



# VIEW Certified Configuration Guide

## Enterasys Networks

Enterasys C20, C20N, C2400, C4110, C5110  
with AP 3605, 3610, 3620, 3630, 3640

## Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

## Copyright Notice

© 2010, Polycom, Inc. All rights reserved. POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

All rights reserved under the International and pan-American copyright Conventions.

No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Polycom, Inc.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

## Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY POLYCOM FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF POLYCOM WHATSOEVER.

## Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.  
4750 Willow Road,  
Pleasanton, CA 94588  
<http://www.polycom.com>

# Contents

<b>Overview .....</b>	<b>5</b>
Certified Product Summary .....	5
Known Limitations .....	6
Polycom References .....	6
Product Support .....	6
Network Topology.....	7
<b>Complete Configuration Guide with step-by-step instructions for optimal settings.....</b>	<b>8</b>
Accessing the HiPath Wireless Controller for the first time.....	8
Reset to Factory Defaults via CLI .....	10
Upgrading the HiPath Wireless Convergence Software .....	12
Provisioning HiPath Wireless Controller .....	13
Default Gateway .....	15
Discovering HiPath Wireless AP .....	16
<b>Configuring HiPath Wireless Controller for SpectraLink 8020/8030.....</b>	<b>17</b>
Defining RADIUS Servers .....	17
Setting up VNS.....	18
Setting up Privacy for WPA2-Enterprise.....	20
Setting up Privacy for WPA2-PSK.....	22
Setting up Authentication for WPA2-Enterprise .....	23
Setting up Authentication for WPA2-PSK .....	24
Setting up Quality of Service (QoS).....	24
Configuring filters.....	26
Setting up multicast configuration .....	27
Setting up Radio Properties.....	28

<b>Overview .....</b>	<b>5</b>
Certified Product Summary .....	5
Known Limitations .....	6
Polycom References .....	6
Product Support .....	6
Network Topology.....	7
<b>Complete Configuration Guide with step-by-step instructions for optimal settings.....</b>	<b>8</b>
Accessing the HiPath Wireless Controller for the first time.....	8
Reset to Factory Defaults via CLI .....	10
Upgrading the HiPath Wireless Convergence Software.....	12
Provisioning HiPath Wireless Controller .....	13
Default Gateway .....	15
Discovering HiPath Wireless AP .....	16
<b>Configuring HiPath Wireless Controller for SpectraLink 8020/8030 .....</b>	<b>17</b>
Defining RADIUS Servers .....	17
Setting up VNS .....	18
Setting up Privacy for WPA2-Enterprise.....	20
Setting up Privacy for WPA2-PSK.....	22
Setting up Authentication for WPA2-Enterprise .....	23
Setting up Authentication for WPA2-PSK .....	24
Setting up Quality of Service (QoS).....	24
Configuring Filters.....	26
Setting up Multicast Configuration.....	27
Setting up Radio Properties.....	28

## Overview

Polycom’s Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink Wireless Telephones and WLAN infrastructure products.

The products listed below have been thoroughly tested in Polycom’s lab and have passed VIEW Certification. This guide describes the configuration of the Enterasys C20, C20N, C2400, C4110, C5110 and the Enterasys AP 3605, 3610, 3620, 3630, 3640 with SpectraLink 8020/8030 Wireless Telephones.

## Certified Product Summary

Manufacturer:	Enterasys Networks: <a href="http://www.enterasys.com">www.enterasys.com</a>			
Certified products:	Controller models: C20, C20N, C2400, C4110, C5110		AP models: 3605, 3610, 3620, 3630, 3640	
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)			
Security:	WPA-PSK, WPA2-PSK, WPA2-Enterprise (EAP-FAST and/or PEAPv0/MSCHAPv2) with OKC (Opportunistic Key-Caching)			
QoS:	Wi-Fi Standard QoS			
AP and controller software version tested:	7.21			
Handset models tested:	SpectraLink 8020/8030 Wireless Telephone*			
Radio mode:	802.11b & b/g mixed		802.11a	
Meets VIEW minimum call capacity per AP:	SVP	Wi-Fi Std	SVP	Wi-Fi Std
	Not supported	6	Not supported	10
Network topology:	Bridge Traffic Locally at HWC Bridge Traffic Locally at AP Routed**			

\*SpectraLink handset models 8020/8030 and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “SpectraLink Wireless Telephones” or “handsets”.

\*\*Routed network topology is only recommended with single controller deployment. If multiple controllers are present then the Mobility feature must be configured.

## Known Limitations

- AP 36XX does not support configurable minimum basic rate for either Radio 1 or Radio 2. (Being addressed in a future release)
- AP 3630/3640 needs to be converted to “Fit” mode. See the [Enterasys Wireless Standalone 802.11n AP User Guide](#) for instructions.

## Polycom References

Please refer to the Polycom *Deploying Enterprise-Grade Wi-Fi Telephony* white paper. This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones*. This document identifies issues and solutions based on Polycom’s extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with SpectraLink 8020/8030 Wireless Telephones.

These two white papers are available at:

[http://www.polycom.com/products/voice/wireless\\_solutions/wifi\\_communications/handsets/spectralink\\_8020\\_wireless.html](http://www.polycom.com/products/voice/wireless_solutions/wifi_communications/handsets/spectralink_8020_wireless.html)

## Product Support

For additional support, contact Enterasys Networks using one of the following methods:

World Wide Web <http://www.enterasys.com/support>

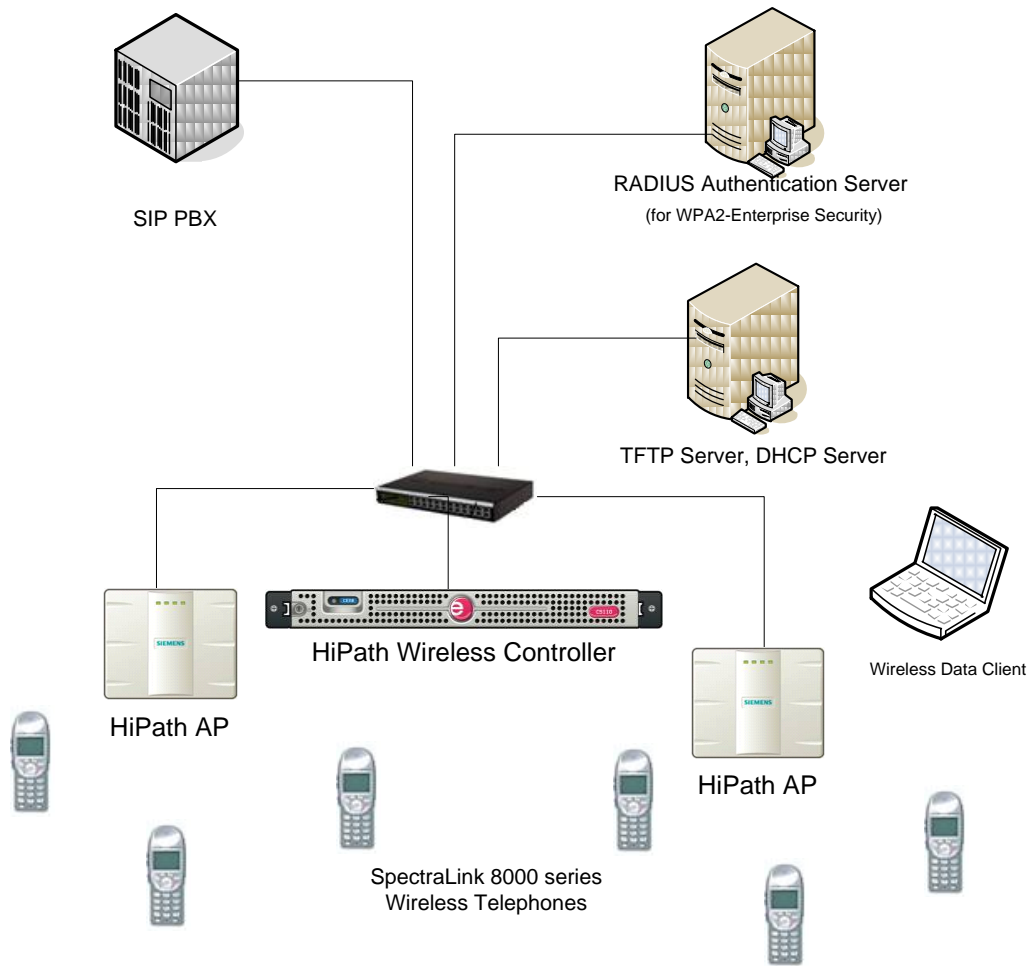
Phone 1-800-872-8440 (toll-free in U.S. and Canada)  
or 1-978-684-1000

For the Enterasys Networks Support toll-free number in your country:  
<http://www.enterasys.com/support>

Internet mail [support@enterasys.com](mailto:support@enterasys.com)

To quicken the response from Enterasys Network Support, please type [**HiPath Wireless Convergence Software**] in the subject line.

## Network Topology



This configuration is not applicable to all customer environments.

# Complete Configuration Guide

## with step-by-step instructions for optimal settings

### Accessing the HiPath Wireless Controller for the first time

#### Via CLI

##### HiPath Wireless Controller C2400

In order to get in to CLI mode in the HiPath Wireless Controller C2400:

1. Connect your laptop to the HiPath Wireless Controller C2400 via Null Modem DB9 F-F (Female to Female) cable.
2. Using a terminal program of choice, configure the following settings for the appropriate COM device:
  - **Speed** – 9600
  - **Databits** – 8
  - **Parity** – None
  - **Stop Bits** – 1
  - **Flow Control** – None

##### HiPath Wireless Controller C20

In order to get in to CLI mode in the HiPath Wireless Controller C20:

3. Download the **CP210x VCP** driver that is specific to your Operating System (OS) from [www.silabs.com](http://www.silabs.com).
4. Connect your laptop to the HiPath Wireless Controller C20 via USB A/B Device Cable.
5. Using a terminal program of choice, configure the following settings for the appropriate COM device:
  - **Speed** – 115200
  - **Databits** – 8
  - **Parity** – None
  - **Stop Bits** – 1

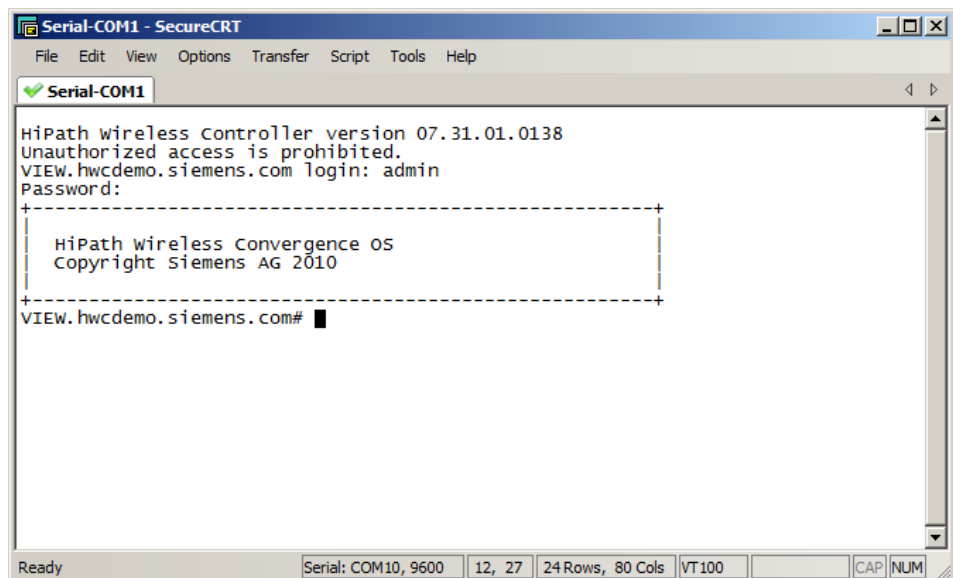
- **Flow Control** – None

## HiPath Wireless Controller C20N, C4110, C5110

In order to get into CLI mode in the HiPath Wireless Controller C20N, C4110, C5110:

1. Connect your laptop to the controller's RS232 serial console port via the Null Modem DB9 F- F (Female to Female) cable.
2. Using a terminal program of choice, configure the following settings for the appropriate COM device:
  - **Speed** – 115200
  - **Databits** – 8
  - **Parity** – None
  - **Stop Bits** – 1
  - **Flow Control** – None

### To access the HiPath Wireless Controller using a terminal program:



```
Serial-COM1 - SecureCRT
File Edit View Options Transfer Script Tools Help
Serial-COM1
HiPath wireless Controller version 07.31.01.0138
Unauthorized access is prohibited.
VIEW.hwcdemo.siemens.com login: admin
Password:
+-----+
| HiPath wireless Convergence OS |
| Copyright Siemens AG 2010     |
+-----+
VIEW.hwcdemo.siemens.com#
```

3. At the **login:** prompt, type **admin**.
4. At the **Password:** prompt, type **abc123**.
5. Press Enter. The **HiPath Wireless Convergence OS** banner is displayed.

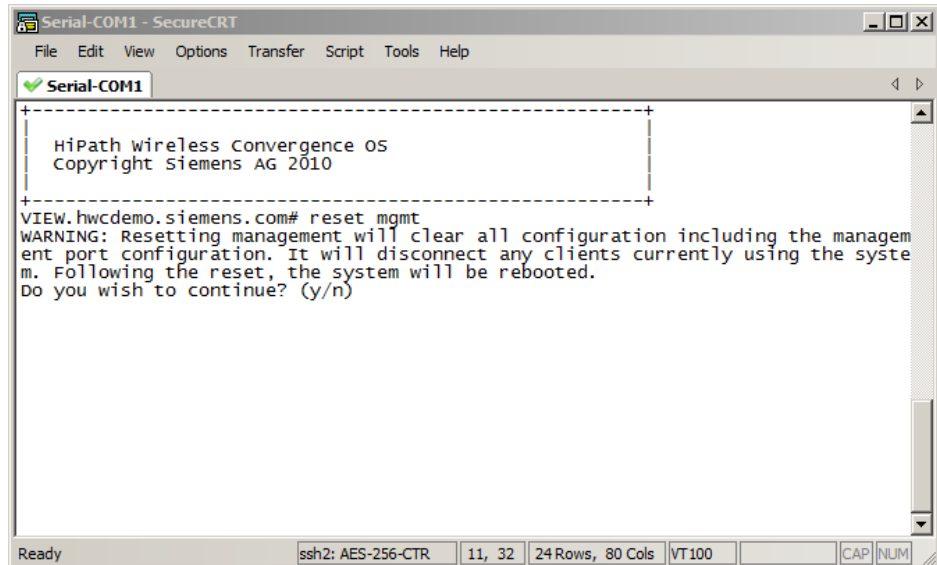


Polycom recommends that you change the default password.

## Reset to Factory Defaults via CLI

### To reset your system configuration:

1. At the prompt, type **reset mgmt**.
2. Press Enter. The following prompt is displayed:



3. At the prompt, type **y**.

## Via GUI

### HiPath Wireless Controller Management port interface

The management port on the HiPath Wireless Controller may be labeled differently depending on the HiPath Wireless Controller.

HiPath Wireless Controller	Management Port Label
C5110	Gb 1
C4110	Gb 1
C2400	Management
C20	Admin
C20N	Ethernet 10/100

*Management port label on the HiPath Wireless Controller*

## To access the HiPath Wireless Controller using a Web-enabled laptop:

1. Statically assign an unused IP address in the 192.168.10.0/24 subnet for the Ethernet port of the laptop computer. You can use any IP address from 192.168.10.2 to 192.168.10.254.
2. Connect the HiPath Wireless Controller's management port to the Web-enabled laptop computer with a cross-over RJ45 Ethernet cable.



The default IP address of the HiPath Wireless Controller's management port is 192.168.10.1.

3. Launch your Web browser.
4. In the address bar, type `https://192.168.10.1:5825`. The **HiPath Wireless Assistant** login screen is displayed.



5. In the **User Name** text box, type admin.
6. In the **Password** text box, type abc123.
7. Click **Login**. The **HiPath Wireless Assistant** is displayed.



The default password should be changed.

## Reset to Factory Defaults via GUI

### To reset your system configuration:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. In the **Reset Configuration** section, select the appropriate configuration reset options:
  - **Remove installed license** – The system reboots and restores all aspects of the system configuration to the initial settings and the license key is removed. However, the Management IP address is preserved. This permits administrators to remain connected through the Management interface.
  - **Remove management port configuration** – The system reboots and resets the entire system configuration to the factory shipping state. The Management IP address reverts to 192.168.10.1.
3. Click **Reset Configuration**.
  - Depending on the configuration reset options you select, a warning message is displayed asking you to confirm your selection.
  - If the **Remove installed license** option is selected, the warning message also displays the license activation key and optional features license keys.

**Warning:** Copy the license key information displayed in the warning message in order to reuse these keys after the HiPath Wireless Controller resets to its factory defaults.
4. Click **Yes** to continue. Your system reboots and the configuration is reset to its factory defaults.

## Upgrading the HiPath Wireless Convergence Software



For the latest HiPath Wireless Convergence software, visit [www.enterasys.com/support](http://www.enterasys.com/support).

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. From the left pane, click **Software Maintenance**. The **HWC Software** tab is displayed.
3. Select **Remote**. The FTP server boxes are displayed.

4. Type the following:

- **FTP Server** – The IP address of the FTP server to retrieve the image file from.
- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The password for the user ID.
- **Confirm** – The password to log on to the FTP server. This field is to confirm you have typed the correct password.
- **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

5. Click the **Upgrade now** button.

## Provisioning HiPath Wireless Controller

### AP Registration

#### To configure AP registration:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.

- From the left pane, click **Topology**. The **Topologies** tab is displayed.
- Choose a Topology to be used for **AP Registration**.

HiPath Wireless Controller	Data Port Label
C5110	esa0, esa1 and esa2
C4110	Port1, Port2, Port3 and Port4
C2400	esa0, esa1, esa2, esa3
C20	esa0 and esa1
C20N	PC.1 and PC.2

Data port label on the HiPath Wireless Controller



The Admin Topology cannot be used for AP Registration.

- Click the desired **Topology**. The **Edit Topology** pop-up window displays.
- In the **Interface IP** box, type the IP address.
- In the **Mask** box, type the subnet mask.
- Select the **AP Registration** option.
- Select the **Management Traffic** option.

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

## Default Gateway

### To define the default gateway:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. From the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.
3. In the **Destination Address** box, type (0.0.0.0).
4. In the **Subnet Mask** box, type (0.0.0.0).
5. In the **Gateway** box, type the IP address of the next hop for the configured data port used for AP Registration, click **Add**.

» View Forwarding Table

Static Routes OSPF

R#	Dest. Addr.	Subnet Mask	Gateway	O/D
1	0.0.0.0	0.0.0.0	10.10.10.1	on

Destination Address:

Subnet Mask:

Gateway:

Override dynamic routes

Add Delete

Save Cancel

6. To Save your changes, click **Save**
7. Connect the HiPath Wireless Controller's data port to the network infrastructure with a RJ45 Ethernet cable.

## Discovering HiPath Wireless AP

### 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 three steps summarize the most commonly used discovery methods (See Getting Started Guide for additional methods):

- **Step 1 - Use Dynamic Host Configuration Protocol (DHCP) Option 60 to query the DHCP server for available HiPath Wireless Controllers. The DHCP server will respond to the Wireless AP with Option 43, which will list the available HiPath Wireless Controllers.**

For the DHCP server to respond to a Wireless AP's Option 60 request, you must configure the DHCP server with the vendor class identifier (VCI) for each Wireless AP. You must also configure the DHCP server with the IP addresses of the HiPath Wireless Controllers. For more information, refer to

[HiPath Wireless Controller, Access Points and Convergence Software Getting Started Guide.](#)

- **Step 2 - Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.**

The Wireless AP tries the DNS server if it is configured in parallel with SLP unicast and SLP multicast.

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 3 - Use a multicast SLP request to find SLP SAs**

The Wireless AP sends a multicast SLP request, looking for any SLP Service Agents providing the Siemens service.

The Wireless AP will try SLP multicast in parallel with other discovery methods.

# Configuring HiPath Wireless Controller for SpectraLink 8020/8030

## Defining RADIUS Servers



Defining a RADIUS server may not be applicable to all customer environments.

### To define RADIUS servers for VNS global settings:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then **Authentication**.
3. To define a new RADIUS server available on the network, click the **New** button. The **RADIUS Settings** pop up window displays.

**RADIUS Settings**

**RADIUS Server**

Server Alias:

Hostname/IP:

Shared Secret:  Unmask

Default Protocol: PAP

**Authentication**

Priority:

Total Number of Tries:

RADIUS Request Timeout:  (seconds)

Port:

**Accounting**

Priority:

Total Number of Tries:

RADIUS Request Timeout:  (seconds)

Interim Accounting Interval:  (minutes)

Port:

Save Cancel

4. In the **Server Alias** box, type a name that you want to assign to the RADIUS server.
5. In the **Hostname/IP** box, type either the RADIUS server's FQDN (fully qualified domain name) or IP address.

6. In the **Shared Secret** box, type the password that will be used to validate the connection between the HiPath Wireless Controller and the RADIUS server.
7. To save your changes, click **Save**. The new server is displayed in the **RADIUS Servers** list.
8. To save your changes, click **Save**.

## Setting up VNS



Polycom recommends that you create a dedicated VNS for SpectraLink Wireless Telephones only.

### To set up the VNS:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane and click **Add VNS (subnet)**.
3. Type a name that will identify the new VNS in the **VNS Name** box.

#### VNS:

The screenshot shows the VNS configuration page. It has a title bar 'Core'. Below it are four main sections:

- Core:** A text input field for 'VNS Name'.
- WLAN Service:** A dropdown menu for 'WLAN Service', followed by 'Edit' and 'New' buttons.
- Default Policies:** Two rows. The first row has a dropdown for 'Non-Authenticated', 'Edit', and 'New' buttons, and 'Topology: Ingress RC: Egress RC:'. The second row has a dropdown for 'Authenticated' (set to '<Same as non-authenticated>'), 'Edit', and 'New' buttons, and 'Topology: Ingress RC: Egress RC:'.
- Status:** 'Synchronize:' with a checked checkbox. Below it, 'Restrict Policy Set:' with an unchecked checkbox and the text 'Replicated when Synchronize Configuration is enabled'. Below that, 'Enable:' with an unchecked checkbox.

A 'Save' button is located at the bottom right of the form.

4. In the WLAN Service area, create a new WLAN Service by clicking the **New** button. The WLAN Service window is displayed.

5. From the Default Policies area, select an existing **Non-Authenticated** and **Authenticated** policy, or create a new one by clicking the **New** button. The Policy configuration window is displayed.
6. From the Topology area, select an existing topology from the **Assigned Topology** drop-down list, or create a new one by clicking the **New** button.
7. Enable the WLAN (\_Note: This location may need to be returned to to enable the WLAN after making changes.)



The SpectraLink telephones can be deployed in **Bridge Traffic Locally at AP**, **Bridge Traffic Locally at HWC** or **Routed** topology. Which one is applicable depends on the customer environment. In **Bridge Traffic Locally at AP** topology, voice traffic is terminated on the AP. In **Bridge Traffic Locally at HWC** and **Routed** (tunneled topology), voice traffic is terminated at the HiPath Wireless Controller. Appropriate network connectivity to the SIP GW should be provided in all three topologies.

### For “Routed” Topology Mode:

1. In the Core area, from the **Mode** drop-down menu, select **Routed**.
2. In the Layer 3 area, in the **Gateway** box, type the network gateway address.

3. In the **Mask** box, type the appropriate values.
4. From the **DHCP Option** drop-down menu, you can select either the **Local DHCP Server** or **Use DHCP Relay**, depending upon your network topology. Click the **Configure** button.
5. In the **Address Range** boxes (**from** and **to**), type the IP address range.
6. To save your changes, click **Save**.

### For “Bridge Traffic Locally At AP Topology” Mode:

1. In the Core area, from the **Mode** drop-down menu, select **Bridge Traffic Locally At AP**.
2. To save your changes, click **Save**.

### For “Bridge Traffic Locally At HWC Topology” Mode:

1. In the Core area, from the **Mode** drop-down menu, select **Bridge Traffic Locally At HWC**.
2. In the Layer 2 area, in the **VLAN ID** box, type the VLAN number.
3. From the **Port** drop-down menu, select the physical interface to egress traffic from.
4. In the Layer 3 area, in the **Interface IP** box, type the network address.
5. In the **Mask** box, type the appropriate values.
6. From the **DHCP Option** drop-down menu, you can select either the **Local DHCP Server** or **Use DHCP Relay**, depending upon your network topology. Click the **Configure** button.
7. In the **Gateway** box, type the network gateway address.
8. In the **Address Range** boxes (**from** and **to**), type the IP address range.
9. To save your changes, click **Save**.

## Setting up Privacy for WPA2-Enterprise



The selected privacy may not be applicable to all customer environments.

### To set up the privacy:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the WLAN Services pane, then select the desired WLAN Service.
3. Click the **Privacy** tab.
4. Select the **WPA** option.
5. Deselect the **WPA v.1** option.
6. Select the **WPA v.2** option.
7. Under **WPA v.2** section, select **AES only** from the **Encryption** drop-down menu.



The SpectraLink telephones must also be configured for WPA v.2 security.

8. From the **Key Management Options** drop-down menu, select **Opportunistic Keying**.



Polycom recommends that you select **Opportunistic Keying** for **WPA v.2** privacy.

The screenshot shows the 'Edit WLAN Service' window with the 'Privacy' tab selected. The 'WLAN Services' pane on the left has 'WPA' selected. In the 'Privacy' section, 'WPA v.1' is unchecked and 'WPA v.2' is checked. Under 'WPA v.2', the 'Encryption' dropdown is set to 'AES only'. The 'Key Management Options' dropdown is set to 'Opportunistic Keying'. The 'Broadcast re-key interval' is checked and set to 3600 seconds. The 'Group Key Power Save Retry' checkbox is unchecked. A note at the bottom states: 'Note: using WEP or WPAv1 privacy will limit 11n performance to legacy AP rates'. Buttons for 'New', 'Delete', 'Save', and 'Cancel' are visible at the bottom.

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

## Setting up Privacy for WPA2-PSK



The selected privacy may not be applicable to all customer environments.

### To set up the privacy:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **WLAN Services** pane, then select the desired WLAN Service.
3. Click the **Privacy** tab.
4. Select the **WPA - PSK** option.
5. Deselect the **WPA v.1** option.
6. Select the **WPA v.2** option.
7. Under **WPA v.2** section, select **AES only** from the **Encryption** drop-down menu.



The SpectraLink telephones must also be configured for WPA v.2 security.

The screenshot shows the 'Edit WLAN Service' window with the 'WLAN: VIEW' tab selected. The 'Privacy' sub-tab is active. On the left, 'WPA - PSK' is selected. Under 'WPA v.2', 'Encryption' is set to 'AES only'. The 'Broadcast re-key interval' is set to 3600 seconds. The 'Pre-shared key String' field contains masked characters. A note at the bottom states: 'Note: using WEP or WPAv1 privacy will limit 11n performance to legacy AP rates'. Buttons for 'New', 'Delete', 'Save', and 'Cancel' are visible at the bottom.

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

## Setting up Authentication for WPA2-Enterprise



The selected authentication may not be applicable to all customer environments.

### To set up the authentication:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **WLAN Services** pane, then select the desired WLAN Service.
3. Click the **Auth & Acct** tab.
4. Under **Authentication** section, select **802.1x** from the **Mode** drop-down menu.
5. From the **Radius Servers** section, select the desired Radius Server from the drop-down menu and click **Use**.
6. Select the **Auth** checkbox.

The screenshot shows the 'Edit WLAN Service' window with the 'Auth & Acct' tab selected. The 'Authentication' section has 'Mode' set to '802.1x'. The 'RADIUS Servers' section shows 'NPS\_1' selected. The 'Auth' checkbox is checked.

Server	Auth	Acct
NPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

7. To save your changes, click Save.

## Setting up Authentication for WPA2-PSK



The selected authentication may not be applicable to all customer environments.

### To set up the authentication:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **WLAN Services** pane, then select the desired WLAN Service.
3. Click the **Auth & Acct** tab.
4. Under **Authentication** section, select **Disabled** from the **Mode** drop-down menu.

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

## Setting up Quality of Service (QoS)

### To set up Quality of Service (QoS):

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

2. In the left pane, expand the **WLAN Services** pane, then select the desired WLAN Service.
3. Click the **QoS** tab.
4. Under the **Wireless QoS** section, select the following:
  - **WMM**
  - **Turbo Voice**
  - **Enable U-APSD**
5. Click the **Advanced** button.
6. Under the **DSCP Classification** section, map the DSCP value **0: CS0 / DE** to **Best Effort (1)**.
7. Under the **Advanced Wireless QoS** section, select **Use Global Admission Control for Voice (VO)** and select **Use Global Admission Control for Video (VI)**.

**Edit WLAN Service**

**WLAN: VIEW**

WLAN Services | Privacy | Auth & Acct | **QoS**

**Wireless QoS**

- Legacy
- WMM
- 802.11e
- Turbo Voice
- U-APSD

**Advanced**

**Priority Processing:**

Priority Override

**DSCP classification**

DSCP	Service Class
0: CS0 / DE	Best Effort (1)
8: CS1	Background (0)
16: CS2	Best Effort (1)
24: CS3	Silver (3)
32: CS4	Gold (4)
40: CS5	Platinum (5)

Reset to Defaults

**Advanced Wireless QoS:**

- Use Global Admission Control for Voice (VO)
- Use Global Admission Control for Video (VI)

UL Policer Action: Do nothing

DL Policer Action: Do nothing

\* Global admission controls are configured through Global Settings

New | Delete | Close



DSCP table can be configured to change the default marking of the outgoing Voice packet on the Wired network. If default values are used, outgoing Voice packet has DSCP marked 46 (EF) in outer IP header (if tunneled VNS) and 802.1p priority set to 6 in the outer L2 header (if 802.1q used).

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

## Configuring Filters



Polycom recommends that you only configure necessary filters for SpectraLink Wireless Telephone to communicate with the network. Otherwise, simply select the **Allow** checkbox for **0.0.0.0/0**.

### To configure the filters:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **Policies** pane and select the policy to configure.
3. On the **Policy Configuration** screen, click the **Filter Rules** tab. The filtering rule for the **Default** filter is displayed in the centre pane.
4. Click the **Add** button, then type the IP address in **IP/Subnet** and **port** boxes.
5. From the **Protocol** drop-down menu, select the protocol.



Filter Rules can be customized for specific ports/protocols to provide granular security.

**Edit Policy**  
Policy: VIEW

VLAN & Class of Service | Filter Rules

Do not change filter settings when this Policy is applied

HWC Filters |  AP Filtering

Rule	In	Out	Allow	IP : Port	Protocol
D	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0/0	N/A

T: local interface, U: user defined, D:default. Rules with Allow unchecked are denied.

Up | Down | Add | Delete

Select filter

IP/subnet: User Defined |

Port: User Defined |

Protocol: N/A |

OK | Cancel

New | Delete | Save | Cancel

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

## Setting up Multicast Configuration



For Bridged Traffic Locally at Controller and Routed Topology Mode only: Before you set up multicast configuration, you must specify the physical port for routing multicast traffic on the **Wireless Controller** configuration screen under **Topologies** and then **Multicast Support**.

### To set up multicast configuration:

1. From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the Topologies pane and select the desired topology.
3. Select the Multicast Filters tab, then select the **Enable Multicast Support** checkbox.
4. From the **Defined groups** drop-down list, select **Spectralink (224.0.1.116)** and then click **Add**.
5. Select the **Wireless Replication** checkbox.

#### Topology: VIEW

General		Multicast Filters	
<input checked="" type="checkbox"/> <b>Multicast Support</b>			
IP	Group	Wireless Replication	
224.0.1.116/32	Spectralink SVP	<input checked="" type="checkbox"/>	
0.0.0.0/0	Default	<input type="checkbox"/>	
<input type="radio"/> <b>IP Group:</b> <input type="text" value="0.0.0.0/0"/> <input type="button" value="Up"/> <input type="button" value="Down"/>			
<input checked="" type="radio"/> <b>Defined groups:</b> <input type="text" value="Spectralink SVP (224.0.1.116)"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>			
<input type="button" value="New"/> <input type="button" value="Delete"/>		<input type="button" value="Save"/>	

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

## Setting up Radio Properties



For the AP3620/3640, under **AP Properties**, select the installed antenna from the drop-down menu for the **Left, Middle, Right Antenna Type**.

### To set up the radio for Voice Wireless LAN in HiPath Wireless 802.11n APs:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen is displayed.
2. From the list of Wireless APs, select the Wireless 802.11n AP that is being used for the SpectraLink VNS.
3. On the **Wireless AP Configuration** screen, select the tab for the radio that is being used for the SpectraLink VNS.
4. For **Radio Mode**, select the protocol to be used for the SpectraLink VNS.



The SpectraLink telephones can be deployed with 'b', 'b/g', 'b/g/n', 'a' or 'a/n' protocol. When deployed in 'n' modes, telephones would coexist with 11n clients.



The SpectraLink telephones must also be configured for the selected protocol.

5. Click the **Advanced** button.
6. Under **Base Settings**, set the **DTIM Period** to **2**.
7. Retain the default values for all other parameters.

**Advanced**

**Base Settings**

DTIM Period  Beacon Period

RTS/CTS Threshold  Frag. Threshold

Max % of non-unicast traffic per Beacon period

Maximum Distance [m]

**Basic Radio Settings**

Dynamic Channel Selection

**11n Settings**

Protection Mode

40MHz Protection Mode

40MHz Prot. Channel Offset

40MHz Channel Busy Threshold

Aggregate MSDUs

Aggregate MSDU Max Length

Aggregate MPDUs

Aggregate MPDU Max Length

Agg. MPDU Max # of Sub-frames

ADDBA Support

Close

8. Click the **WLAN Assignment** tab.
9. Select the radio that is being used for the SpectraLink VNS named VIEW.

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x
WLAN Name		Radio 1	Radio 2		
VIEW		<input checked="" type="checkbox"/>	<input type="checkbox"/>		

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