discarded by the controller.

---

The non-authenticated filter is applied by the HiPath Wireless Controller to sessions until they successfully complete authentication. The authentication procedure results in an adjustment to the user's applicable filters for access policy. The authentication procedure may result in the specification of a specific filter ID or the application of the default filter for the VNS.

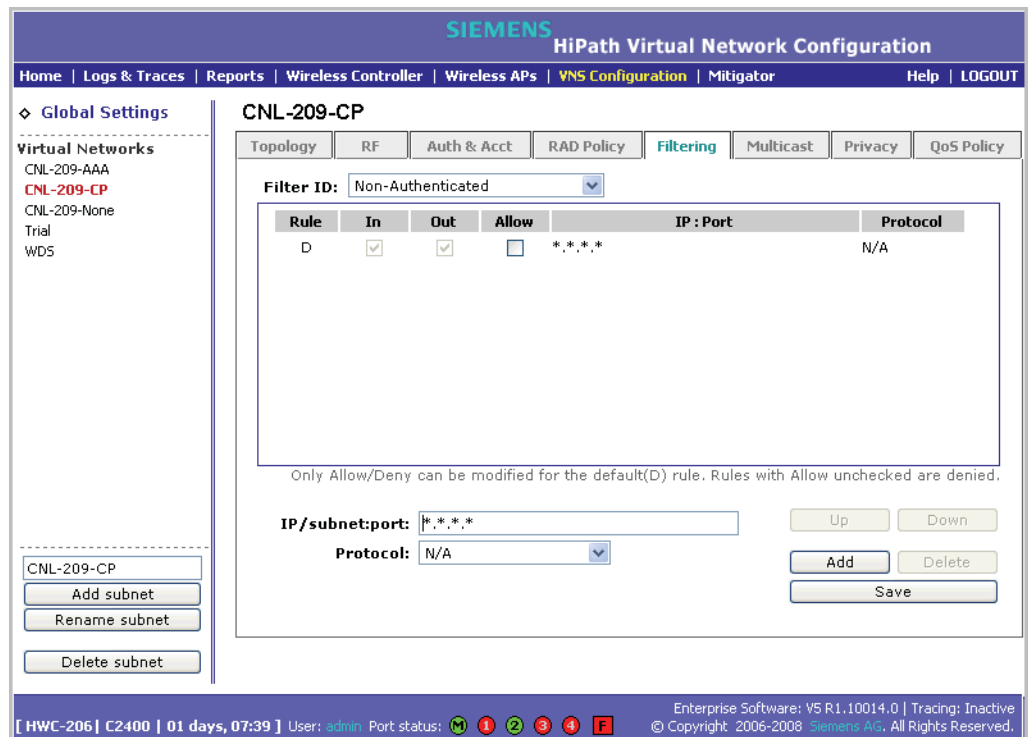
Typically, default filter ID access is less restrictive than a non-authenticated profile. It is the administrator's responsibility to define the correct set of access privileges.

#### To define filtering rules for a non-authenticated filter:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define filter ID values for. The **Topology** tab is displayed.
3. Click the **Filtering** tab.
4. From the **Filter ID** drop-down list, click **Non-Authenticated**.

## Virtual Network configuration

### Configuring filtering rules for a VNS



The **Filtering** tab automatically provides a Deny All rule already in place. Use this rule as the final rule in the non-authenticated filter for Captive Portal.

5. For each filtering rule you are defining, do the following:
  - In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
  - In the **Protocol** drop-down list, click the applicable protocol. The default is N/A.
6. For Captive Portal assignment, define a rule to allow access to the default gateway for this VNS:
  - Select **IP/Port**.
  - Type the default gateway IP address that you defined in the **Topology** tab for this VNS.
7. Click **Add**. The information is displayed in the **Filter Rules** section of the tab.
8. Click the new filter, then do the following:
  - If applicable, select **In** to refer to traffic from the wireless device that is trying to get on the network.
  - If applicable, select **Out** to refer to traffic from the network host that is trying to get to a wireless device.

## Virtual Network configuration

### Configuring filtering rules for a VNS

- Select the **Allow** checkbox applicable to the rule you defined.
9. To edit the order of filters, click the filter, and then click the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.
  10. To save your changes, click **Save**.

---

**Note:** Administrators must ensure that the non-authenticated filter allows access to the corresponding authentication server:

- **Internal Captive Portal** – IP address of the VNS interface
  - **External Captive Portal** – IP address of external Captive Portal server
- 

#### 6.9.2.1 Non-authenticated filter examples

A basic non-authenticated filter for internal Captive Portal should have three rules, in the following order:

In	Out	Allow	IP / Port	Description
x	x	x	IP address of default gateway (VNS Interface IP)	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		*.*.*.*	Deny everything else.

Table 15 Non-authenticated filter example A

---

**Note:** For external Captive Portal, an additional rule to Allow (in/out) access to the external Captive Portal authentication/Web server is required.

---

If you place URLs in the header and footer of the Captive Portal page, you must explicitly allow access to any URLs mentioned in the authentication's server page, such as:

- **Internal Captive Portal** – URLs referenced in a header or footer
- **External Captive Portal** – URLs mentioned in the page definition

Here is another example of a non-authenticated filter that adds two more filtering rules. The two additional rules do the following:

- Deny access to a specific IP address.
- Allows only HTTP traffic.



In	Out	Allow	IP / Port	Description
x	x	x	IP address of the default gateway	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as:0/24).
x	x	x	*.*.*.*:80	Allow all port 80 (HTTP) traffic.
x	x		*.*.*.*	Deny everything else.

*Table 16 Non-authenticated filter example B*

Once a wireless device user has logged in on the Captive Portal page, and has been authenticated by the RADIUS server, then the following filters will apply:

- **Filter ID** – If a filter ID associated with this user was returned by the authentication server.
- **Default filter** – If no matching filter ID was returned from the authentication server.

### 6.9.3 Filtering rules for a filter ID group

When the wireless device user provides the identification credentials, identification is sent by the HiPath Wireless Controller to the RADIUS server, or other authentication server, through a sequence of exchanges depending on the type of authentication protocol used.

When the server allows this request for authentication—the server sends an access-accept message, the RADIUS server may also send back to the HiPath Wireless Controller a filter ID attribute value associated with the user. For an AAA VNS, a Login-LAT-Group identifier for the user may also be returned. VNS Policy is also applicable for Captive Portal and MAC-based authorization.

If the filter ID attribute value (or Login-LAT-Group attribute value) from the RADIUS server matches a filter ID value that you have set up on the HiPath Wireless Controller, the HiPath Wireless Controller applies the filtering rules that you defined for that filter ID value to the wireless device user.

If no filter ID is returned by the authentication server, or no match is found on the HiPath Wireless Controller, the filtering rules in the default filter will apply to the wireless device user.

## Virtual Network configuration

### Configuring filtering rules for a VNS

#### To define filtering rules for a filter ID group:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define filtering rules for a filter ID group. The **Topology** tab is displayed.
3. Click the **Filtering** tab.
4. From the **Filter ID** drop-down list, click one of the names you defined in the **Filter ID Values** field on the **RAD Policy** tab. For example, select one of your organization's user groups, such as Sales, Engineering, Teacher, Guest, etc.

The **Filtering** tab automatically provides a Deny All rule already in place. This rule can be modified to Allow All, if appropriate to the network access needs for this VNS.

5. For each filtering rule you are defining, do the following:
  - In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
  - In the **Protocol** drop-down list, click the applicable protocol. The default is N/A.
6. Click **Add**. The information is displayed in the **Filter Rules** section of the tab.
7. Click the new filter, then do the following:

- If applicable, select **In** to refer to traffic from the wireless device that is trying to get on the network.
  - If applicable, select **Out** to refer to traffic from the network host that is trying to get to a wireless device.
  - Select the **Allow** checkbox applicable to the rule you defined.
8. To edit the order of filters, click the filter, and then click the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.
9. To save your changes, click **Save**.

### 6.9.3.1 Filtering rules by filter ID examples

Below are two examples of possible filtering rules for a filter ID. The first example disallows some specific access before allowing everything else.

In	Out	Allow	IP / Port	Description
x	x		*.*.*.:22-23	SSH and telnet sessions
x	x		[specific IP address, range]	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.*	Allow everything else

*Table 17 Filtering rules by filter ID example A*

The second example does the opposite of the first example. It allows some specific access and denies everything else.

In	Out	Allow	IP / Port	Description
x	x	x	[specific IP address, range]	Allow traffic to a specific IP address or address range.
x	x		*.*.*.*	Deny everything else.

*Table 18 Filtering rules by filter ID example B*

### 6.9.4 Filtering rules for a default filter

After authentication of the wireless device user, the default filter will apply only after:

- No match is found for the Exception filter rules.
- No filter ID attribute value is returned by the authentication server for this user.
- No match is found on the HiPath Wireless Controller for a filter ID value.

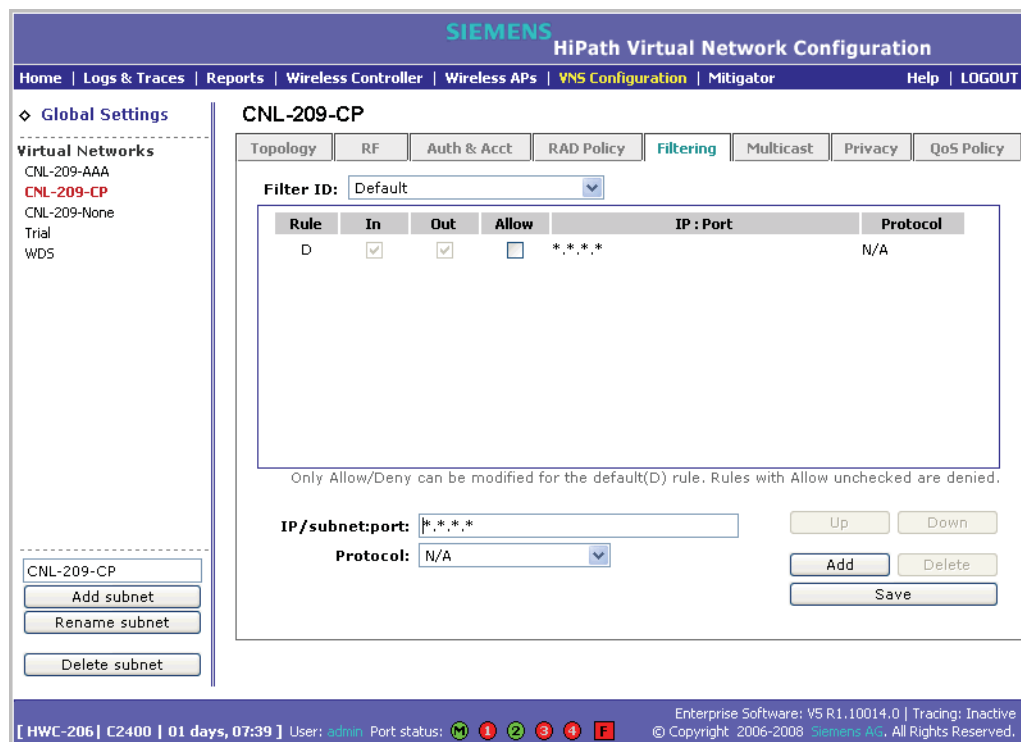
## Virtual Network configuration

### Configuring filtering rules for a VNS

The final rule in the default filter should be a catch-all rule for any traffic that did not match a filter. A final Allow All rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found. VNS Policy is also applicable for Captive Portal and MAC-based authorization.

#### To define the filtering rules for a default filter:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to define the filtering rules for a default filter. The **Topology** tab is displayed.
3. Click the **Filtering** tab.
4. From the **Filter ID** drop-down list, click **Default**.



The **Filtering** tab automatically provides a Deny All rule already in place. This rule can be modified to Allow All, if appropriate to the network access needs for this VNS.

#### 6.9.4.1 Default filter examples

The following are examples of filtering rules for a default filter:

In	Out	Allow	IP / Port	Description
x	x		Intranet IP, range	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to Web browsing
x	x		Intranet IP	Deny all access to a specific IP
x	x	x	*.*.*.*	Allow everything else

Table 19 Default filter example A

In	Out	Allow	IP / Port	Description
x			Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to Web browsing the host
	x		Intranet IP 10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as TELNET (port 23) or FTP (port 21)
x		x	Intranet IP 10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network
	x	x	Intranet IP 10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x		*.*.*.*	Deny everything else

Table 20 Default filter example B

### 6.9.4.2 Filtering rules for an AAA child group VNS

If you defined a child group for an AAA VNS, it will have the same authentication parameters and filter IDs as the parent VNS. However, you can define different filtering rules for the filters IDs in the child configuration from those in the parent configuration.

### 6.9.4.3 Filtering rules between two wireless devices

Traffic from two wireless devices that are on the same VNS and are connected to the same Wireless AP will pass through the HiPath Wireless Controller and therefore be subject to filtering policy. You can set up filtering rules that allow each wireless device access to the default gateway, but also prevent each device from communicating with each other.

Add the following two rules to a filter ID filter, before allowing everything else:

## Virtual Network configuration

### Enabling multicast for a VNS

In	Out	Allow	IP / Port	Description
x	x	x	[Intranet IP]	Allow access to the Gateway IP address of the VNS only
x	x		[Intranet IP, range]	Deny all access to the VNS subnet range (such as 0/24)
x	x	x	*.*.*.*	Allow everything else

Table 21 Rules between two wireless devices

## 6.10 Enabling multicast for a VNS

A mechanism that supports multicast traffic can be enabled as part of a VNS definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.

---

**Note:** To use the mobility feature with this VNS, you must select the **Enable Multicast Support** checkbox for the data port.

---

Define a list of multicast groups whose traffic is allowed to be forwarded to and from the VNS. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

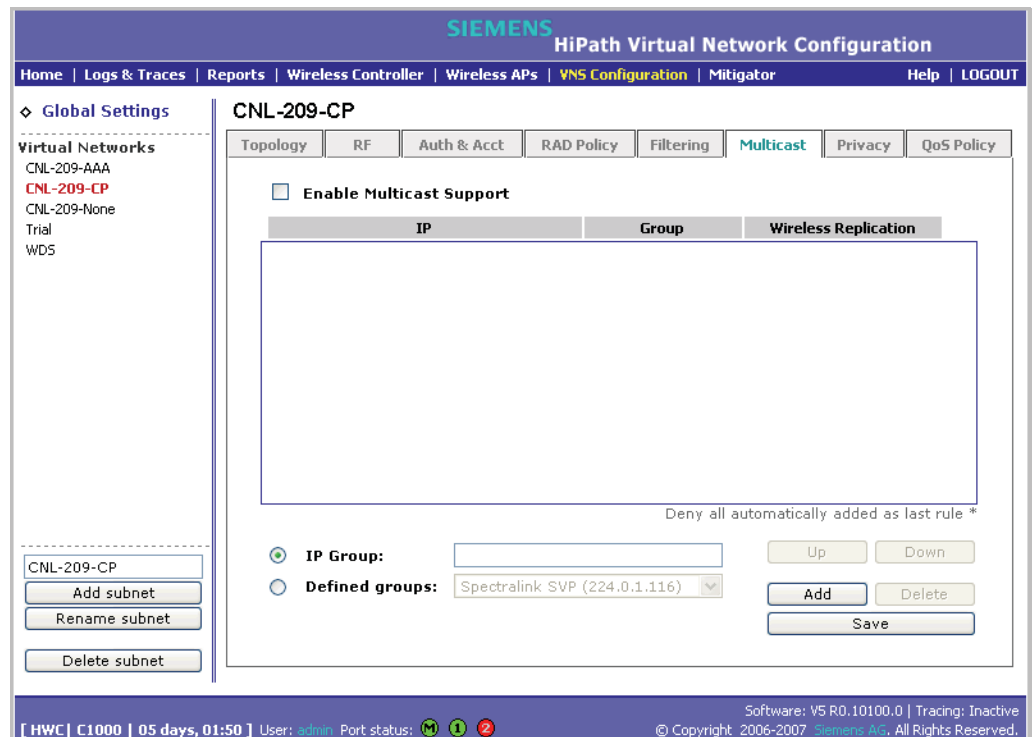
---

**Note:** Before enabling multicast filters and depending on the topology of the VNS, you may need to define which physical interface to use for multicast relay. Define the multicast port on the **IP Addresses** page. For more information, see [Section 3.2.4, "Setting up the data ports"](#), on page 42.

---

### To enable multicast for a VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to enable Multicast for. The **Topology** tab is displayed.
3. Click the **Multicast** tab.



4. To enable the multicast function, select **Enable Multicast Support**.
5. Define the multicast groups by selecting one of the radio buttons:
  - **IP Group** – Type the IP address range.
  - **Defined groups** – Click from the drop-down list.
6. Click **Add**. The group is added to the list above.
7. To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** checkbox.
8. To modify the priority of the multicast groups, click the group row, and then click the **Up** or **Down** buttons.
 

A Deny All rule is automatically added as the last rule, IP = \*.\*.\* and the **Wireless Replication** checkbox is not selected. This rule ensures that all other traffic is dropped.
9. To save your changes, click **Save**.

---

**Note:** The multicast packet size should not exceed 1450 bytes.

---

## 6.11 Configuring privacy for a VNS

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. The following section describes how the Privacy mechanism is handled for a Captive Portal VNS and an AAA VNS.

### 6.11.1 Privacy for a VNS for Captive Portal

For the Captive Portal VNS, there are three options for the privacy mechanism:

- **None**
- **Static Wired Equivalent Privacy (WEP)** – Keys for a selected VNS, so that it matches the WEP mechanism used on the rest of the network. Each radio can support up to eight SSIDs (16 SSIDs per AP). Each AP can participate in up to 50 VNSs. For each VNS, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.
- **Wi-Fi Protected Access (WPA) Pre-Shared key (PSK)** – Privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.

#### Wireless 802.11n APs and WPA authentication

If a VNS is configured to use WPA authentication, any Wireless 802.11n AP within that VNS will do the following:

- WPA v.1 – If WPA v.1 is enabled, the Wireless 802.11n AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 – If WPA v.2 is enabled, the Wireless 802.11n AP will do the following:
  - If WPA v.1 is enabled, the Wireless 802.11n AP will advertise TKIP as an available encryption protocol.
  - If WPA v.1 is disabled, the Wireless 802.11n AP will advertise the encryption cipher AES (Advanced Encryption Standard).

#### To configure privacy by static WEP for a Captive Portal VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to configure privacy by static WEP for a Captive Portal. The **Topology** tab is displayed.
3. Click the **Privacy** tab.
4. Select **Static Keys (WEP)**.



The screenshot shows the Siemens HiPath Virtual Network Configuration web interface. The main title is "SIEMENS HiPath Virtual Network Configuration". The navigation bar includes "Home", "Logs & Traces", "Reports", "Wireless Controller", "Wireless APs", "VNS Configuration", "Mitigator", "Help", and "LOGOUT".

The left sidebar shows "Global Settings" and "Virtual Networks". Under "Virtual Networks", there is a tree view with "aaa", "CNL-209-3rdCP", "CNL-209-AAA", "engineering", and "CNL-209-CP". Below this are buttons for "Add subnet", "Rename subnet", and "Delete subnet".

The main content area is titled "CNL-209-3rdCP" and has several tabs: "Topology", "RF", "Auth & Acct", "RAD Policy", "Filtering", "Multicast", "Privacy" (selected), and "QoS Policy".

Under the "Privacy" tab, there are three radio button options:
 

- None
- Static Keys (WEP)
  - WEP Key Length: 64 bit (dropdown menu)
  - Input Method:  Input Hex  Input String
  - WEP Key: [text input box] (format XX:XX:XX:XX:XX)
- WPA - PSK

At the bottom right of the configuration area are "Save" and "Cancel" buttons. The status bar at the bottom shows: "[ HWC-206 | C2400 | 01 days, 07:39 ] User: admin Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] [ F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright: 2006-2008 Siemens AG. All Rights Reserved."

5. From the **WEP Key Length** drop-down list, click the WEP encryption key length:
  - 64-bit
  - 128-bit
  - 152-bit
6. Select one of the following input methods:
  - **Input Hex** – If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.
  - **Input String** – If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The WEP Key box is automatically filled by the corresponding Hex code.
7. To save your changes, click **Save**.

#### To configure privacy by WPA-PSK for a Captive Portal VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.
3. Click the **Privacy** tab.

## Virtual Network configuration

### Configuring privacy for a VNS

4. Select **WPA-PSK**.
5. To enable WPA v1 encryption, select **WPA v.1**.
6. If WPA v.1 is enabled, click one of the following encryption types from the **Encryption** drop-down list:
  - **Auto** – The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
  - **TKIP only** – The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.
7. To enable WPA v2-type encryption, select **WPA v.2**.

The other options for this drop-down list are:

- **Auto** – If you click Auto, the Wireless AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
- **AES only** – If you click AES, the Wireless AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.

The screenshot displays the Siemens HiPath Virtual Network Configuration web interface. The main title is "SIEMENS HiPath Virtual Network Configuration". The navigation bar includes "Home", "Logs & Traces", "Reports", "Wireless Controller", "Wireless APs", "VNS Configuration", "Mitigator", "Help", and "LOGOUT". The left sidebar shows "Global Settings" and "Virtual Networks" with a tree view containing "aaa", "CNL-209-3rdCP", "CNL-209-AAA", "engineering", and "CNL-209-CP". The main content area is titled "CNL-209-3rdCP" and has tabs for "Topology", "RF", "Auth & Acct", "RAD Policy", "Filtering", "Multicast", "Privacy", and "QoS Policy". The "Privacy" tab is active, showing radio button options for "None", "Static Keys (WEP)", and "WPA - PSK". The "WPA - PSK" option is selected. Under "WPA - PSK", there are checkboxes for "WPA v.1" and "WPA v.2", both of which are checked. Each has an "Encryption" dropdown menu set to "Auto". There is also a checked checkbox for "Broadcast re-key interval" with a value of "3600" seconds. A "Pre-shared key" field is present with an "Unmask" button. At the bottom right of the form are "Save" and "Cancel" buttons. The footer contains system information: "[ HWC-206 | C2400 | 01 days, 07:39 ] User: admin Port status: [ icons ] Enterprise Software: V5 R1.10014.0 | Trading: Inactive © Copyright 2006-2008 Siemens AG. All Rights Reserved."

8. To enable re-keying after a time interval, select **Broadcast re-key interval**.  
If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.
9. In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.
10. In the **Pre-Shared Key** box, type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key.
11. To proofread your entry before saving the configuration, click **Unmask** to display the Pre-Shared Key. To mask the key, click **Mask**.
12. To save your changes, click **Save**.

## 6.11.2 Privacy for a VNS for AAA

For a VNS with authentication by 802.1x (AAA), there are four Privacy options:

- Static keys (WEP)
- Dynamic keys
- Wi-Fi Protected Access (WPA) version 1, with encryption by Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access (WPA) version 2, with encryption by Advanced Encryption Standard with Counter-Mode/CBC-MAC Protocol (AES-CCMP)

---

**Note:** In order to use WPA with 802.1x authentication, network assignment must be AAA.

---

### Wireless 802.11n APs and WPA authentication

If a VNS is configured to use WPA authentication, any Wireless 802.11n AP within that VNS will do the following:

- WPA v.1 – If WPA v.1 is enabled, the Wireless 802.11n AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 – If WPA v.2 is enabled, the Wireless 802.11n AP will do the following:
  - If WPA v.1 is enabled, the Wireless 802.11n AP will advertise TKIP as an available encryption protocol.

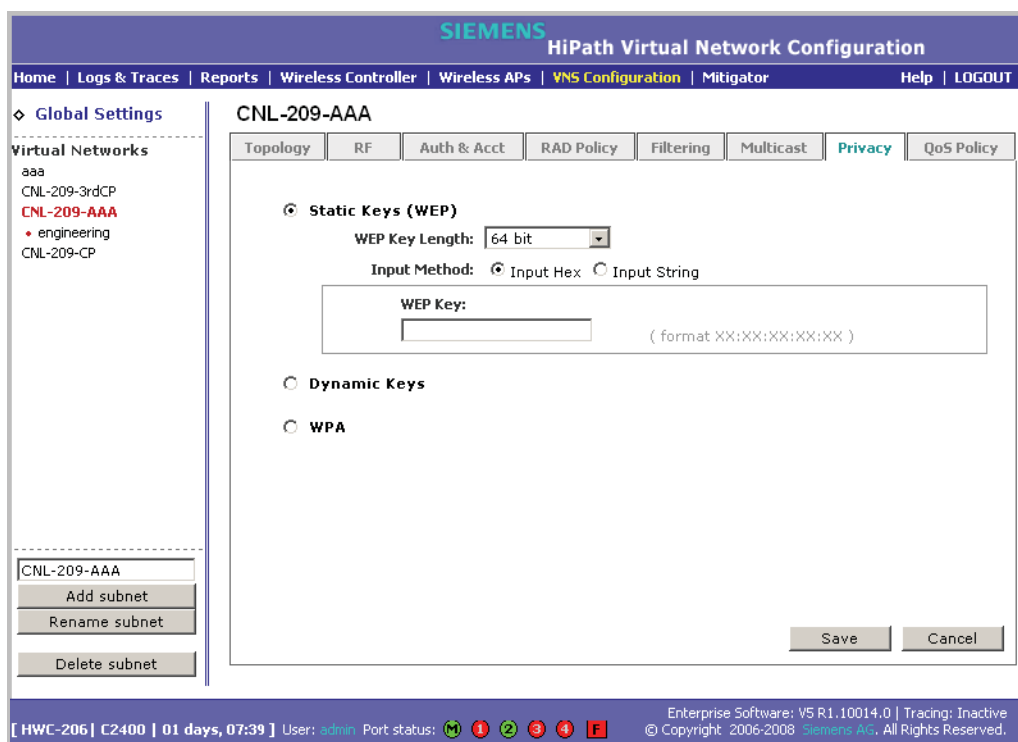
## Virtual Network configuration

### Configuring privacy for a VNS

- If WPA v.1 is disabled, the Wireless 802.11n AP will advertise the encryption cipher AES (Advanced Encryption Standard).

#### To set up static WEP privacy for an AAA VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the AAA VNS you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.
3. Click the **Privacy** tab.



4. Select **Static Keys (WEP)**.
5. From the **WEP Key Length** drop-down list, click the WEP encryption key length:
  - 64-bit
  - 128-bit
  - 152-bit
6. Select one of the following input methods:
  - **Input Hex** – If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.

- **Input String** – If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The WEP Key box is automatically filled by the corresponding Hex code.

7. To save your changes, click **Save**.

#### 6.11.2.1 Dynamic WEP privacy for an AAA VNS

The dynamic key WEP mechanism changes the key for each user and each session.

**To set up dynamic WEP privacy for a selected AAA VNS:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the AAA VNS you want to set up dynamic WEP privacy for. The **Topology** tab is displayed.
3. Click the **Privacy** tab.
4. Select **Dynamic Keys**.
5. To save your changes, click **Save**.

#### 6.11.2.2 Wi-Fi Protected Access (WPA v1 and WPA v2) Privacy for an AAA VNS

The VNS Privacy feature supports Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management.

The authentication portion of WPA for AAA is in Enterprise Mode:

- Specifies 802.1x with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet (unicast key) or after the specified re-key time interval (broadcast key) expires
- An extended WEP key length of 256-bits

## Virtual Network configuration

### Configuring privacy for a VNS

- An enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise
- A Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, which ensures that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

- A 128 bit key length, for the WPA2/802.11i implementation of AES
- Four stages that make up one round. Each round is iterated 10 times.
- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval expires.
- The Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include:
  - Counter mode (CTR) that achieves data encryption
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

The following is an overview of the WPA authentication and encryption process:

- **Step one** – The wireless device client associates with Wireless AP.
- **Step two** – Wireless AP blocks the client's network access while the authentication process is carried out (the HiPath Wireless Controller sends the authentication request to the RADIUS authentication server).
- **Step three** – The wireless client provides credentials that are forwarded by the HiPath Wireless Controller to the authentication server.
- **Step four** – If the wireless device client is not authenticated, the wireless client stays blocked from network access.
- **Step five** – If the wireless device client is authenticated, the HiPath Wireless Controller distributes encryption keys to the Wireless AP and the wireless client.
- **Step six** – The wireless device client gains network access via the Wireless AP, sending and receiving encrypted data. The traffic is controlled with permissions and policy applied by the HiPath Wireless Controller.

### 6.11.2.3 Key Management Options

Wi-Fi Protected Access (WPA v1 and WPA v2) Privacy offers you the following key management options:

- None
- Opportunistic Keying
- Pre-authentication
- Opportunistic Keying & Pre-auth

The following sections explain the key management options.

#### None

The wireless client device performs a complete 802.1X authentication each time it associates or tries to connect to a Wireless AP.

#### Opportunistic Keying

Opportunistic Keying or opportunistic key caching (OKC) enables the client devices to roam fast and securely from one Wireless AP to another in 802.1X authentication setup.

The client devices that run applications such as video streaming and VoIP require rapid reassociation during roaming. OKC helps such client devices by enabling them to rapidly reassociate with the Wireless APs. This avoids delays and gaps in transmission and thus helps in secure fast roaming (SFR).

---

**Note:** The client devices should support OKC to use the OKC feature in the HiPath WLAN.

---

#### Pre-authentication

Pre-authentication enables a client device to authenticate simultaneously with multiple Wireless APs in 802.1X authentication setup. When the client device roams from one Wireless AP to another, it does not have to perform the complete 802.1X authentication to reassociate with the new Wireless AP as it is already pre-authenticated with it. This reduces the reassociation time and thus helps in seamless roaming.

---

**Note:** The client devices should support pre-authentication to use the pre-authentication feature in HiPath WLAN.

---

## Virtual Network configuration

### Configuring privacy for a VNS

#### Opportunistic Keying & Pre-auth

Opportunistic Keying and Pre-auth options is meant for the device clients that support both the authentication processes. For example, the Microsoft-operated device clients support opportunistic keying by default, but they can be configured to support pre-authentication too.

#### To set up Wi-Fi Protected Access privacy (WPA) for an AAA VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the AAA VNS you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.
3. Click the **Privacy** tab.
4. Select **WPA**.

The screenshot displays the Siemens HiPath Virtual Network Configuration web interface. The top navigation bar includes 'Home', 'Logs & Traces', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar shows 'Global Settings' and a list of 'Virtual Networks' including 'CNL-209-AAA', 'CNL-209-CP', 'CNL-209-None', 'Trial', and 'WDS'. The main content area is titled 'CNL-209-AAA' and features several tabs: 'Topology', 'RF', 'Auth & Acct', 'RAD Policy', 'Filtering', 'Multicast', 'Privacy', and 'QoS Policy'. The 'Privacy' tab is active, showing three radio button options: 'Static Keys (WEP)', 'Dynamic Keys', and 'WPA'. The 'WPA' option is selected. Under 'WPA', there are two checked checkboxes: 'WPA v.1' and 'WPA v.2'. Each has an 'Encryption' dropdown menu set to 'Auto'. Below these is a 'Key Management Options' dropdown set to 'Pre-authentication'. A checked checkbox for 'Broadcast re-key interval' is set to '3600 seconds (30 - 86400 seconds)'. 'Save' and 'Cancel' buttons are at the bottom right. The footer contains system information: '[ HWC-206 | C2400 | 01 days, 07:39 ] User: admin Port status: [ M 1 2 3 4 F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright: 2006-2008 Siemens AG. All Rights Reserved.'

5. To enable WPA v1 encryption, select **WPA v.1**.

- From the **Encryption** drop-down list, select one of the following encryption types:



- **Auto** – The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
  - **TKIP only** – The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.
6. To enable WPA v2 encryption, select **WPA v.2**.
- From the **Encryption** drop-down list, click one of the following encryption types:
    - **Auto** – The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
    - **AES only** – The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.
  - From the **Key Management options**, click one of the following key management options:
    - **None** – The mobile units (client devices) performs a complete 802.1X authentication each time it associates or connects to a Wireless AP.
    - **Opportunistic Keying** – Enables secure fast roaming (SFR) of mobile units. For more information, see [Section 6.11.2.3, “Opportunistic Keying”](#), on page 215.
    - **Pre-authentication** – Enables seamless roaming. For more information, see [Section 6.11.2.3, “Pre-authentication”](#), on page 215.
    - **Opportunistic Keying & Pre-auth** – For more information, see [Section 6.11.2.3, “Opportunistic Keying & Pre-auth”](#), on page 216.
7. To enable re-keying after a time interval, select **Broadcast re-key interval**.  
If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.
8. In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.
9. To save your changes, click **Save**.

## Virtual Network configuration

### *Defining a VNS with no authentication*

## 6.12 Defining a VNS with no authentication

You can set up a VNS that will bypass all authentication mechanisms and run Controller, Access Points and Convergence Software with no authentication of a wireless device user.

A VNS with no authentication can still control network access using filtering rules. For more information on how to set up filtering rules that allow access only to specified IP addresses and ports, see [Section 6.9.2, “Defining non-authenticated filters”](#), on page 197.

### **To define a VNS with no authentication:**

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane, type a name that will identify the new VNS in the **Add subnet** box.
3. Click **Add subnet**. The name is displayed in the **Virtual Networks** list. The **Topology** tab is displayed.
4. From the **Assignment by** drop-down list, click **SSID**.
5. Configure the topology for this VNS, and then click **Save**. For more information, see [Section 6.3.1, “Configuring topology for a VNS for Captive Portal”](#), on page 165.

You must save your changes before moving to the next tab.

6. Click the **Auth & Acct** tab.
7. Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** window is displayed.
8. Select **No Captive Portal Support**. You must save your changes before moving to the next tab.
9. Click the **Filtering** tab.
10. Define a default filter that will control specific network access for any wireless device users on this VNS. For more information, see [Section 6.9, “Configuring filtering rules for a VNS”](#), on page 194.

These rules should be very restrictive and the final rule should be a Deny All rule. The non-authenticated filter for a VNS with no authentication will not have a Captive Portal page for login.

11. To save your changes, click **Save**.

## 6.13 Defining priority level and service class for VNS traffic

Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks are enabling the integration of internet telephony technology on wireless networks. Various issues including Quality-of-Service (QoS), call control, network capacity, and network architecture are factors in VoIP over 802.11 WLANs.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called isochronous data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn, in order to avoid data collisions. Regular traffic on a wireless network is an asynchronous process in which data streams are broken up by random intervals.

To reconcile the needs of isochronous data, mechanisms are added to the network that give voice data traffic or another traffic type priority over all other traffic, and allow for continuous transmission of data.

In order to provide better network traffic flow, the Controller, Access Points and Convergence Software provides advanced Quality of Service (QoS) management. These management techniques include:

- **WMM (Wi-Fi Multimedia)** – Enabled on individual VNSs, the standard provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service) or DSCP (Diffserv Codepoint)** – The ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header—this is referred to as Adaptive QoS.

### 6.13.1 Defining the service class for the VNS

Service class is determined by the combination of the following operations:

- The class of treatment given to a packet. For example, queuing or per hop behavior (PHB).
- The packet marking of the output packets (user traffic and/or transport).

Service class name (number)	Priority level
Network Control (7)	7 (highest priority)
Premium (Voice) (6)	6
Platinum (video) (5)	5
Gold (4)	4

## Virtual Network configuration

### Working with Quality of Service (QoS)

Service class name (number)	Priority level
Silver (3)	3
Bronze (2)	2
Best Effort (1)	1
Background (0)	0 (lowest priority)

Table 22 Service classes

The service class is equivalent to the 802.1D UP (user priority) with the exception that its scale is linear:

SC name	SC Value	802.1d UP	AC	Queue
Network Control	7	7	VO	VO or TVO
Premium (voice)	6	6	VO	VO or TVO
Platinum (video)	5	5	VI	VI
Gold	4	4	VI	VI
Silver	3	3	BE	BE
Bronze	2	0	BE	BE
Best Effort	1	2	BK	BK
Background	0	1	BK	BK

Table 23 Relationship between service class and 802.1D UP.

### 6.13.2 Configuring the priority override

Priority override allows you to define the desired priority level. Priority override can be used with any combination, as shown in Table 24. You can user is allowed to configure the service class (L2 override) and the DSCP values (L3 override values).

When **Priority Override** is enabled, the configured service class overrides the queue selection in the downlink direction, the 802.1P UP for the VLAN tagged Ethernet packets, and the UP for the wireless QoS packets (WMM or 802.11e) according to the mapping in Table 23. If **Priority Override** is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

## 6.14 Working with Quality of Service (QoS)

QoS policy is configured for each VNS and applies to routed, bridged at AP, and bridged at controller VNSs.

Each VNS has a configurable policy for the QoS characteristics of the VNS. For every user associated with the VNS there will be a different behavior on the wireless traffic.

---

**Note:** Active QoS is only applied on the wireless/802.11 domain, not on the wired domain.

---

### 6.14.1 QoS modes

You can enable the following QoS modes for a VNS:

- **Legacy** – If enabled, the AP will classify and prioritize the downlink traffic for all clients according to the same rules used for the WMM and 802.11e.
- **WMM** – If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.
- **802.11e** – If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic.
- **Turbo Voice** – If any of the above QoS modes are enabled, the Turbo Voice mode is available. If enabled, all the downlink traffic that is classified to the Voice (VO) AC and belongs to that VNS is transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. The TVO queue is tailored in terms of contention parameters and number of retries to maximize voice quality and voice capacity.

---

**Note:** The HiPath Wireless 802.11n supports only the WMM mode.

---

All combinations of the three modes are valid. The following table summarizes all possible combinations:

Configuration	Legacy mode	x		x		x		x
	WMM mode		x	x			x	x
	802.11e mode				x	x	x	x
Traffic that is classified and prioritized	To legacy client	x		x		x		x
	From legacy client							
	To WMM client	x	x	x		x	x	x
	From WMM client		x	x			x	x
	To 802.11e client	x		x	x	x	x	x
	From 802.11e client				x	x	x	x

## Virtual Network configuration

### Working with Quality of Service (QoS)

Table 24 QoS mode combinations

The APs are capable of supporting 5 queues. The queues are implemented per radio. For example, 5 queues per radio. The queues are:

Queue Name	Purpose
AC_VO	Voice
AC_VI	Video
AC_BK	Background
AC_BE	Best Effort
AC_TVO	Turbo Voice

Table 25 Queues

The HiPath Wireless Controller supports the definition of 8 levels of user priority (UP). These priority levels are mapped at the AP to the best appropriate access class. Of the 8 levels of user priority, 6 are considered low priority levels and 2 are considered high priority levels.

WMM clients have the same 5 AC queues. WMM clients will classify the traffic and use these queues when they are associated with a WMM-enabled AP. WMM clients will behave like non-WMM clients—map all traffic to the Best Effort (BE) queue—when not associated with WMM-enabled AP.

The prioritization of the traffic on the downstream (for example, from wired to wireless) and on the upstream (for example, from wireless to wired) is dictated by the configuration of the VNS and the QoS tagging within the packets, as set by the wireless devices and the host devices on the wired network.

Both Layer 3 tagging (DSCP) and Layer 2 (802.1d) tagging are supported, and the mapping is conformant with the WMM specification. If both L2 and L3 priority tags are available, then both are taken into account and the chosen AC is the highest resulting from L2 and L3. If only one of the priority tags is present, it is used to select the queue. If none is present, the default queue AC\_BE is chosen.

**Note:** If the wireless packets to be transmitted must include the L2 priority (send to a WMM client from a WMM-enabled AP), the outbound L2 priority is copied from the inbound L2 priority if available, or it is inferred from the L3 priority using the above table if the L2 inbound priority is missing.

VNS type	Packet Source	Packet type	L2	L3
Tunneled	Wired	Untagged	No	Yes
Branch	Wired	VLAN tagged	Yes	Yes
Branch	Wired	Untagged	No	Yes
Branch or Tunneled	Wireless	WMM	Yes	Yes

VNS type	Packet Source	Packet type	L2	L3
Branch or Tunneled	Wireless	non-WMM	No	Yes

*Table 26 Traffic prioritization*

## 6.15 Configuring the QoS policy on a VNS

The following is an overview of the steps involved in configuring the QoS on a VNS.

### Step one – Define the QoS mode to employ on the VNS:

- **Legacy** – Enables DL (downlink) classification for all clients
- **WMM:**
  - Enables WMM support
  - Enables DL classification for WMM clients
  - Enables UL (uplink) classification in WMM clients
- **802.11e:**
  - Enables 802.11e support
  - Enables DL classification for 802.11e clients
  - Enables UL classification in 802.11e clients

WMM and 802.11e are similar but, they use different signaling (same as WPA and WPA2).

### Step two – Enabling Turbo Voice:

- Ensures VNS is optimized for voice performance and capacity
- Can be enabled or disabled on individual VNSs
  - If Turbo Voice is enabled, together with QoS modes **Legacy**, **WMM**, or **802.11e**, DL voice traffic is sent via Turbo Voice queue instead of voice queue. A separate turbo voice queue allows for some VNSs to use the Turbo Voice parameters for voice traffic, while other VNSs use the voice parameters for voice traffic.
  - If WMM mode is also enabled, WMM clients use Turbo Voice-like contention parameters for UL voice traffic.
  - If 802.11e mode is also enabled, 802.11e clients use Turbo Voice-like contention parameters for UL voice traffic.

## Virtual Network configuration

### Configuring the QoS policy on a VNS

#### Step 3 – Defining the DSCP and service class classifications:

All 64 DSCP code-points are supported. The IETF defined codes are listed by name and code. Un-defined codes are listed by code. The following is the default DSCP service class classification:

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS0/DE	2/0	AF11	2/0	AF33	4/4
CS1	0/1	AF12	2/0	AF41	5/5
CS2	1/2	AF13	2/0	AF42	5/5
CS3	3/3	AF21	3/3	AF43	5/5
CS4	4/4	AF22	3/3	EF	6/6
CS5	5/5	AF23	3/3	Others	0/1
CS6	6/6	AF31	4/4		
CS7	7/7	AF32	4/4		

#### Step 4 – Enable Priority override:

- click the applicable service class and implicitly desired UP
  - Updates UP in user packet
  - Updates UP for WASSP frame (if field exists) sent by AP
- Select the desired DSCP
  - Updates DSCP for WASSP frames sent by AP
  - Does not change DSCP in user packet

#### Step 5 – Configure the advanced wireless QoS:

- Enable the **Unscheduled Automatic Power Save Delivery (U-APSD)** feature
- Works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled

#### Step 5 – Configure Global Admission Control:

- Enable admission control. Admission control protects admitted traffic against new bandwidth demands.
- Available for Voice and Video.

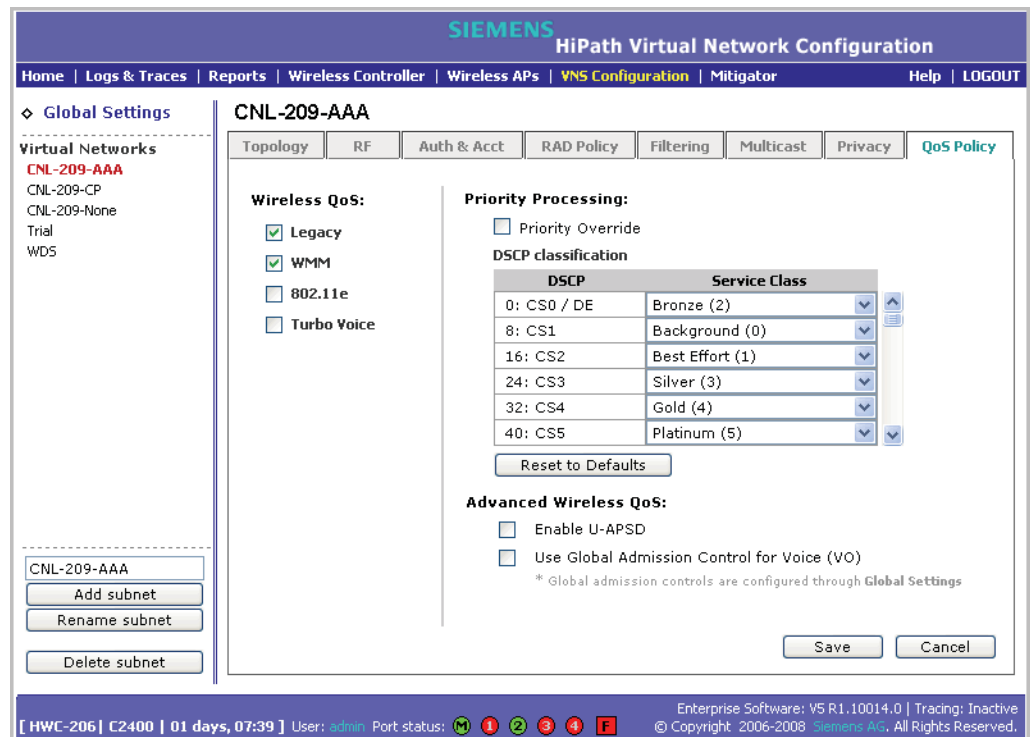
#### To configure QoS Policy on a VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the VNS you want to configure for QoS.
3. Click the **QoS Policy** tab.



## Virtual Network configuration

### Configuring the QoS policy on a VNS



#### 4. From the **Wireless QoS** list, do the following:

- **Legacy** – Select if your VNS will support legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic. If selected, the Turbo Voice option is displayed.
- **WMM** – Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all WMM clients. Note that WMM clients will also classify and prioritize the uplink traffic. WMM is part of the 802.11e standard for QoS. If selected, the **Turbo Voice** and the **Advanced Wireless QoS** options are displayed.
- **802.11e** – Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic. If selected, the **Turbo Voice** and the **Advanced Wireless QoS** options are displayed:
- **Turbo Voice** – Select to enable all downlink traffic that is classified to the Voice (VO) AC and belongs to that VNS to be transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. When **Turbo Voice** is enabled together with **WMM** or **802.11e**, the WMM

## Virtual Network configuration

### Configuring the QoS policy on a VNS

and/or 802.11e clients in that VNS are instructed by the AP to transmit all traffic classified to VO AC with special contention parameters tailored to maximize voice performance and capacity.

---

**Note:** The HiPath Wireless 802.11n supports only the **WMM** QoS mode.

---

5. To define the service class and DSCP marking for the VNS, select the **Priority Override** checkbox. For each DSCP you can click one of the eight service classes.
  - **Service class** – From the drop-down list, click the appropriate priority level:
    - Network control (7) – The highest priority level.
    - Premium (Voice) (6)
    - Platinum (5)
    - Gold (4)
    - Silver (3)
    - Bronze (2)
    - Best Effort (1)
    - Background (0) – The lowest priority level
  - **DSCP marking** – From the drop-down list, click the DSCP value used to tag the IP header of the encapsulated packets.

---

**Note:** The HiPath Wireless 802.11n does not support the **Priority Override** feature.

---

6. If you want to assign a service class to each DSCP marking, clear the **Priority Override** checkbox and define the DSCP service class priorities in the DSCP classification table.

When **Priority Override** is enabled, the configured service class overrides queue selection in the downlink direction, the 802.1P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority. If **Priority Override** is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

7. The **Advanced Wireless QoS** options are only displayed if the WMM or 802.11e checkboxes are selected:

- **Enable U-APSD** – Select to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature. This feature can be used by mobile devices to efficiently sustain one or more real-time streams while being in power-save mode. This feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.
- **Use Global Admission Control for Voice (VO)** – Select to enable admission control for Voice. With admission control, clients are forced to request admission in order to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands.
- **Use Global Admission Control for Video (VI)** – This feature is only available if admission control is enabled for Voice. Select to enable admission control for Video. With admission control, clients are forced to request admission in order to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands.

---

**Note:** The HiPath Wireless 802.11n AP does not support the **Advanced Wireless QoS** features.

---

8. To save your changes, click **Save**.

## 6.16 Bridging traffic locally

A VNS must first be setup before traffic can be bridged locally. For more information, see [Chapter 5, "Virtual Network Services"](#).

### To bridge traffic locally:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane, type a name that will identify the new VNS in the **Add subnet** box.
3. Click **Add subnet**. The name is displayed in the **Virtual Networks** list. The **Topology** tab is displayed.
4. In the **VNS Mode** drop-down list, click **Bridge Traffic Locally at AP** to enable branch office mode.
5. To define the VLAN Setting, select one of the following:
  - **Tagged**
  - **Untagged**

## Virtual Network configuration

### Bridging traffic locally

If you select **Tagged**, type the VLAN ID in the **VLAN ID** box.

**Note:** The VLAN IDs are assigned by the branch office network administrator. The AP will operate correctly if you set the VLAN ID corresponding to the VLAN ID that was setup in the LAN.

Configuring two untagged branch VNSs to the same AP on different radios is permitted. This is similar to having two untagged branch VNSs with the same VLAN ID assigned to the same AP on different radios. In both cases, the AP will connect the two VNSs. That type of configuration can be viewed as a single VNS/VLAN with different SSIDs on different radios.

An effective scenario of the configuration described above, in which the same subnet is used with different SSIDs on radio a and b/g, is when this configuration is defined consistently on all APs. It would allow dual band a+b/g clients to associate to one of the radios by specifying the correct SSID. This is particularly effective with Microsoft clients that do not allow defining a preferred radio.

6. To save your changes, click **Save**.

**Note:** In previous releases, an entire AP had to be put into branch mode. In the current release, an individual VNS can be put into bridging mode. An AP can have bridged and non-bridged VNSs.

If it has more than one branch mode VNS, only one bridged VNS can be

untagged per AP per radio. The other branch mode VNSs need to have unique VLAN ID. You must have VLAN aware L2 switches to support this feature.

---

**Note:** When a VNS is setup for bridged mode, it cannot be switched to tunneled mode. The administrator must delete and re-add the VNS.

---

## 6.17 Wireless Distribution System

A Wireless Distribution System (WDS) enables you to expand the wireless network by interconnecting the Wireless APs through wireless links in addition to the traditional method of interconnecting Wireless APs via a wired network.

---

**Note:** The HiPath Wireless 802.11n AP and the Scalance AP W788-2 do not support WDS.

---

A WDS deployment is ideally suited for locations, where installing ethernet cabling is too expensive, or physically impossible.

The WDS can be deployed in three configurations:

- Simple WDS Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

### 6.17.1 Simple WDS configuration

In a typical configuration, the Wireless APs are connected to the distribution system via an Ethernet network, which provides connectivity to the HiPath Wireless Controller.

However, when a Wireless AP is installed in a remote location and can't be wired to the distribution system, an intermediate Wireless AP is connected to the distribution system via the Ethernet link. This intermediate Wireless AP forwards and receives the user traffic from the remote Wireless AP over a radio link.

The intermediate Wireless AP that is connected to the distribution system via the Ethernet network is called Root AP, and the Wireless AP that is remotely located is called the Satellite AP.

The following figure illustrates the Simple WDS configuration:

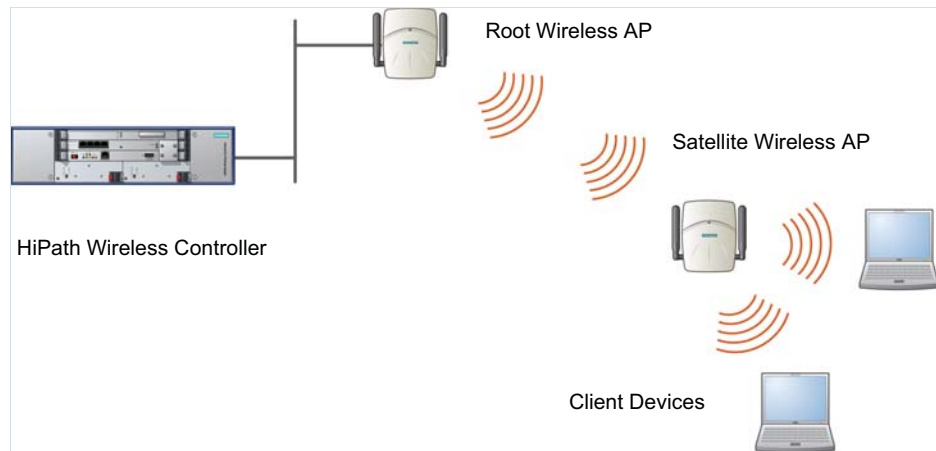


Figure 10 Simple WDS configuration

### 6.17.2 Wireless Repeater configuration

In Wireless Repeater configuration, a Repeater Wireless AP is installed between the Root Wireless AP and the Satellite Wireless AP. The Repeater Wireless AP relays the user traffic between the Root Wireless AP and the Satellite Wireless AP. This increases the WLAN range.

The following figure illustrates the Wireless Repeater configuration:

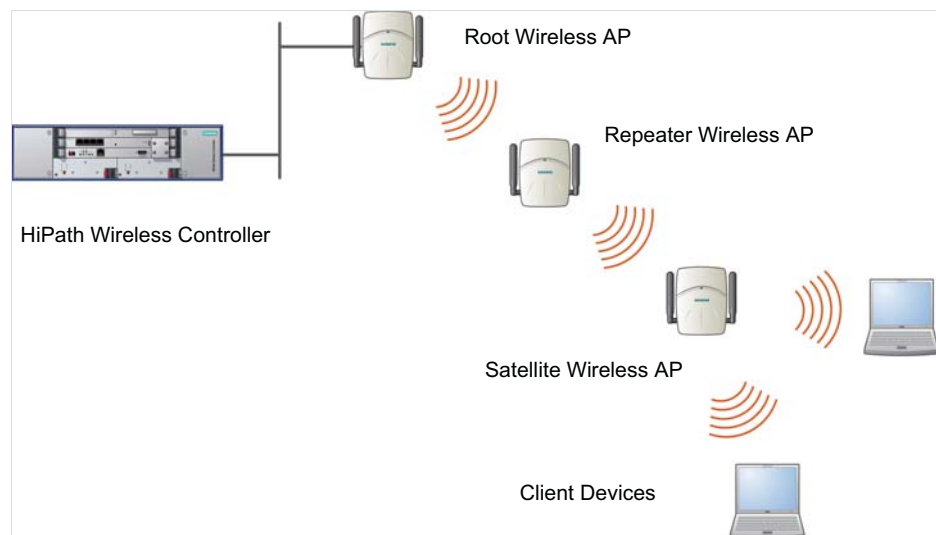


Figure 11 Wireless Repeater configuration

---

**Note:** The number of Repeater hops that you can deploy in a Wireless Repeater configuration is restricted to three. There should be no more than two Repeater Wireless APs between the Satellite AP and the Root AP.

---

### 6.17.3 Wireless Bridge configuration

In Wireless Bridge configuration, the traffic between two Wireless APs that are connected to two separate wired LAN segments is bridged via WDS link. You may also install a Repeater Wireless AP between the two Wireless APs connected to two separate LAN segments.

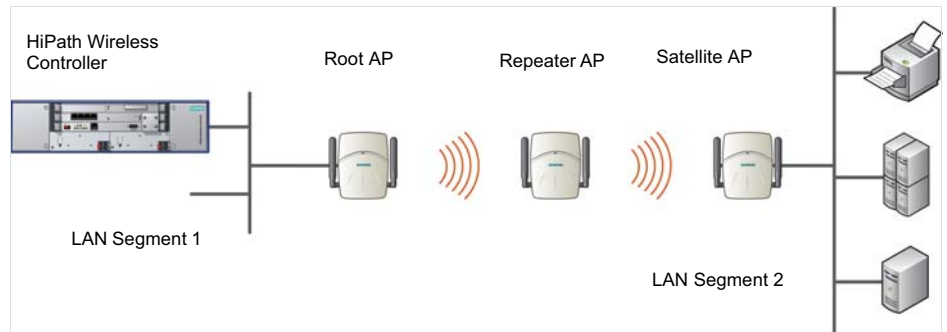


Figure 12 Wireless Bridge configuration

When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Satellite AP is connected to the wired LAN.

### 6.17.4 Examples of deployment

The following illustration depicts a few examples of WDS deployment.

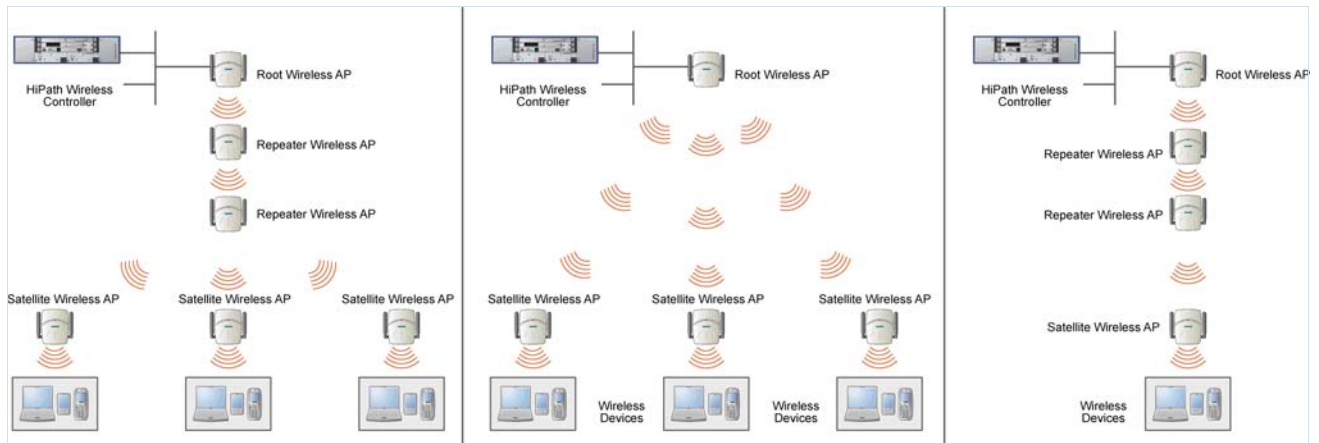


Figure 13 Examples of WDS deployment

### 6.17.5 WDS VNS

In a traditional HiPath WLAN deployment, each radio of the Wireless AP can interact with the client devices on a maximum of eight network VNSs.

## Virtual Network configuration

### Wireless Distribution System

In WDS deployment, one of the radios of every WDS Wireless AP establishes a WDS link on an exclusive VNS. The WDS Wireless AP is therefore limited to seven network VNSs on the WDS radio. The other radio can interact with the client-devices on a maximum of eight VNSs.

---

**Note:** The Root Wireless AP and the Repeater Wireless APs can also be configured to interact with the client-devices. For more information, see [Section 6.17.7.3, “Assigning the Satellite Wireless APs’ radios to the network VNSs”](#), on page 246.

---

The VNS on which the Wireless APs establish the WDS link is called the WDS VNS.

A WDS can be setup either by using either a single WDS VNS or multiple WDS VNSs. The following figures illustrate the point.

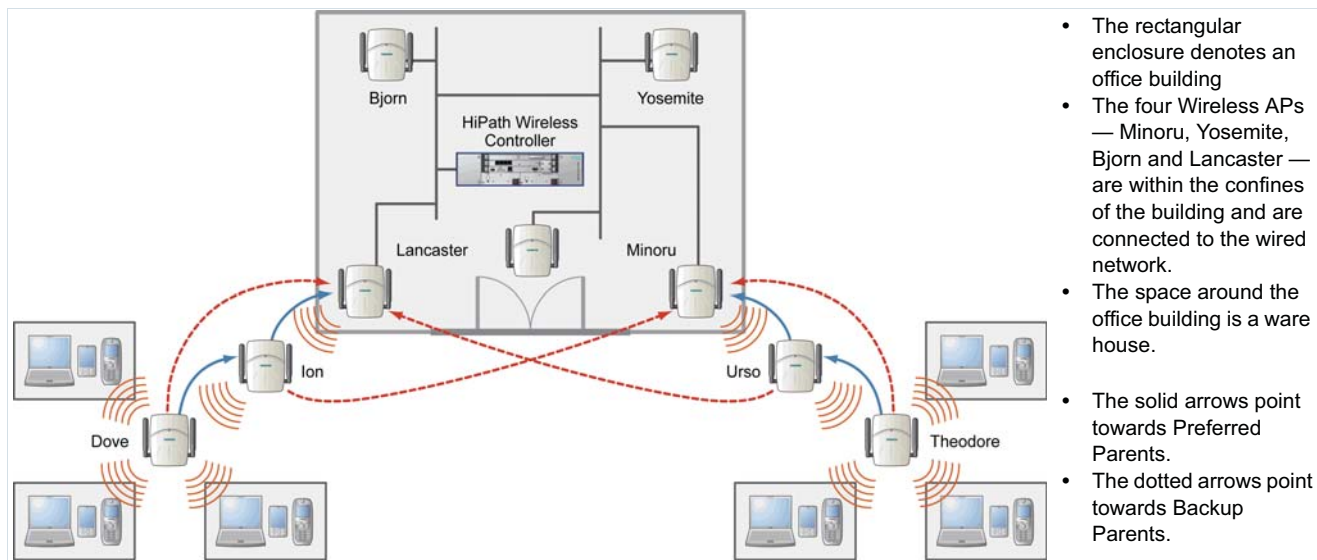


Figure 14 Deployment Example

### WDS setup with a single WDS VNS

Deploying the WDS for the above example using a single WDS VNS results in the following structure.



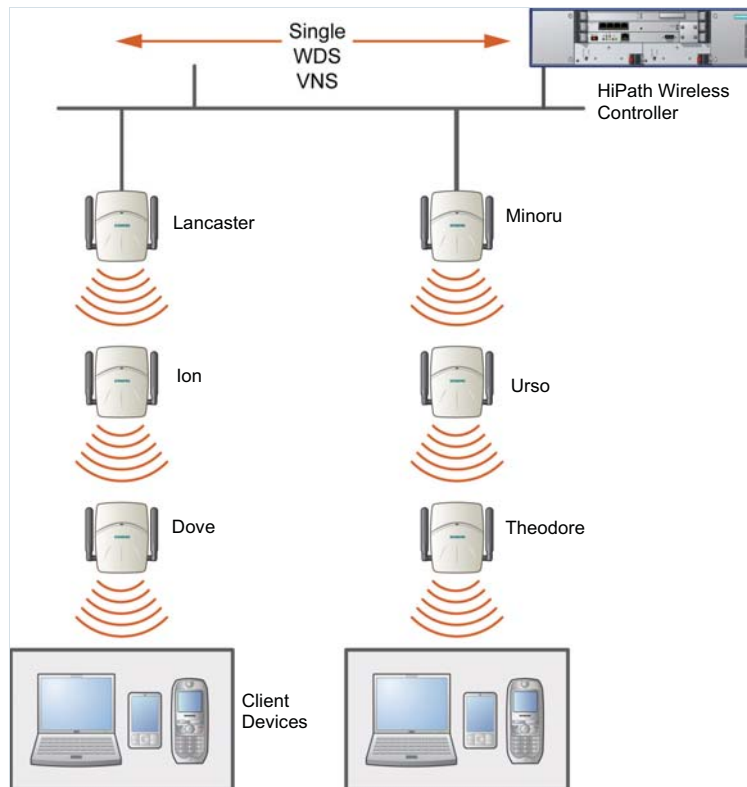


Figure 15 WDS setup with a single WDS VNS

The tree will operate as a single WDS entity. It will have a single WDS SSID and a single pre-shared key for WDS links. This tree will have multiple roots. For more information, see [Section 6.17.6.3, “Multi-root WDS topology”](#), on page 236.

### WDS setup with multiple WDS VNSs

You can also deploy the same WDS in [Figure 14](#) using two WDS VNSs. The Two WDS VNSs will create two independent WDS trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

## Virtual Network configuration

### Wireless Distribution System

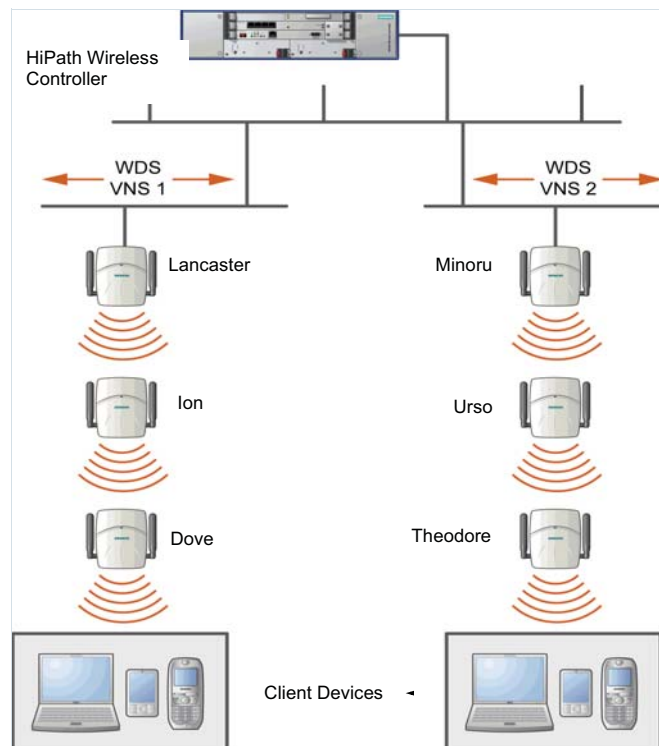


Figure 16 WDS setup with multiple WDS VNSs

### 6.17.6 Key features of WDS

Some key features of WDS are:

- Tree-like topology
- Radio Channels
- Multi-root WDS topology
- Automatic discovery of parent and backup parent Wireless APs
- Link security

#### 6.17.6.1 Tree-like topology

The Wireless APs in WDS configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Root Wireless AP being the tree root, and the Satellite Wireless AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The Wireless AP that provides the WDS service to the other Wireless APs in the downstream direction is a parent. The Wireless APs that establish a link with the Wireless AP in the upstream direction for WDS service are children.

---

**Note:** If a parent Wireless AP fails or stops to act a parent, the children Wireless APs will attempt to discover their backup parents. If the backup parents are not defined, the children Wireless APs will be left stranded.

---

The following figure illustrates the parent-child relationship between the nodes in a WDS topology.

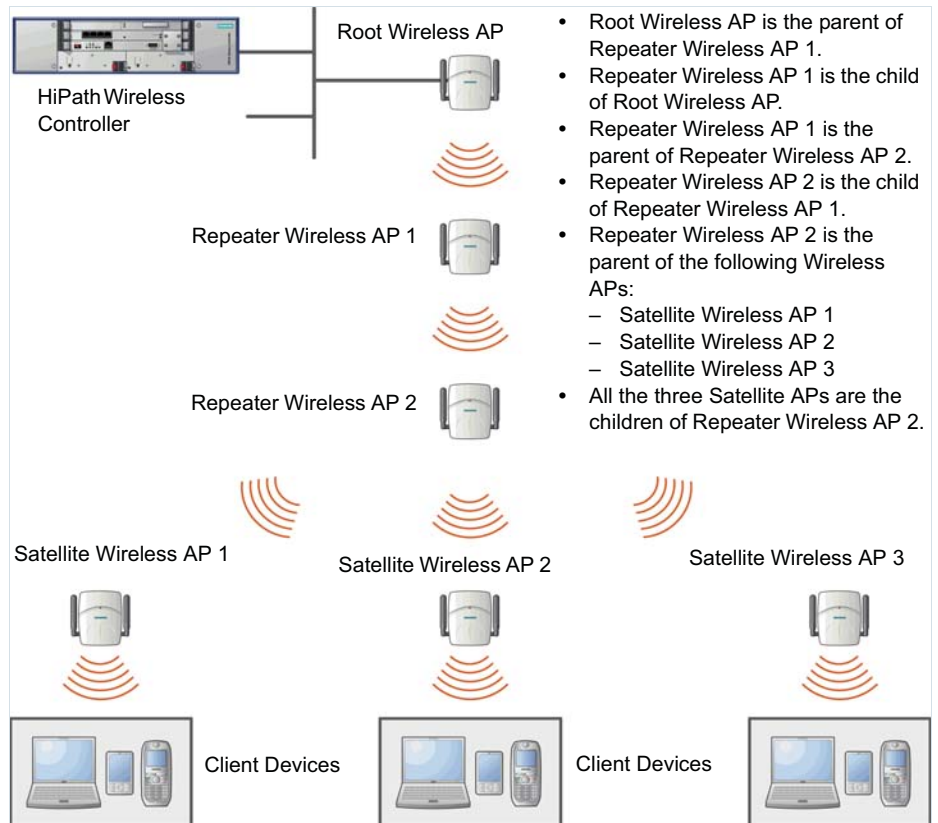


Figure 17 Parent-child relationship between Wireless APs in WDS configuration

## Virtual Network configuration

### Wireless Distribution System

The WDS system enables you to configure the Wireless AP's role — **parent**, **child** or **both** — from the HiPath Wireless Controller's interface. If the WDS Wireless AP will be serving as a parent and a child in a given topology, its role is configured as **both**.

---

**Note:** It is recommended to limit the number of APs participating in a WDS tree to 8. This limit guarantees decent performance in most typical situations.

---

---

**Note:** If a Wireless AP is configured to serve as a scanner in Mitigator, it cannot be used in a WDS tree. For more information, see [Chapter 9, "Working with the Mitigator"](#).

---

#### 6.17.6.2 Radio Channels

The radio channel on which the child Wireless AP operates is determined by the parent Wireless AP.

A Wireless AP may connect to its parent Wireless AP and children Wireless APs on the same radio, or on different radios. Similarly, a Wireless AP can have two children operating on two different radios.

---

**Note:** When a Wireless AP is connecting to its parent Wireless AP and children APs on the same radio, it uses the same channel for both the connections.

---

#### 6.17.6.3 Multi-root WDS topology

A WDS topology can have multiple Root Wireless APs.

[Figure 18](#) illustrates the multiple-root WDS topology.

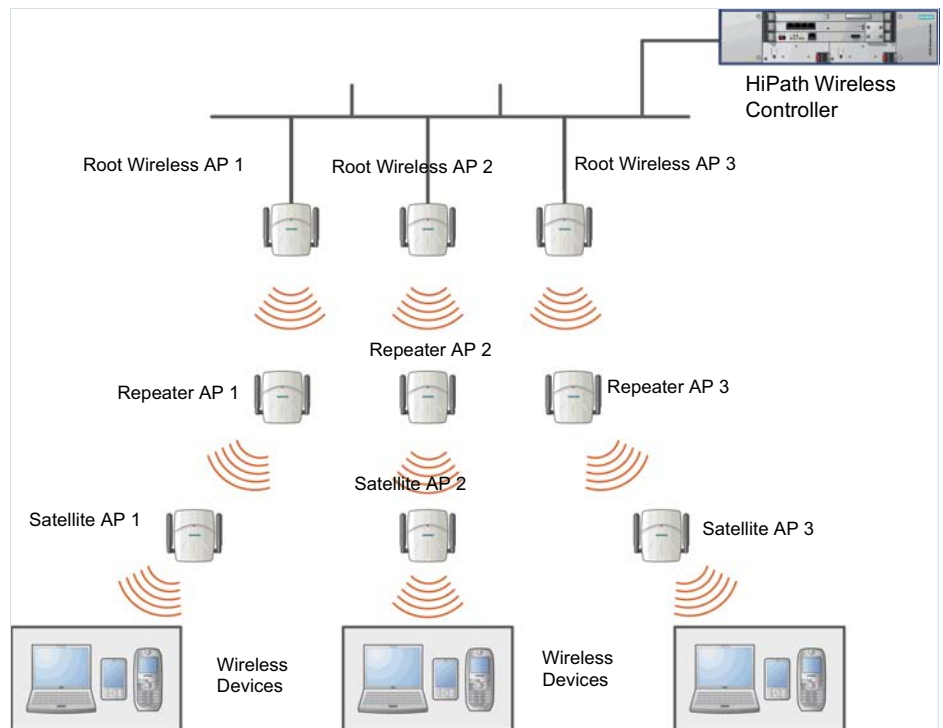


Figure 18 Multiple-root WDS topology

#### 6.17.6.4 Automatic discovery of parent and backup parent Wireless APs

The children Wireless APs, including the Repeater Wireless AP and the Satellite Wireless APs, scan for their respective parents at a startup.

You can configure a parent and backup parent for the children Wireless APs. The Wireless APs will first try to negotiate a WDS link with the parent Wireless AP. If the WDS link negotiation is unsuccessful, the Wireless AP will try to negotiate a link with the backup parent.

#### 6.17.6.5 Link security

The WDS link is encrypted using Advance Encryption Standard (AES).

---

**Note:** The keys for AES are configured prior to deploying the Repeater or Satellite Wireless APs.

---

## 6.17.7 Deploying the WDS system

Before you start configuring the WDS Wireless APs, you must ensure the following:

- The Wireless APs that are part of the wired HiPath WLAN are connected to the wired network.
- The wired Wireless APs that will serve as the Root AP/Root APs of the proposed WDS topology are operating normally.
- The HiPath WLAN is operating normally.

### Sketching the WDS topology

You may sketch the proposed WLAN topology on a paper before you start the WDS deployment process. You should clearly identify the following in the sketch:

- WDS Wireless APs with their names
- Parent-Child relationships between Wireless APs
- Radios that you will choose to link the Wireless AP's parents and children

### Provisioning the WDS Wireless APs

This step is of crucial importance and involves connecting the WDS Wireless APs to the enterprise network via the Ethernet link. This is done to enable the WDS Wireless APs to connect to the HiPath Wireless Controller so that they can derive their WDS configuration.

The WDS Wireless AP's configuration includes pre-shared key, its role, preferred parent name and the backup parent name.

---

**Note:** The provisioning of WDS Wireless APs must be done before they are deployed at the target location. If the Wireless APs are not provisioned, they will not work at their target location.

---

### WDS deployment overview

The following is the high-level overview of the WDS deployment process:

1. Connecting the WDS Wireless APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the HiPath Wireless Controller. For more information, see [Section 4.2, "Discovery and registration overview"](#), on page 71.
2. Disconnecting the WDS Wireless APs from the enterprise network after they have discovered and registered with the HiPath Wireless Controller.
3. Creating a WDS VNS.
4. Assigning roles, parents and backup parents to the WDS Wireless APs.

5. Assigning the Satellite Wireless APs' radios to the network VNSs.
6. Connecting the WDS Wireless APs to the enterprise network via the Ethernet link for provisioning. For more information, see [Section 6.17.7, "Provisioning the WDS Wireless APs"](#), on page 238.
7. Disconnecting the WDS Wireless APs from the enterprise network and moving them to the target location.

---

**Note:** During the WDS deployment process, the WDS Wireless APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the HiPath Wireless Controller, and then the second time to enable them to obtain the provisioning from the HiPath Wireless Controller.

---

#### 6.17.7.1 Connecting the WDS Wireless APs to the enterprise network for discovery and registration

Connect each WDS Wireless AP to the enterprise network to enable it to discover and register themselves with the HiPath Wireless Controller.

---

**Note:** Before you connect the WDS Wireless APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the HiPath Wireless Controller is defined according to your security needs. The **Security mode** property dictates how the HiPath Wireless Controller behaves when registering new and unknown devices. For more information, see [Section 4.3.1, "Defining properties for the discovery process"](#), on page 83.

If the **Security mode** is set to **Allow only approved Wireless APs to connect** (this is also known as secure mode), you must manually approve the WDS Wireless APs after they are connected to the network for the discovery and registration. For more information, see [Section 4.4, "Adding and registering a Wireless AP manually"](#), on page 86.

---

Depending upon the number of Ethernet ports available, you may connect one or more WDS Wireless AP at a time, or you may connect all of them together.

Once a WDS Wireless AP has discovered and registered itself with the HiPath Wireless Controller, disconnect it from the enterprise network.

#### 6.17.7.2 Configuring the WDS Wireless APs through the HiPath Wireless Controller

Configuring the WDS Wireless APs involves the following steps:

## Virtual Network configuration

### Wireless Distribution System

1. Creating a WDS VNS.
2. Defining the SSID name and the pre-shared key.
3. Assigning roles, parents and backup parents to the WDS Wireless APs.

For the ease of understanding, the WDS configuration process is explained with the help of an example. The following illustration depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four Wireless APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the ware house.

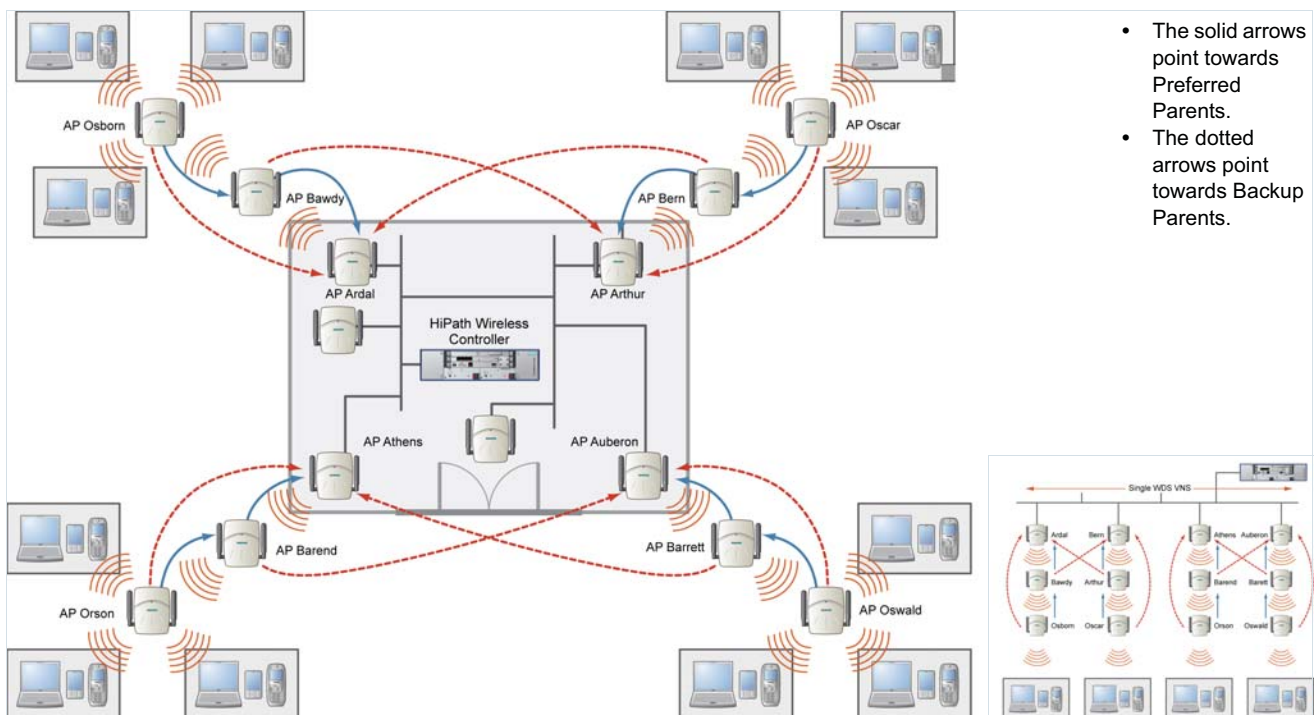


Figure 19 WDS Deployment

**Note:** With the single WDS VNS, the tree structure for the WDS deployment will be as depicted on the bottom right of Figure 19. You can also implement the same deployment using four WDS VNSs, each for a set of Wireless APs in the four corners of the building. Each set of Wireless APs will form an isolated topology and will operate using a separate **SSID** and a separate **Pre-shared** key. For more information, see Section 6.17.5, “WDS VNS”, on page 231.



To configure the WDS Wireless APs through the HiPath Wireless Controller:

**Note:** You must identify and mark the Preferred Parents, Backup Parents and the Child Wireless APs in the proposed WDS topology before starting the configuration process.

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane, type the WDS VNS name in the **Add subnet** box.
3. Click **Add subnet**. The name is displayed in the virtual networks list and the **Topology** tab is displayed.

4. From the **VNS Mode** drop-down list, click **WDS**. The **WDS Topology** tab is displayed.

## Virtual Network configuration

### Wireless Distribution System

The screenshot shows the Siemens HiPath Virtual Network Configuration interface. The top navigation bar includes links for Home, Logs & Traces, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. The main content area is titled "C2000-203wds" and contains a "Topology" tab. A dropdown menu for "VNS Mode" is open, showing "WDS" as the selected option. Below the dropdown are buttons for "Add subnet", "Rename subnet", and "Delete subnet". At the bottom right of the main area are "Save" and "Cancel" buttons. The status bar at the bottom indicates the user is "admin" and provides system information.

5. To save your changes, click **Save**. The **Topology** tab is displayed.

The screenshot shows the Siemens HiPath Virtual Network Configuration interface. The top navigation bar includes links for Home, Logs & Traces, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. The main content area is titled "C2000-203wds" and contains a "Topology" tab. A dropdown menu for "VNS Mode" is open, showing "RF" as the selected option. Below the dropdown are buttons for "Add subnet", "Rename subnet", and "Delete subnet". At the bottom right of the main area are "Save" and "Cancel" buttons. The status bar at the bottom indicates the user is "admin" and provides system information.

- Click the **RF** tab.

The screenshot shows the 'test-wds' configuration page in the Siemens HiPath Virtual Network Configuration software. The 'RF' tab is selected. The SSID is 'test-wds-ssid1' and the Pre-shared Key is '1234567890'. Below this, there is a table titled 'Wireless APs services' with columns for AP Name, b/g, a, Preferred Parent, Backup Parent, and WDS bridge. The table lists several APs, all with 'none' selected for b/g and a modes.

AP Name	b/g	a	Preferred Parent	Backup Parent	WDS bridge
Ardal	none	none			<input type="checkbox"/>
Arthur	none	none			<input type="checkbox"/>
Athens	none	none			<input type="checkbox"/>
Auberon	none	none			<input type="checkbox"/>
Bawdy	none	none			<input type="checkbox"/>
Bern	none	none			<input type="checkbox"/>
Barend	none	none			<input type="checkbox"/>
Barett	none	none			<input type="checkbox"/>
Osborn	none	none			<input type="checkbox"/>
Oscar	none	none			<input type="checkbox"/>
Orson	none	none			<input type="checkbox"/>
Oswald	none	none			<input type="checkbox"/>

- In the **SSID** box, type a name that will identify the new WDS SSID.
- In the **Pre-shared Key** box, type the key.

**Note:** The pre-shared key must be 8 to 63 characters long. The WDS Wireless APs use this pre-shared key to establish a WDS link between them.

**Note:** Changing the pre-shared key after the WDS is deployed can be a lengthy process. For more information, see [Section 6.17.8, “Changing the pre-shared key in WDS VNS”](#), on page 249.

- Assign the roles, preferred parents and backup parents to the Wireless APs.

**Note:** The roles — **parent**, **child**, and **both** — are assigned to the radios of the Wireless APs. A Wireless AP may connect to its parent Wireless AP and children Wireless APs on the same radio, or on different radios. Similarly, a Wireless AP can have two children operating on two different radios. The radio channel on which the child Wireless AP operates is determined by

## Virtual Network configuration

### Wireless Distribution System

the parent Wireless AP.

If the Wireless AP will be serving both as parent and child, you must select **both** as its role.

---

To configure the WDS as illustrated in [Figure 19](#) with a single WDS VNS, you must assign the roles, preferred parents and backup parents to the Wireless APs according to the following table:

Wireless AP	Radio b/g	Radio a	Preferred Parent	Backup Parent
Ardal	Parent	Parent	See the note below.	See the note below.
Arthur	Parent	Parent	See the note below.	See the note below.
Athens	Parent	Parent	See the note below.	See the note below.
Auberon	Parent	Parent	See the note below.	See the note below.
Bawdy	Both	Child	Ardal	Arthur
Bern	Both	Child	Arthur	Ardal
Barend	Both	Child	Athens	Auberon
Barett	Both	Child	Auberon	Athens
Osborn	Child	Child	Bawdy	Ardal
Oscar	Child	Child	Bern	Arthur
Orson	Child	Child	Barend	Athens
Oswald	Child	Child	Barett	Auberon

Table 27 *Wireless APs and their roles*

---

**Note:** Since the Root Wireless APs — Ardal, Arthur, Athens and Auberon — are the highest entities in the tree structure, they do not have parents. Therefore, the **Preferred Parent** and **Backup Parent** drop-down lists of the Root Wireless APs do not display any Wireless AP. You must leave these two fields blank.

---

---

**Note:** You must first assign the 'parent' role to the Wireless APs that will serve as the parents. Unless this is done, the Parent Wireless APs will not be displayed in the **Preferred Parent** and **Backup Parent** drop-down lists of other Wireless APs.

---

---

**Note:** The **WDS Bridge** feature on the user interface relates to WDS Bridge configuration. When you are configuring the WDS Bridge topology, you must select **WDS Bridge** for Satellite Wireless AP that is connected to the wired network. For more information, see [Section 6.17.3, "Wireless Bridge configuration"](#), on page 231.

---

#### To assign the roles, preferred parent and backup parent:

- a) From the radio **b/g** drop-down list of the Root Wireless APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
- b) From the radio **a** drop-down list of the Root Wireless APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
- c) From the radio **a** and radio **b/g** drop-down list of other Wireless APs, click the roles according to [Table 27](#).
- d) From the **Preferred Parent** drop-down list of other Wireless APs, click the parents according to [Table 27](#).
- e) From the **Backup Parent** drop-down list of other Wireless APs, click the backup parents according to [Table 27](#).

## Virtual Network configuration

### Wireless Distribution System

The screenshot shows the Siemens HiPath Virtual Network Configuration interface. The main content area is titled 'test-wds' and has two tabs: 'Topology' and 'RF'. The 'RF' tab is active, showing the following configuration:

- SSID: test-wds-ssid1
- Pre-shared Key: 1234567890

Below this, there is a section for 'Wireless APs services' with a table:

AP Name	b/g	a	Preferred Parent	Backup Parent	WD: bridge
Ardal	parent	parent			<input type="checkbox"/>
Arthur	parent	parent			<input type="checkbox"/>
Athens	parent	parent			<input type="checkbox"/>
Auberon	parent	parent			<input type="checkbox"/>
Bawdy	both	child	Ardal	Arthur	<input type="checkbox"/>
Bern	both	child	Arthur	Ardal	<input type="checkbox"/>
Barend	both	child	Athens	Auberon	<input type="checkbox"/>
Barett	both	child	Auberon	Athens	<input type="checkbox"/>
Osborn	child	child	Bawdy	Ardal	<input type="checkbox"/>
Oscar	child	child	Bern	Arthur	<input type="checkbox"/>
Orson	child	child	Barend	Athens	<input type="checkbox"/>
Oswald	child	child	Barett	Auberon	<input type="checkbox"/>

At the bottom of the interface, there are 'Save' and 'Cancel' buttons. The status bar at the very bottom shows: [ HWC-206 | C2400 | 01 days, 07:39 ] User: admin Port status: [ M 1 2 3 4 F ] Enterprise Software: V5 R1.10014.0 | Tracing: Inactive © Copyright 2006-2008 Siemens AG, All Rights Reserved.

10. To save your changes, click **Save**.

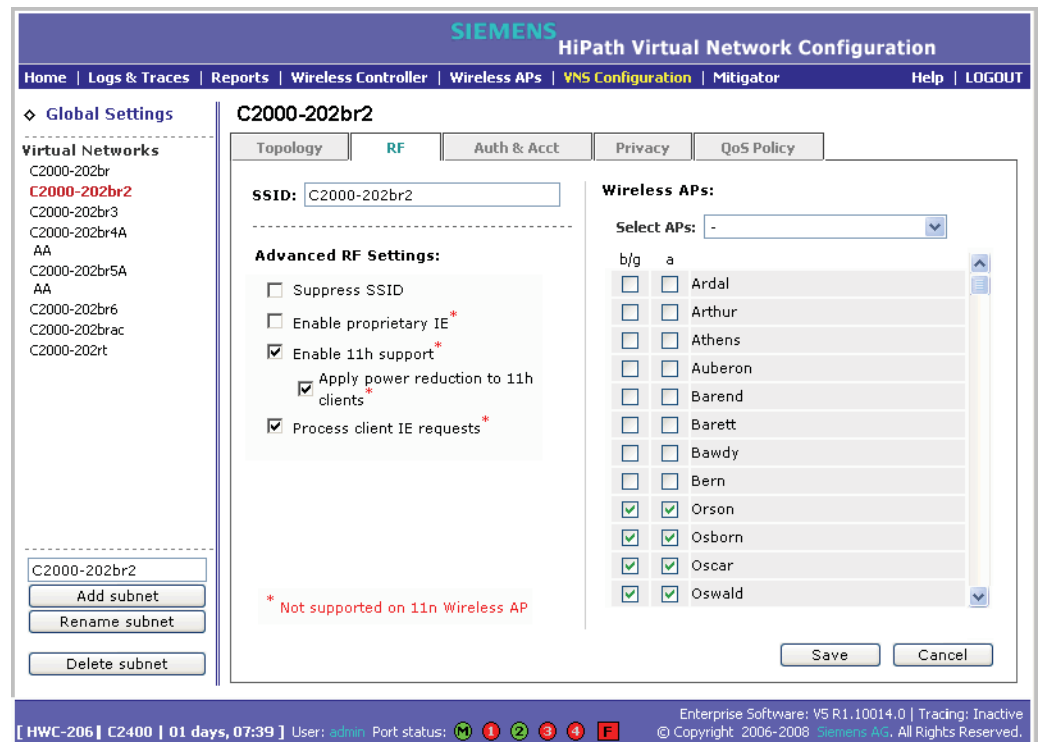
### 6.17.7.3 Assigning the Satellite Wireless APs' radios to the network VNSs

You must assign the Satellite Wireless APs's radios to the network VNSs.

**Note:** The network VNSs are the usual VNSs on which the Wireless APs service the client devices. **Routed, Bridge Traffic Locally at HWC** and **Bridge Traffic Locally at AP** VNSs are the network VNSs. For more information, see [Section 6.1, "VNS Types", on page 163.](#)

#### To assign the Satellite Wireless APs' radios to the network VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** page is displayed.
2. In the left pane **Virtual Networks** list, click the network VNS that you want to assign to the radios of Satellite Wireless APs.
3. Click the **RF** tab.



4. In the **Wireless APs** list, select the radios of the Satellite APs — Osborn, Oscar, Orson and Oswald.

---

**Note:** If you want the Root Wireless AP and the Repeater Wireless APs to service the client devices, you must select their radios in addition to the radios of the Satellite Wireless APs.

---

5. To save your changes, click **Save**.
6. Log out from the HiPath Wireless Controller.

#### 6.17.7.4 Connecting the WDS Wireless APs to the enterprise network for provisioning

You must connect the WDS Wireless APs to the enterprise network once more in order to enable them to obtain their configuration from the HiPath Wireless Controller. The configuration includes the pre-shared key, the Wireless AP's role, preferred parent and backup parent. For more information, see [Provisioning the WDS Wireless APs on page 238](#).

---

**Warning:** If you skip this step, the WDS Wireless APs will not work at their target location.

---

#### 6.17.7.5 Moving the WDS Wireless APs to the target location

1. Disconnect the WDS Wireless APs from the enterprise network, and move them to the target location.
2. Install the WDS Wireless APs at the target location.
3. Connect the Wireless APs to a power source. The discovery and registration processes are initiated.

---

**Note:** If you change any of the following configuration parameters of a WDS Wireless AP, the WDS Wireless AP will reject the change:

- Reassigning the WDS Wireless AP's role from **Child** to **None**
- Reassigning the WDS Wireless AP's role from **Both** to **Parent**
- Changing the **Preferred Parent** of the WDS Wireless AP

However, the HiPath Wireless Controller will display your changes, as these changes will be saved in the database. To enable the WDS Wireless AP to obtain your changes, you must remove it from the WDS location and then connect it to the HiPath Wireless Controller via the wired network.

---

---

**Note:** If you change any of the following radio properties of a WDS Wireless AP, the WDS Wireless AP will reject the change:

- Disabling the radio on which the WDS link is established
  - Changing the radio's Tx Power of a radio on which the WDS link is established
  - Changing the country
-



## 6.17.8 Changing the pre-shared key in WDS VNS

### To change the pre-shared key in WDS VNS:

1. Create a new WDS VNS with a new pre-shared key.
2. Assign the RF of the Wireless APs from the old WDS to the new WDS VNS.
3. Check the **WDS Wireless AP Statistics** report page to ensure that all the WDS Wireless APs have connected to the HiPath Wireless Controller via the new WDS VNS. For more information, see [Section 10.1.2, "Viewing statistics for Wireless APs"](#), on page 295.
4. Delete the old WDS VNS. For more information, see [Section 6.5, "Deleting a VNS"](#), on page 176.

**Virtual Network configuration**  
*Wireless Distribution System*