7.5 Viewing the Wireless AP availability display

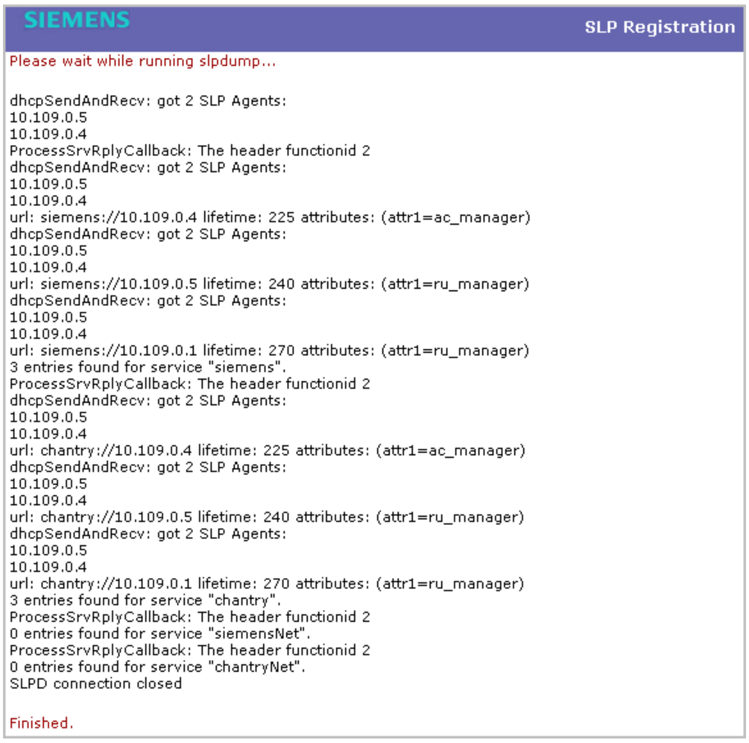
For more information, see Section 11.3, “Viewing the Wireless AP availability display”, on page 455.

7.6 Viewing SLP activity

In normal operations, the primary HiPath Wireless Controller registers as an SLP service called ac_manager. The controller service directs the Wireless APs to the appropriate HiPath Wireless Controller. During an outage, if the remaining HiPath Wireless Controller is the secondary controller, it registers as the SLP service ru_manager.

To view SLP activity:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless APs** screen is displayed.
2. In the left pane, click **AP Registration**. The **Wireless AP Registration** screen is displayed.
3. To confirm SLP registration, click **View SLP Registration**. A pop-up screen displays the results of the diagnostic slpdump tool, to confirm SLP registration.



```
Please wait while running slpdump...

dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
ProcessSrvRplyCallback: The header functionid 2
dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
url: siemens://10.109.0.4 lifetime: 225 attributes: (attr1=ac_manager)
dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
url: siemens://10.109.0.5 lifetime: 240 attributes: (attr1=ru_manager)
dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
url: siemens://10.109.0.1 lifetime: 270 attributes: (attr1=ru_manager)
3 entries found for service "siemens".
ProcessSrvRplyCallback: The header functionid 2
dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
url: chantry://10.109.0.4 lifetime: 225 attributes: (attr1=ac_manager)
dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
url: chantry://10.109.0.5 lifetime: 240 attributes: (attr1=ru_manager)
dhcpSendAndRecv: got 2 SLP Agents:
10.109.0.5
10.109.0.4
url: chantry://10.109.0.1 lifetime: 270 attributes: (attr1=ru_manager)
3 entries found for service "chantry".
ProcessSrvRplyCallback: The header functionid 2
0 entries found for service "siemensNet".
ProcessSrvRplyCallback: The header functionid 2
0 entries found for service "chantryNet".
SLPD connection closed

Finished.
```

8 Configuring Mobility

This chapter describes the mobility concept, including:

- Mobility overview
- Mobility domain topologies
- Configuring mobility domain

8.1 Mobility overview

The HiPath Wireless Controller, Access Points and Convergence Software system allows up to 12 HiPath Wireless Controllers on a network to discover each other and exchange information about a client session. This technique enables a wireless device user to roam seamlessly between different Wireless APs on different HiPath Wireless Controllers.

The solution introduces the concept of a mobility manager; one HiPath Wireless Controller on the network is designated as the **mobility manager** and all others are designated as **mobility agents**.

The wireless device keeps the IP address, and the service assignments it received from its home HiPath Wireless Controller—the HiPath Wireless Controller that it first connected to. The WLAN Service on each HiPath Wireless Controller must have the same SSID and RF privacy parameter settings.

You have two options for choosing the mobility manager:

- Rely on SLP with DHCP Option 78
- Define at the agent the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended to provide tighter control of the registration steps for multi-domain installations.

The HiPath Wireless Controller designated as the mobility manager:

- Is explicitly identified as the manager for a specific mobility domain. Agents will connect to this manager to establish a mobility domain.
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Uses SLP, if this method is preferred, to register itself with the SLP Directory Agent as SiemensNet.
- Defines the registration behavior for a multi-controller mobility domain set:

  - **Open mode** – A new agent is automatically able to register itself with the mobility manager and immediately becomes part of the mobility domain
  - **Secure mode** – The mobility manager does not allow a new agent to automatically register. Instead, the connection with the new agent is placed in pending state until the administrator approves the new device.
- Listens for connection attempts from mobility agents.
- Establishes connections and sends a message to the mobility agent specifying the heartbeat interval, and the mobility manager's IP address if it receives a connection attempt from the agent.
- Sends regular heartbeat messages containing wireless device session changes and agent changes to the mobility agents and waits for a returned update message

The HiPath Wireless Controller designated as a mobility agent does the following:

- Uses SLP or a statically configured IP address to locate the mobility manager
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Attempts to establish a TCP/IP connection with the mobility manager
- Sends updates, in response to the heartbeat message, on the wireless device users and the data tunnels to the mobility manager.

If a controller configured as the mobility manager is lost, the following occurs:

- Agent to agent connections remain active.
- Mobility agents continue to operate based on the mobility information last coordinated before the manager link was lost. The mobility location list remains relatively unaffected by the controller failure. Only entries associated with the failed controller are cleared from the registration list, and users that have roamed from the manager controller to other agents are terminated and required to re-register as local users with the agent where they are currently located.
- The data link between active controllers remains active after the loss of a mobility manager
- Mobility agents continue to use the last set of mobility location lists to service known users
- Existing users remain in the mobility scenario, and if the users are known to the mobility domain, they continue to be able to roam between connected controllers
- New users become local at attaching controller

- Roaming to another controller resets session

The mobility network that includes all the HiPath Wireless Controllers and the Wireless APs is called the **Mobility Domain**.

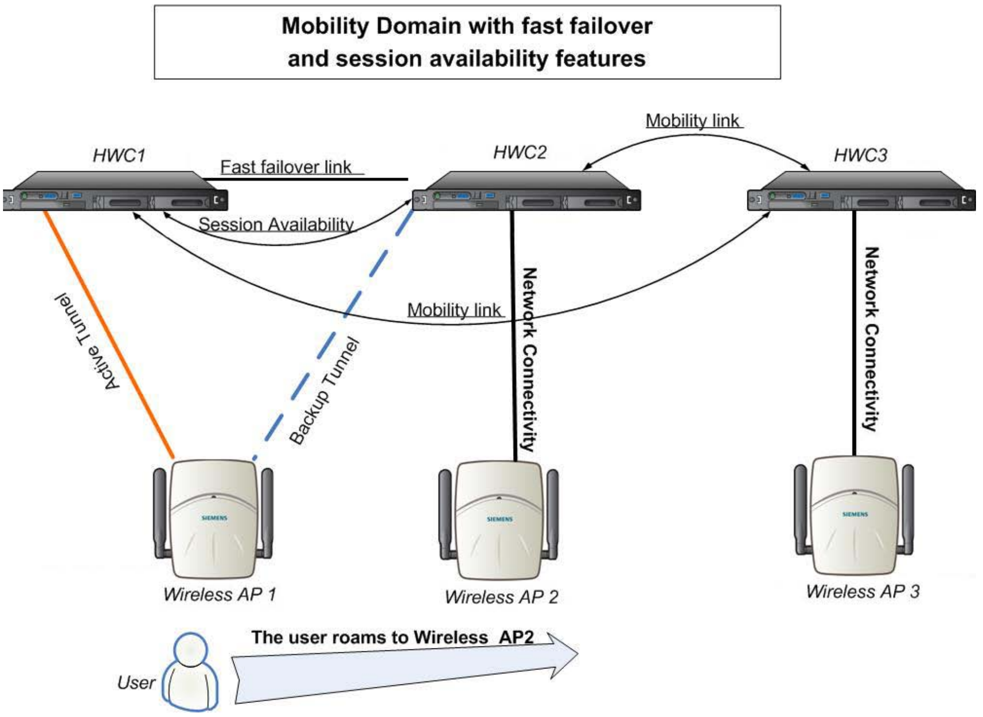
Note: The mobility feature is not backward compatible. This means that all the HiPath Wireless Controllers in the mobility domain must be running the most recent HiPath Wireless Convergence Software release.

8.2 Mobility domain topologies

You can configure a mobility domain in the following scenarios:

- Mobility domain without any availability
- Mobility domain with availability
- Mobility domain with session availability

Note: If you are configuring mobility, you must synchronize time on all the HiPath Wireless Controllers that are part of the mobility domain. For more information, see Section 3.4.11, “Configuring network time”, on page 92.



- HWC1 and HWC2 are configured for session availability.
- HWC1, HWC2, HWC3, Wireless AP1, Wireless AP2 and Wireless AP3 form a Mobility Domain
- HWC3 is the Mobility Manager whereas HWC1 and HWC2 are Mobility Agents

Figure 27 Mobility Domain with fast failover and session availability features

- The user's home session is with HWC1.
- When the user roams from Wireless AP 1 to Wireless AP 2, he establishes his home session with HWC2.
- When the user roams, the Wireless AP 1 receives a notification that the user has roamed away following which it marks the user session as "inactive". Consequently, no statistics are sent to the HWC1 for that user.
- In response to the heart beat message from the mobility manager (HWC3), the HWC2 sends updates that the user has a new home on HWC2. Upon receiving the updates, the mobility manager updates its own tables.

Note: The mobility manager's heart beat time is configurable. If you are configuring a mobility domain with session availability, you should configure the heart beat time as one second to enable the mobility manager to update its tables quickly.

- If a failover takes place, and the user is still associated with Wireless AP1:
  - The Wireless AP 1 fails over, and establishes an active session with HWC2.

    - In response to the heart beat message from the mobility manager (HWC3), the HWC2 sends updates to the mobility manager on the failover Wireless AP and its user.

- If a failover takes place, and the user has roamed to Wireless AP 2:
    - As part of roaming, the user’s home session moves from HWC1 to HWC2.
    - Wireless AP 1 establishes active session with HWC 2. Wireless AP 2 is not impacted by the failover.

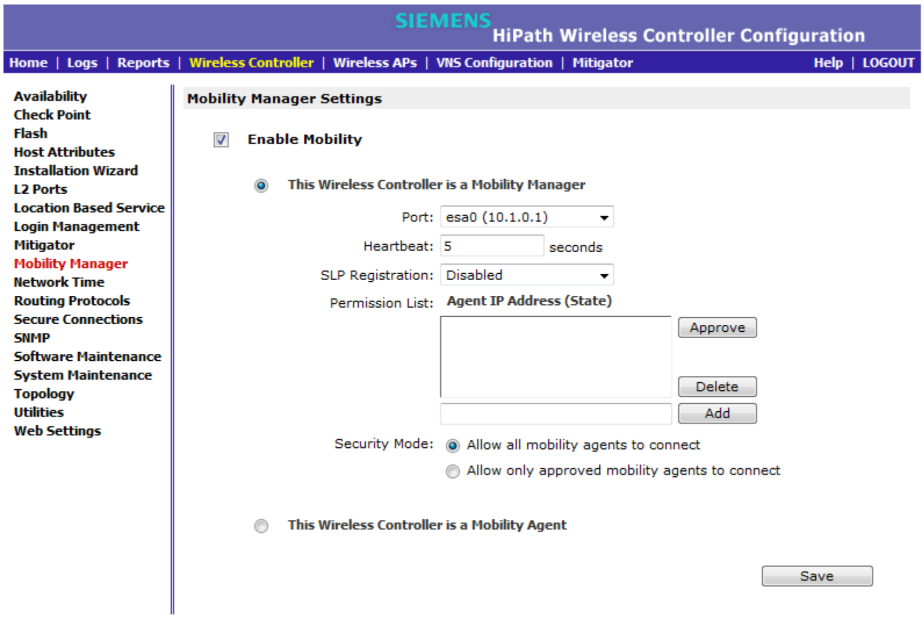
8.3 Configuring mobility domain

If you are configuring a mobility domain with availability or session availability, you must synchronize time on all the HiPath Wireless Controllers that are part of your mobility domain. For more information, see Section 3.4.11, “Configuring network time”, on page 92.

To designate a mobility manager:

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

2. In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.



Mobility Manager Settings

☑ Enable Mobility

● This Wireless Controller is a Mobility Manager

Port: esa0 (10.1.0.1)

Heartbeat: 5 seconds

SLP Registration: Disabled

Permission List: Agent IP Address (State)

Security Mode: ● Allow all mobility agents to connect
○ Allow only approved mobility agents to connect

○ This Wireless Controller is a Mobility Agent

3. To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options are displayed.

4. Select the **This Wireless Controller is a Mobility Manager** option. The mobility manager options are displayed.

5. In the **Port** drop-down list, select the interface on the HiPath Wireless Controller to be used for the mobility manager process. Ensure that the selected interface's IP address is routable on the network.

6. In the **Heartbeat** box, type the time interval (in seconds) at which the mobility manager sends a Heartbeat message to a mobility agent.

   Note: If the mobility domain is configured for fast failover and session availability, you should configure the mobility manager's heart beat time as one second.

7. In the **SLP Registration** drop-down list, select whether to enable or disable SLP registration.

8. In the **Permission** list, select the agent IP addresses you want to approve that are in pending state, by selecting the agent and clicking **Approve**. New agents are only added to the domain if they are approved.

   You can also add or delete controllers that you want to be part of the mobility domain. To add a controller, type the agent IP address in the box, and then click **Add**. To delete a controller, click the controller in the list, and then click **Delete**.

9. Select the **Security Mode** option:

   - **Allow all mobility agents to connect** – All mobility agents can connect to the mobility manager.

   - **Allow only approved mobility agents to connect** – Only approved mobility agents can connect to the mobility manager.

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

Note: If you set up one HiPath Wireless Controller on the network as a mobility manager, all other HiPath Wireless Controllers must be set up as mobility agents.

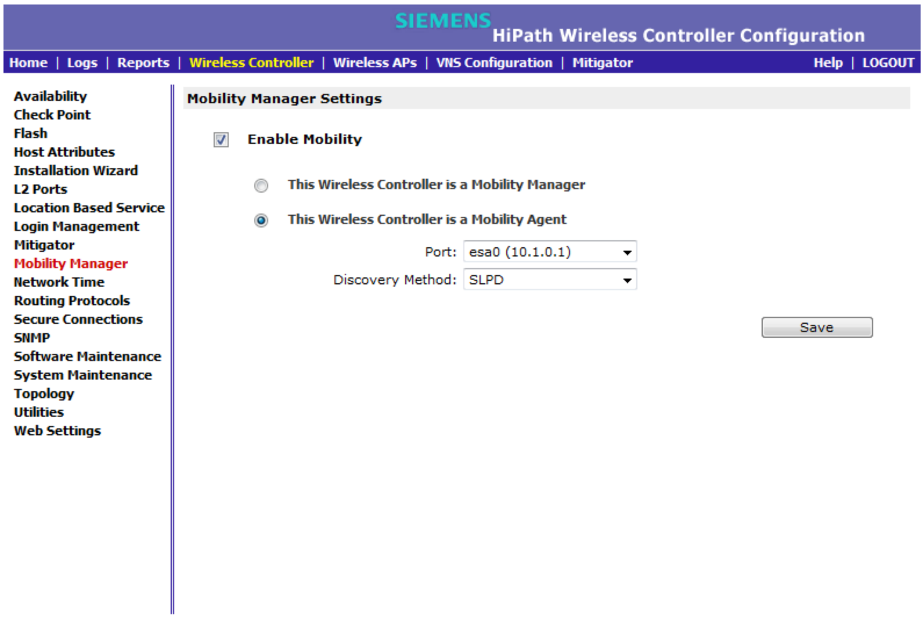
To designate a mobility agent:

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

2. In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.

3. To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options are displayed.

4. Select the **This Wireless Controller is a Mobility Agent** option. The mobility agent options are displayed.



Mobility Manager Settings

☑ Enable Mobility

○ This Wireless Controller is a Mobility Manager

● This Wireless Controller is a Mobility Agent

Port: esa0 (10.1.0.1)

Discovery Method: SLPD

5. From the **Port** drop-down list, select the port on the HiPath Wireless Controller to be used for the mobility agent process. Ensure that the port selected is routable on the network.

6. From the **Discovery Method** drop-down list, select one of the following:

   – **SLPD** – Service Location Protocol Daemon, a background process acting as an SLP server, provides the functionality of the Directory Agent and Service Agent for SLP. Use SLP to support the discovery of siemensNET service to attempt to locate the area mobility manager controller.

   – **Static Configuration** – You must provide the IP address of the mobility manager manually. Defining a static configuration for a mobility manager IP address bypasses SLP discovery.

     In the **Mobility Manager Address** box, type the IP address for the designated mobility manager.

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

For information about viewing mobility manager displays, see Section 11.7, “Viewing displays for the mobility manager”, on page 465.

9 Working with third-party APs

You can set up the HiPath Wireless Controller to handle wireless device traffic from third-party APs, while still providing policy and network access control. This process requires the following steps:

- Define a physical topology to operate in 3rd Party mode.
- Define a WLAN Service of type Third Party AP.
- Define a policy
- Define a VNS

9.1 Define authentication by Captive Portal for the third-party AP WLAN Service:

802.1x Authentication is not supported directly by the HiPath Wireless Controller. However, this type of authentication can be supported by the actual third-party AP. All other options for authentication are supported at the controller.

1. On the WLAN configuration window for the third-party WLAN Service, click the **Auth & Acct** tab.
2. In the **Authentication Mode** drop-down list, click **Internal** or **External**, then click the **Configure** button.
3. Define the Captive Portal configuration as described in Section 6.9.3.7, “Configuring Captive Portal for internal or external authentication”, on page 358.

9.2 Define the third-party APs list

1. In the **WLAN Services** panel, select the third-party WLAN Service.
2. In the **IP Address** field, type the IP address of a third-party AP.
3. In the **Wired MAC Address** field, type the MAC address of the AP.
4. Click the **Add** button to add the AP to the list.
5. Repeat for all third-party APs to be assigned to this WLAN Service.

9.3 Define filtering rules for the third-party APs:

1. Because the third-party APs are mapped to a physical port, you must define the Exception filters on the physical topology, using the **Exception Filters** tab. For more information, see Section 6.8.3, “Exception filtering”, on page 327.
2. Define filtering rules that allow access to other services and protocols on the network such as HTTP, FTP, telnet, SNMP.
3. On the **Multicast Filters** tab, select **Enable Multicast Support** and configure the multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. For more information, see Section 6.8.4, “Multicast filtering”, on page 330.

In addition, modify the following functions on the third-party AP:

- Disable the AP's DHCP server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the HiPath Wireless Controller with VNS information.
- Disable the third-party AP's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

The following are the differences between third-party APs and Wireless APs on the HiPath Wireless Controller, Access Points and Convergence Software system:

- A third-party AP exchanges data with the HiPath Wireless Controller's data port using standard IP over Ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party APs, the VNS is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A HiPath Wireless Controller cannot directly control or manage the configuration of a third-party access point.
- Third-party APs are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other VNS.
- Roaming from third-party APs to Wireless APs and vice versa is not supported.

10 Working with the Mitigator

This chapter describes Mitigator concepts, including:

10.1 Mitigator overview

The Mitigator is a mechanism that assists in the detection of rogue APs.

Mitigator functionality on the Wireless AP does the following:

- Runs a radio frequency (RF) scanning task.
- Alternating between scan functions, providing its regular service to the wireless devices on the network.

Note: If a Wireless AP is part of a WDS link you cannot configure it to act as a scanner in Mitigator.

Mitigator functionality on the HiPath Wireless Controller does the following:

- Runs a data collector application that receives and manages the RF scan messages sent by the Wireless AP. RF data collector data includes lists of all connected Wireless APs, third-party APs, and the RF scan information that has been collected from the Wireless APs selected to perform the scan.
- Runs an Analysis Engine that processes the scan data from the data collector through algorithms that make decisions about whether any of the detected APs or clients are rogue APs or are running in an unsecure environment (for example, ad-hoc mode).

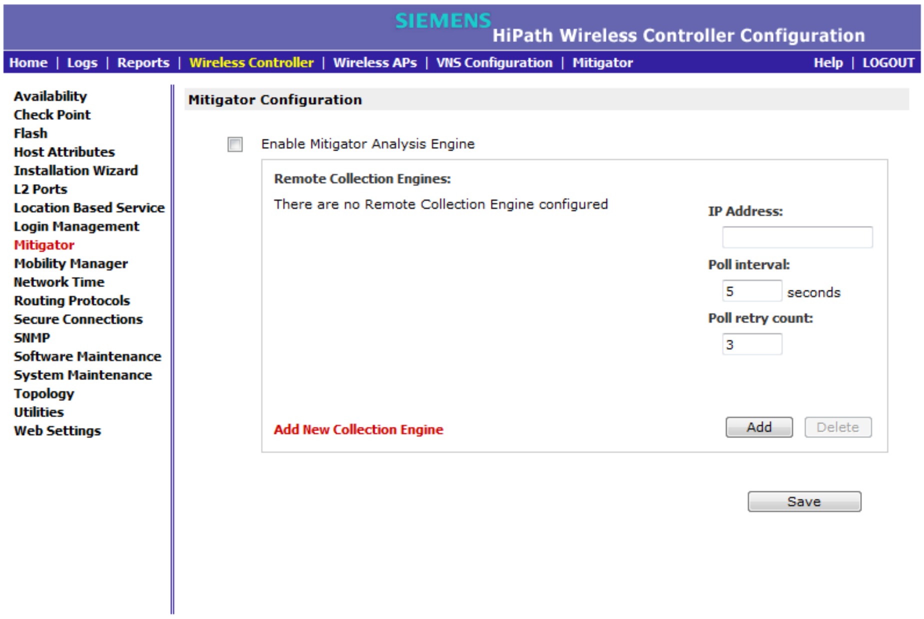
  Note: In a network with more than one HiPath Wireless Controller, it is not necessary for the data collector to be running on the same controller as the Analysis Engine. One controller can be a dedicated Analysis Engine while the other controllers run data collector functionality. No more than one Analysis Engine can be running at a time. You must ensure that the controllers are all routable.

10.2 Enabling the Analysis and data collector engines

Before using the Mitigator, you must enable and define the Analysis and data collector engines.

To enable the Analysis engine:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Mitigator**. The **Mitigator Configuration** screen is displayed.



Mitigator Configuration

□ Enable Mitigator Analysis Engine

Remote Collection Engines:

There are no Remote Collection Engine configured

IP Address:

Poll interval: 5 seconds

Poll retry count: 3

Add New Collection Engine

3. To enable the Mitigator Analysis Engine, select the **Enable Mitigator Analysis Engine** checkbox.
4. To identify the remote RF Data Collector Engine that the Analysis Engine will poll for data, type the IP address of the HiPath Wireless Controller on which the remote Data Collector resides in the **IP Address** box.

Note: Currently, the HiPath Wireless Controller C20N/C20 does not support the Remote Collection Engines functionality of the HiPath Wireless Controller, Access Points and Convergence Software solution.

5. Set the following for the data collection engine:
   - In the **Poll interval** box, type (in seconds) the interval that the Analysis Engine will poll the RF Data Collector to maintain connection status. The default is **30** seconds.
   - In the **Poll retry count** box, type the number of times the Analysis Engine will attempt to poll the RF Data Collector to maintain connection status, before it stops sending requests. The default is **2** attempts.
6. Click **Add**. The IP address of the Data Collection Engine, with its Poll Interval and Poll Retry parameters, is displayed in the list.

Note: For each remote RF Data Collection Engine defined here, you must do the following:

• Enable it by selecting the **Enable Mitigator Analysis Engine** checkbox on the remote HiPath Wireless Controller.
• Ensure that the controllers are routable by whatever means you use (for example, static routes or OSPF).

7. To add a new collection engine, click **Add Collection Engine**.
8. Repeat steps 4 to 7.
9. To save your changes, click **Apply**.

10.3 Running Mitigator scans

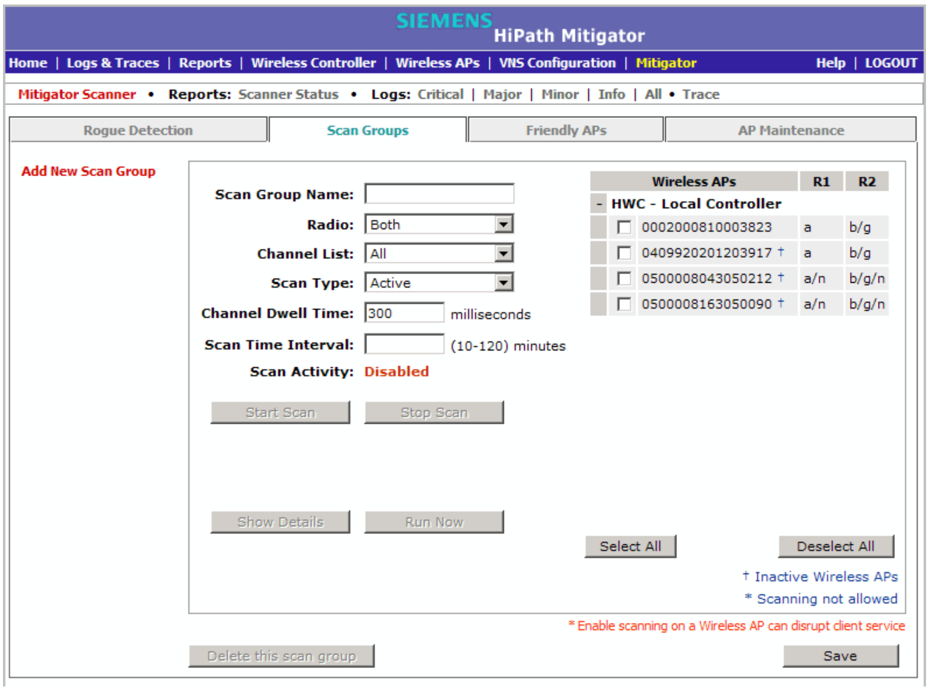
The Mitigator feature allows you to view the following:

- Scan Groups
- Friendly APs
- AP Maintenance

Note: A scan will not run on an inactive AP, even though it is displayed as part of the Scan Group. If it becomes active, it will be sent a scan request during the next periodic scan.

To run the Mitigator scan task mechanism:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Scan Groups** tab.


SIEMENS
HiPath Mitigator
Home | Logs & Traces | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly APs
AP Maintenance
Add New Scan Group
Start Scan
Stop Scan
Show Details
Run Now
Select All
Deselect All
Delete this scan group
Save

Scan Group Name:
Radio: Both
Channel List: All
Scan Type: Active
Channel Dwell Time: 300 milliseconds
Scan Time Interval: (10-120) minutes
Scan Activity: Disabled

Wireless APs	R1	R2
- HWC - Local Controller		
□ 0002000810003823	a	b/g
□ 0409920201203917 †	a	b/g
□ 0500008043050212 †	a/n	b/g/n
□ 0500008163050090 †	a/n	b/g/n

† Inactive Wireless APs
* Scanning not allowed
* Enable scanning on a Wireless AP can disrupt client service

3. In the **Scan Group Name** box, type a unique name for this scan group.

4. In the **Wireless APs** list, select the checkbox corresponding to the Wireless APs you want included in the new scan group, which will perform the scan function.

Note: A Wireless AP can participate in only one Scan Group at a time. Siemens recommends that the Scan Groups represent geographical groupings of Wireless APs.

5. In the **Radio** drop-down list, click one of the following:
   - **Both** – Radio 1 and Radio 2 both perform the scan function.
   - **radio 1** – Only Radio 1 performs the scan function.
   - **radio 2** – Only Radio 2 performs the scan function.
6. In the **Channel List** drop-down list, click one of the following:
   - **All** – Scanning is performed on all channels.
   - **Current** – Scanning is performed on only the current channel.
7. In the **Scan Type** drop-down list, click one of the following:
   - **Active** – The Wireless AP sends out ProbeRequests and waits for ProbeResponse messages from any access points.
   - **Passive** – The Wireless AP listens for 802.11 beacons.
8. In the **Channel Dwell Time** box, type the time (in milliseconds) for the scanner to wait for a response from either 802.11 beacons in passive scanning, or ProbeResponse in active scanning.
9. In the **Scan Time Interval** box, type the time (in minutes) to define the frequency at which a Wireless AP within the Scan Group will initiate a scan of the RF space. The range is from one minute to 120 minutes.
10. To initiate a scan using the periodic scanning parameters defined above, click **Start Scan**.
11. To initiate an immediate scan that will run only once, click **Run Now.**

Note: If necessary, you can stop a scan by clicking **Stop Scan**.
A scan must be stopped before modifying any parameters of the Scan Group, or before adding or removing a Wireless AP from a Scan Group.

The **Scan Activity** box displays the current state of the scan engine.

12. To view a pop-up report displaying the timeline of scan activity and scan results, click **Show Details**.
13. To save your changes, click **Save**.

10.4 Analysis engine overview

The Analysis engine relies on a database of known devices on the Controller, Access Points and Convergence Software system. The Analysis engine compares the data from the RF Data Collector with the database of known devices.

This database includes the following:

- **Wireless APs** – Registered with any HiPath Wireless Controller with its RF Data Collector enabled and associated with the Analysis Engine on this HiPath Wireless Controller.
- **Third-party APs** – Defined and assigned to a VNS.
- **Friendly APs** – A list created in the Mitigator user interface as potential rogue access points are designated by the administrator as Friendly.
- **Wireless devices** – Registered with any HiPath Wireless Controller that has its RF Data Collector enabled and has been associated with the Analysis Engine on this HiPath Wireless Controller.

The Analysis Engine looks for access points with one or more of the following conditions:

- **Unknown MAC address and unknown SSID** (critical alarm)
- **Unknown MAC, with a valid SSID** - a known SSID is being broadcast by the unknown access point (critical alarm)
- **Known MAC, with an unknown SSID** - a rogue may be spoofing a MAC address (critical alarm)
- **Inactive Wireless AP with valid SSID** (critical alarm)
- **Inactive Wireless AP with unknown SSID** (critical alarm)
- **Known Wireless AP with an unknown SSID** (major alarm)
- **In ad-hoc mode** (major alarm)

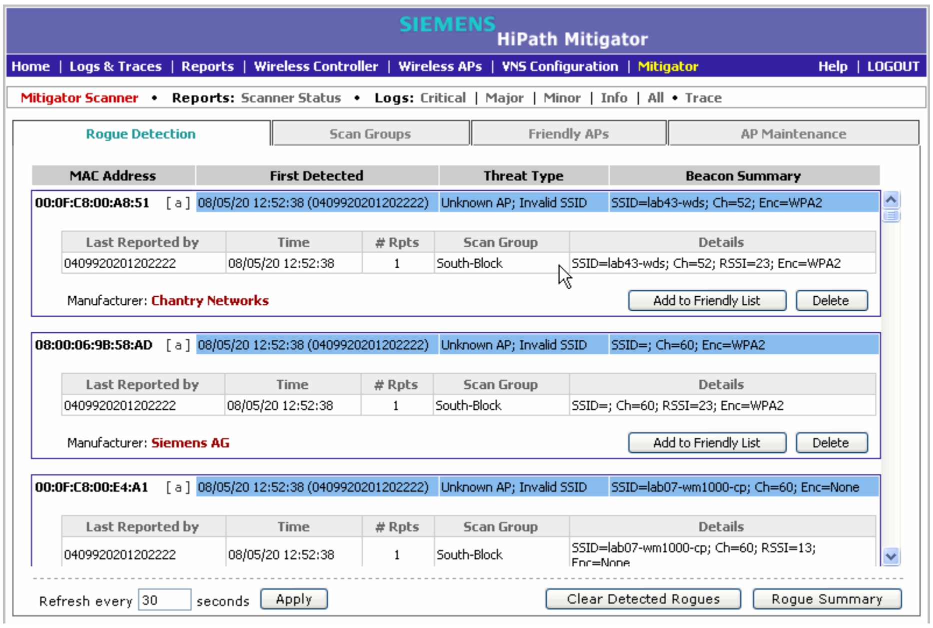
Note: In the current release, there is no capability to initiate a DoS attack on the detected rogue access point. Containment of a detected rogue requires an inspection of the geographical location of its Scan Group area, where its RF activity has been found.

10.5 Working with Mitigator scan results

When viewing the Mitigator scan results, you can delete individual or all of the access points from the scan results. You can also add access points from the scan results to the **Friendly AP** list.

To view Mitigator scan results:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Rogue Detection** tab.
3. To modify the page's refresh rate, type a time (in seconds) in the **Refresh every __ seconds** box.
4. Click **Apply**. The new refresh rate is applied.


SIEMENS
HiPath Mitigator
Home | Logs & Traces | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly APs
AP Maintenance

MAC Address		First Detected	Threat Type	Beacon Summary
00:0F:C8:00:A8:51	[a]	08/05/20 12:52:38 (0409920201202222)	Unknown AP; Invalid SSID	SSID=lab43-wds; Ch=52; Enc=WPA2

Last Reported by	Time	# Rpts	Scan Group	Details
0409920201202222	08/05/20 12:52:38	1	South-Block	SSID=lab43-wds; Ch=52; RSSI=23; Enc=WPA2

Manufacturer: Chantry Networks

Add to Friendly List
Delete

MAC Address		First Detected	Threat Type	Beacon Summary
08:00:06:9B:58:AD	[a]	08/05/20 12:52:38 (0409920201202222)	Unknown AP; Invalid SSID	SSID=; Ch=60; Enc=WPA2

Last Reported by	Time	# Rpts	Scan Group	Details
0409920201202222	08/05/20 12:52:38	1	South-Block	SSID=; Ch=60; RSSI=23; Enc=WPA2

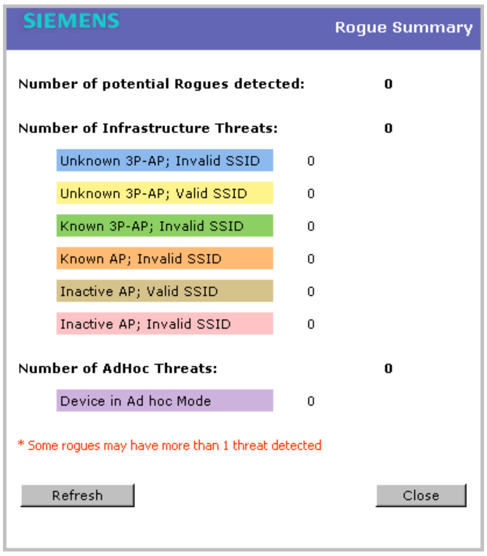
Manufacturer: Siemens AG

MAC Address		First Detected	Threat Type	Beacon Summary
00:0F:C8:00:E4:A1	[a]	08/05/20 12:52:38 (0409920201202222)	Unknown AP; Invalid SSID	SSID=lab07-wm1000-cp; Ch=60; Enc=None

Last Reported by	Time	# Rpts	Scan Group	Details
0409920201202222	08/05/20 12:52:38	1	South-Block	SSID=lab07-wm1000-cp; Ch=60; RSSI=13; Enc=None

Refresh every 30 seconds

5. To view the Rogue Summary report, click **Rogue Summary**. The Rogue Summary report is displayed in a pop-up window.



Number of potential Rogues detected:	0
Number of Infrastructure Threats:	0
Unknown 3P-AP; Invalid SSID	0
Unknown 3P-AP; Valid SSID	0
Known 3P-AP; Invalid SSID	0
Known AP; Invalid SSID	0
Inactive AP; Valid SSID	0
Inactive AP; Invalid SSID	0
Number of AdHoc Threats:	0
Device in Ad hoc Mode	0

* Some rogues may have more than 1 threat detected

6. To clear all detected rogue devices from the list, click **Clear Detected Rogues**.

Note: To avoid the Mitigator's database becoming too large, Siemens recommends that you either delete Rogue APs or add them to the **Friendly APs** list, rather than leaving them in the **Rogue** list.

To add an AP from the Mitigator scan results to the list of friendly APs:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Rogue Detection** tab.
3. To add a Wireless AP to the **Friendly APs** list, click **Add to Friendly List**. The AP is removed from this list and is displayed in the **Friendly AP Definitions** section of the **Friendly AP's** tab.

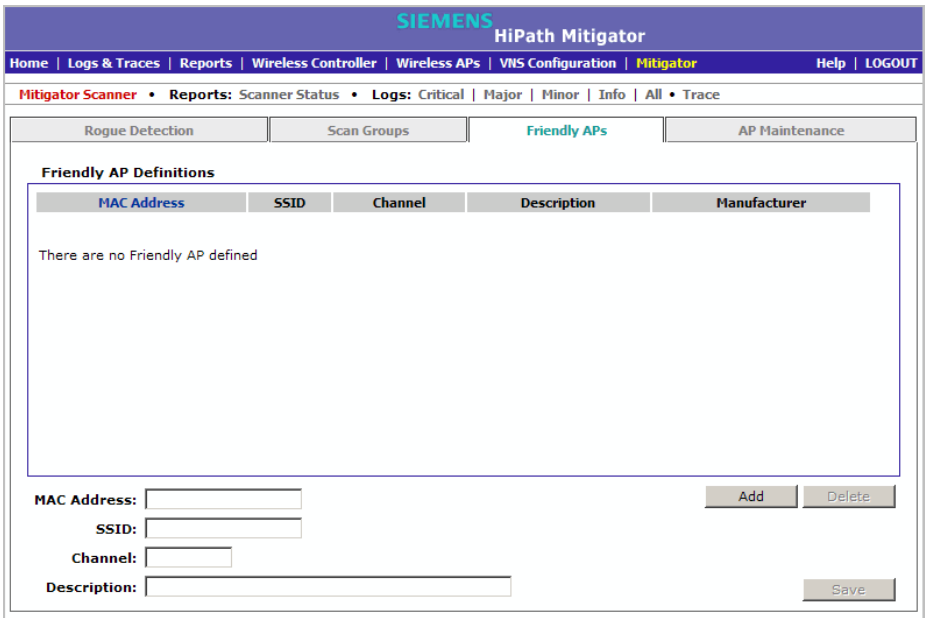
To delete an AP from the Mitigator scan results:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Rogue Detection** tab.
3. To delete a specific AP from the Mitigator scan results, click the corresponding **Delete** button. The AP is removed from the list.
4. To clear all rogue access points from the Mitigator scan results, click **Clear Detected Rogues**. All APs are removed from the list.

10.6 Working with friendly APs

To view the friendly APs:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Friendly APs** tab.


SIEMENS
HiPath Mitigator
Home | Logs & Traces | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly APs
AP Maintenance
Add
Delete
Save

Friendly AP Definitions

MAC Address	SSID	Channel	Description	Manufacturer

There are no Friendly AP defined

MAC Address:
SSID:
Channel:
Description:

To add friendly APs manually:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Friendly APs** tab.
3. To add friendly access points manually to the **Friendly AP Definitions** list, type the following:
   - **MAC Address** – Specifies the MAC address for the friendly AP
   - **SSID** – Specifies the SSID for the friendly AP
   - **Channel** – Specifies the current operating channel for the friendly AP
   - **Description** – Specifies a brief description for the friendly AP
4. Click **Add**. The new access point is displayed in the list above.

To delete a friendly AP:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Friendly APs** tab.
3. In the **Friendly AP Definitions** list, click the access point you want to delete.

4. Click **Delete**. The selected access point is removed from the **Friendly AP Definitions** list.

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

To modify a friendly AP:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.

2. Click the **Friendly APs** tab.

3. In the **Friendly AP Definitions** list, click the access point you want to modify.

4. Modify the access point by making the appropriate changes.

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

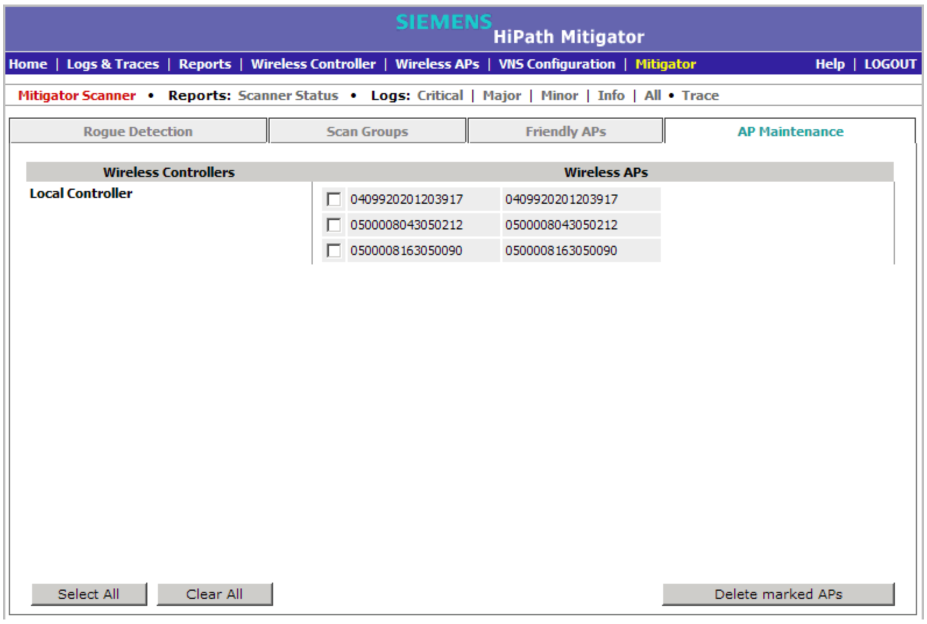
10.7 Maintaining the Mitigator list of APs

To maintain the Wireless APs:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.

2. Click the **AP Maintenance** tab. Inactive APs and known third-party APs are displayed.

3. Select the applicable APs.



SIEMENS
HiPath Mitigator
Home | Logs & Traces | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly APs
AP Maintenance
Select All
Clear All
Delete marked APs

Wireless Controllers	Wireless APs	
Local Controller	□ 0409920201203917	0409920201203917
	□ 0500008043050212	0500008043050212
	□ 0500008163050090	0500008163050090

4. To delete the selected APs, click **Delete marked APs**.

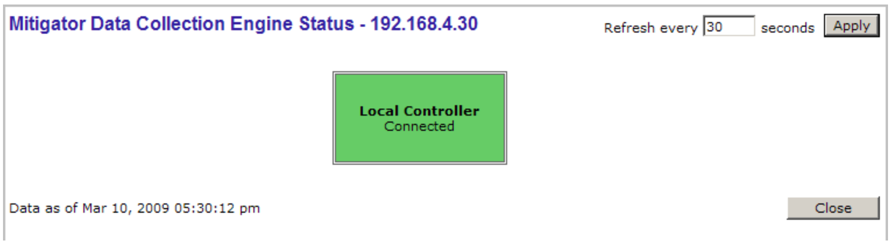
Note: The selected APs are deleted from the Mitigator database, not from the HiPath Wireless Controller database. You can delete the APs from the HiPath Wireless Controller database after you delete them from the Wireless AP Configuration **Access Approval** screen of the corresponding RF Data Collector Engine. You can also delete the selected third-party APs if they are removed from the corresponding VNS in the RF Collector Engine, or if that VNS has been deleted from the VNS list.

10.8 Viewing the Scanner Status report

When the Mitigator is enabled, you can view a report on the connection status of the RF Data Collector Engines with the Analysis Engine.

To view the Mitigator scanner engine status display:

1. From the main menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Reports: Scanner Status**. The Scanner Status report is displayed.



Mitigator Data Collection Engine Status - 192.168.4.30

Refresh every 30 seconds

Local Controller
Connected

Data as of Mar 10, 2009 05:30:12 pm

The boxes display the IP address of the Data Collector engine. The status of the Data Collector engine is indicated by one of the following colors:

- **Green** – The Analysis Engine has connection with the Data Collector on that HiPath Wireless Controller.
- **Yellow** – The Analysis Engine has connected to the communication system of the other controller, but has not synchronized with the Data Collector. Ensure that the Data Collector is running on the remote controller.
- **Red** – The Analysis Engine is aware of the Data Collector and attempting connection.

If no box is displayed, the Analysis Engine is not attempting to connect with that Data Collector Engine.

Note: If the box is displayed red and remains red, ensure your IP address is correctly set up to point to an active controller. If the box remains yellow, ensure the Data Collector is running on the remote controller.

11 Working with reports and displays

This chapter describes the various reports and displays available in the HiPath Wireless Controller, Access Points and Convergence Software system.

11.1 Available reports and displays

The following displays are available in the HiPath Wireless Controller, Access Points and Convergence Software system:

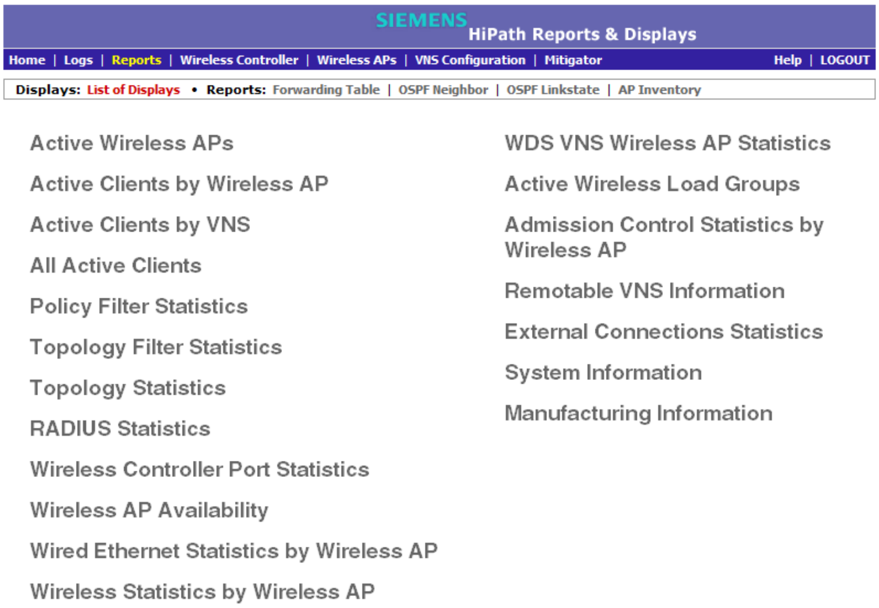
- Active Wireless APs
- Active Clients by Wireless AP
- Active Clients by VNS
- All Active Clients
- Active Wireless Load Groups
- Policy Filter Statistics
- Topology Filter Statistics
- Topology Statistics
- RADIUS Statistics
- Wireless Controller Port Statistics
- Wireless AP Availability
- Wired Ethernet Statistics by Wireless AP
- Wireless Statistics by Wireless AP
- Admission Control Statistics by Wireless AP
- Client Location in Mobility Zone
- Mobility Tunnel Matrix
- WDS VNS Wireless AP Statistics
- External Connections Statistics
- Remoteable VNS Information
- System Information
- Manufacturing Information

Note: The **Client Location in Mobility Zone** and **Mobility Tunnel Matrix** displays only appear if you have enabled the mobility manager function for the controller. Otherwise, the **Agent Mobility Tunnel Matrix** display is listed.

11.2 Viewing reports and displays

To view reports and displays:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.


SIEMENS
HiPath Reports & Displays
Home | Logs | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | AP Inventory

Active Wireless APs

Active Clients by Wireless AP

Active Clients by VNS

All Active Clients

Policy Filter Statistics

Topology Filter Statistics

Topology Statistics

RADIUS Statistics

Wireless Controller Port Statistics

Wireless AP Availability

Wired Ethernet Statistics by Wireless AP

Wireless Statistics by Wireless AP

WDS VNS Wireless AP Statistics

Active Wireless Load Groups

Admission Control Statistics by Wireless AP

Remotable VNS Information

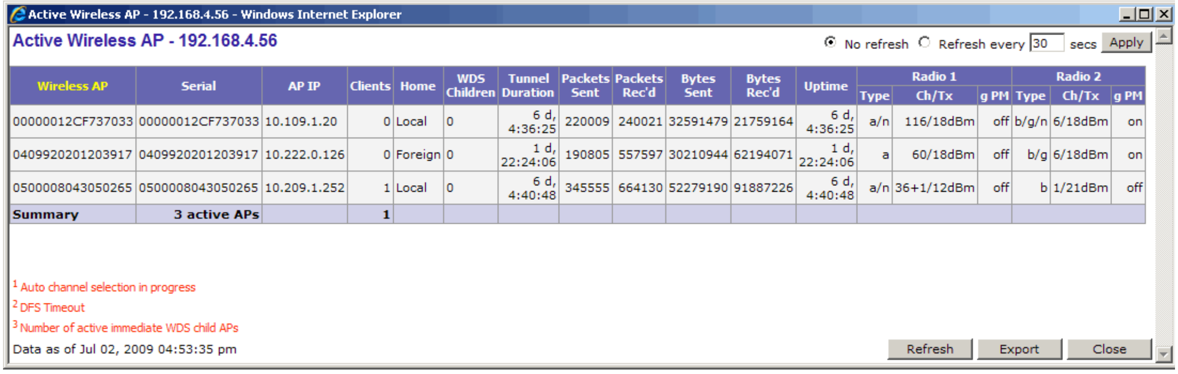
External Connections Statistics

System Information

Manufacturing Information

Note: The **Client Location in Mobility Zone** and **Mobility Tunnel Matrix** displays only appear if you have enabled the mobility manager function for the controller.

2. In the **List of Displays**, click the display you want to view.


Active Wireless AP - 192.168.4.56 - Windows Internet Explorer
Apply
Refresh
Export
Close

Active Wireless AP - 192.168.4.56

● No refresh ○ Refresh every 30 secs

Wireless AP	Serial	AP IP	Clients	Home	WDS Children	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	Radio 1			Radio 2		
												Type	Ch/Tx	g PM	Type	Ch/Tx	g PM
00000012CF737033	00000012CF737033	10.109.1.20	0	Local	0	6 d, 4:36:25	220009	240021	32591479	21759164	6 d, 4:36:25	a/n	116/18dBm	off	b/g/n	6/18dBm	on
0409920201203917	0409920201203917	10.222.0.126	0	Foreign	0	1 d, 22:24:06	190805	557597	30210944	62194071	1 d, 22:24:06	a	60/18dBm	off	b/g	6/18dBm	on
0500008043050265	0500008043050265	10.209.1.252	1	Local	0	6 d, 4:40:48	345555	664130	52279190	91887226	6 d, 4:40:48	a/n	36+1/12dBm	off	b	1/21dBm	off
Summary	**3 active APs**		**1**														

[1] Auto channel selection in progress

[2] DFS Timeout

[3] Number of active immediate WDS child APs

Data as of Jul 02, 2009 04:53:35 pm

Note: Statistics are expressed in respect to the AP. Therefore, **Packets Sent** indicates the packets the AP has sent to a client and **Packets Rec'd** indicates the packets the AP has received from a client.

11.3 Viewing the Wireless AP availability display

In session availability, the Wireless Availability report displays the state of both the tunnels — active tunnel and backup tunnel — on both the primary and secondary HiPath Wireless Controllers.

The report uses the **Color Legend** to indicate the tunnel state:

- **Green** – Wireless AP has established an active tunnel.
- **Blue** – Wireless AP has established a backup tunnel.
- **Red** – Wireless AP is not connected.

In the report, each Wireless AP is represented by a box.

- The label, **Foreign** or **Local**, indicates whether the Wireless AP is local or foreign on the HiPath Wireless Controller.
- The color in the upper pane of the box represents the state of the tunnel that is established to the current HiPath Wireless Controller.

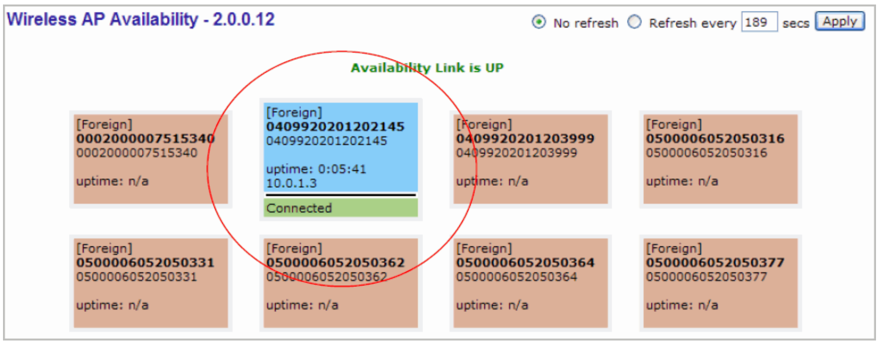
Note: The current HiPath Wireless Controller is the one on which the Wireless AP Availability report is viewed.

- The color in the lower pane of the box represents the state of the tunnel that is established with the other HiPath Wireless Controller.

For the ease of understanding, take the example of the following scenario:

- HWC1 and HWC2 are paired in session availability
- A Wireless AP has established an active tunnel to HWC1.
- The same Wireless AP has established a backup tunnel to HWC2.

If you open the Wireless AP Availability report on HWC2, the report will appear as follows:



Wireless AP Availability - 2.0.0.12

● No refresh ○ Refresh every 189 secs Apply

Availability Link is UP

[Foreign]
0002000007515340
0002000007515340
uptime: n/a

[Foreign]
0409920201202145
0409920201202145
uptime: 0:05:41
10.0.1.3
Connected

[Foreign]
0409920201203999
0409920201203999
uptime: n/a

[Foreign]
0500006052050316
0500006052050316
uptime: n/a

[Foreign]
0500006052050331
0500006052050331
uptime: n/a

[Foreign]
0500006052050362
0500006052050362
uptime: n/a

[Foreign]
0500006052050364
0500006052050364
uptime: n/a

[Foreign]
0500006052050377
0500006052050377
uptime: n/a

In the above example, the circled Wireless AP has established a backup tunnel to the foreign (secondary) HiPath Wireless Controller, and an active tunnel to the local (Primary) HiPath Wireless Controller.

11.4 Viewing statistics for Wireless APs

Several displays are snapshots of activity at that point in time on a selected Wireless AP:

- Wired Ethernet Statistics by Wireless AP
- Wireless Statistics by Wireless AP
- Active Clients by Wireless AP
- WDS VNS Wireless AP Statistics
- Admission Control Statistics by Wireless AP

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

The following Wireless AP displays allow you to search for clients, either by user name, MAC address, or IP address that are associated to the Wireless APs.

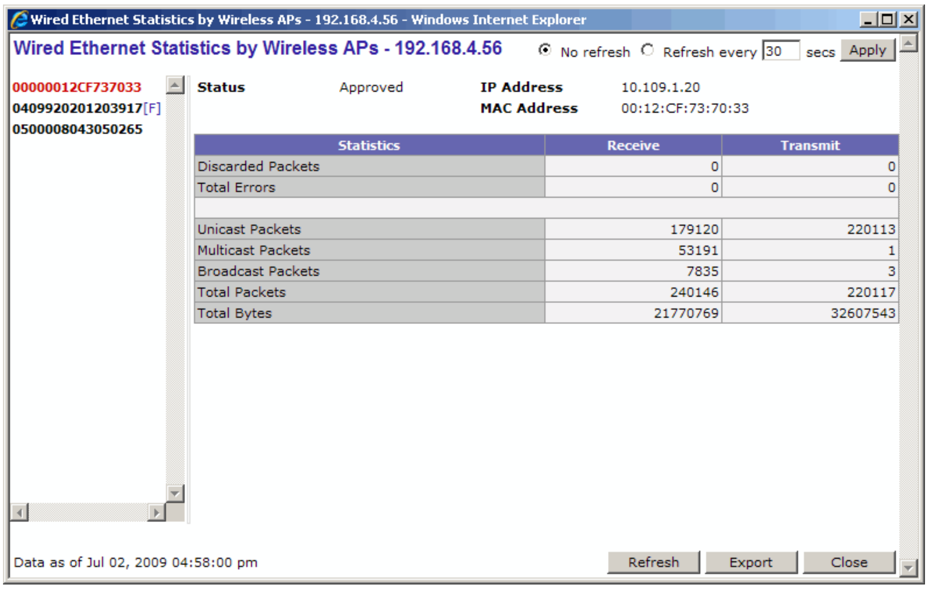
- Active Clients by Wireless AP
- Active Clients by VNS
- Admission Control Statistics by Wireless AP
- All Active Clients

You can also use the **Select All** and **Deselect All** buttons for selecting the Wireless AP on those displays.

To view wired Ethernet statistics by Wireless AP:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.

2. Click the **Wired Ethernet Statistics by Wireless AP** display option. The **Wired Ethernet Statistics by Wireless APs** display opens in a new browser window.



Wired Ethernet Statistics by Wireless APs - 192.168.4.56 - Windows Internet Explorer

Wired Ethernet Statistics by Wireless APs - 192.168.4.56

● No refresh ○ Refresh every 30 secs

00000012CF737033
0409920201203917[F]
0500008043050265

Status Approved
IP Address 10.109.1.20
MAC Address 00:12:CF:73:70:33

Statistics	Receive	Transmit
Discarded Packets	0	0
Total Errors	0	0
Unicast Packets	179120	220113
Multicast Packets	53191	1
Broadcast Packets	7835	3
Total Packets	240146	220117
Total Bytes	21770769	32607543

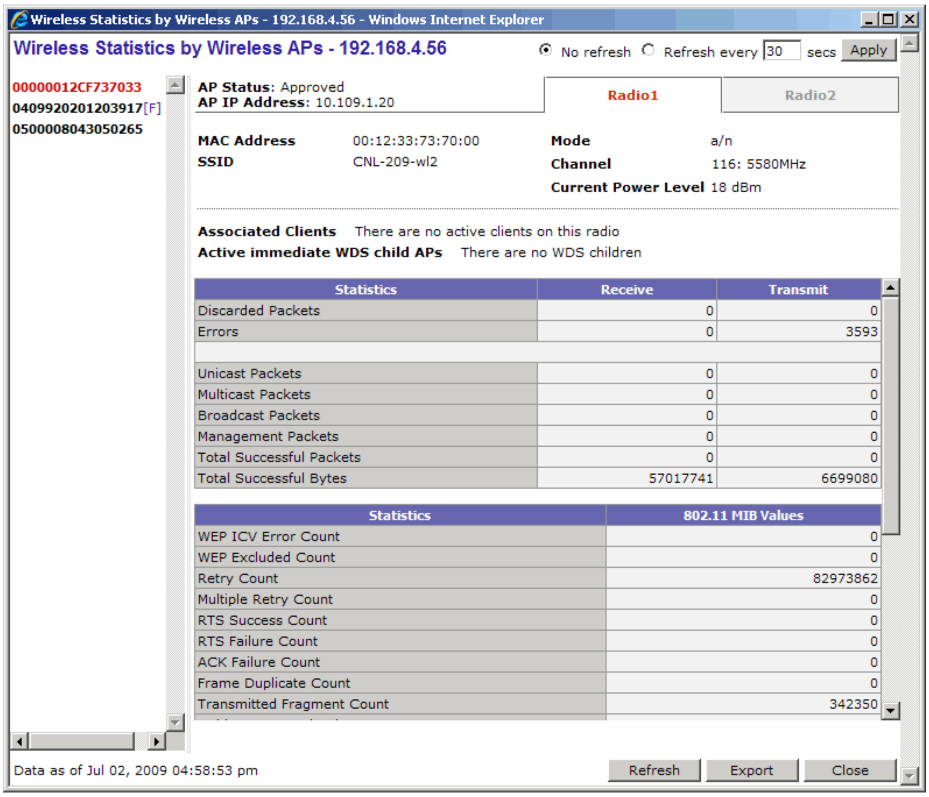
Data as of Jul 02, 2009 04:58:00 pm

3. In the **Wired Ethernet Statistics by Wireless APs** display, click a registered Wireless AP to display its information.

To view Wireless Statistics by Wireless AP:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.

2. Click the **Wireless Statistics by Wireless AP** display option. The **Wireless Statistics by Wireless APs** display opens in a new browser window.



Wireless Statistics by Wireless APs - 192.168.4.56 - Windows Internet Explorer

Wireless Statistics by Wireless APs - 192.168.4.56

● No refresh ○ Refresh every 30 secs Apply

00000012CF737033
0409920201203917[F]
0500008043050265

AP Status: Approved
AP IP Address: 10.109.1.20

Radio1 | Radio2

MAC Address	00:12:33:73:70:00	**Mode**	a/n
SSID	CNL-209-wl2	**Channel**	116: 5580MHz
		Current Power Level	18 dBm

Associated Clients There are no active clients on this radio
Active immediate WDS child APs There are no WDS children

Statistics	Receive	Transmit
Discarded Packets	0	0
Errors	0	3593
Unicast Packets	0	0
Multicast Packets	0	0
Broadcast Packets	0	0
Management Packets	0	0
Total Successful Packets	0	0
Total Successful Bytes	57017741	6699080

Statistics	802.11 MIB Values
WEP ICV Error Count	0
WEP Excluded Count	0
Retry Count	82973862
Multiple Retry Count	0
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	0
Frame Duplicate Count	0
Transmitted Fragment Count	342350

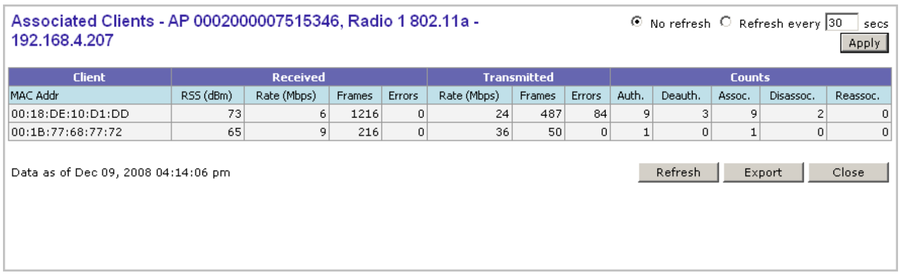
Data as of Jul 02, 2009 04:58:53 pm

Refresh Export Close

3. In the **Wireless Statistics by Wireless APs** display, click a registered Wireless AP to display its information.

4. Click the appropriate tab to display information for each Radio on the Wireless AP.

5. To view information on the associated clients, click **View Clients**. The **Associated Clients** display opens in a new browser window.



Associated Clients - AP 0002000007515346, Radio 1 802.11a - 192.168.4.207

● No refresh ○ Refresh every 30 secs Apply

Client	Received				Transmitted			Counts				
MAC Addr	RSS (dBm)	Rate (Mbps)	Frames	Errors	Rate (Mbps)	Frames	Errors	Auth.	Deauth.	Assoc.	Disassoc.	Reassoc.
00:18:DE:10:D1:DD	73	6	1216	0	24	487	84	9	3	9	2	0
00:1B:77:68:77:72	65	9	216	0	36	50	0	1	0	1	0	0

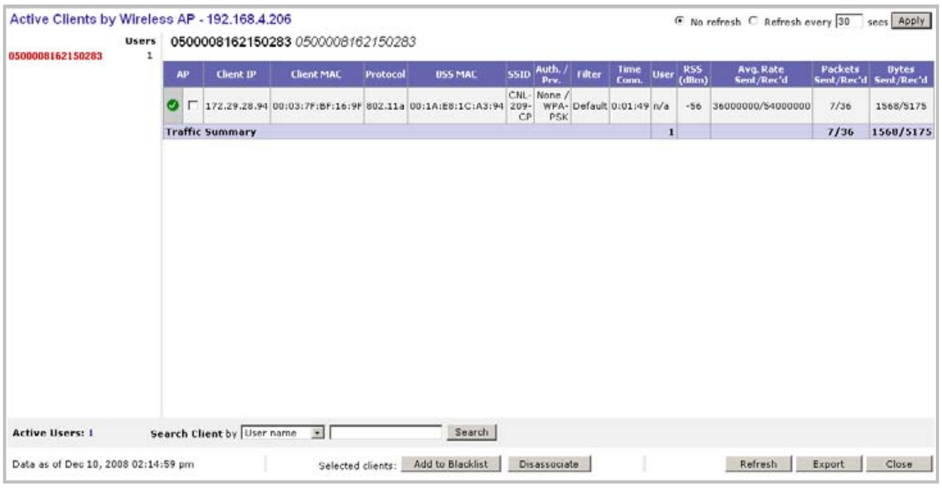
Data as of Dec 09, 2008 04:14:06 pm

Refresh Export Close

To view Active Clients by Wireless AP statistics:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.

2. Click the **Active Clients by Wireless APs** display option. The **Active Clients by Wireless APs** display opens in a new browser window.



Active Clients by Wireless AP - 192.168.4.206

● No refresh ○ Refresh every 30 secs Apply

Users

0500008162150283 1

0500008162150283 *0500008162150283*

AP		Client IP	Client MAC	Protocol	BSS MAC	SSID	Auth. / Prv.	Filter	Time Conn.	User	RSS (dBm)	Avg. Rate Sent/Rec'd	Packets Sent/Rec'd	Bytes Sent/Rec'd
✓	□	172.29.28.94	00:03:7F:BF:16:9F	802.11a	00:1A:E8:1C:A3:94	CNL-209-CP	None / WPA-PSK	Default	0:01:49	n/a	-56	36000000/54000000	7/36	1568/5175
Traffic Summary										1			7/36	1568/5175

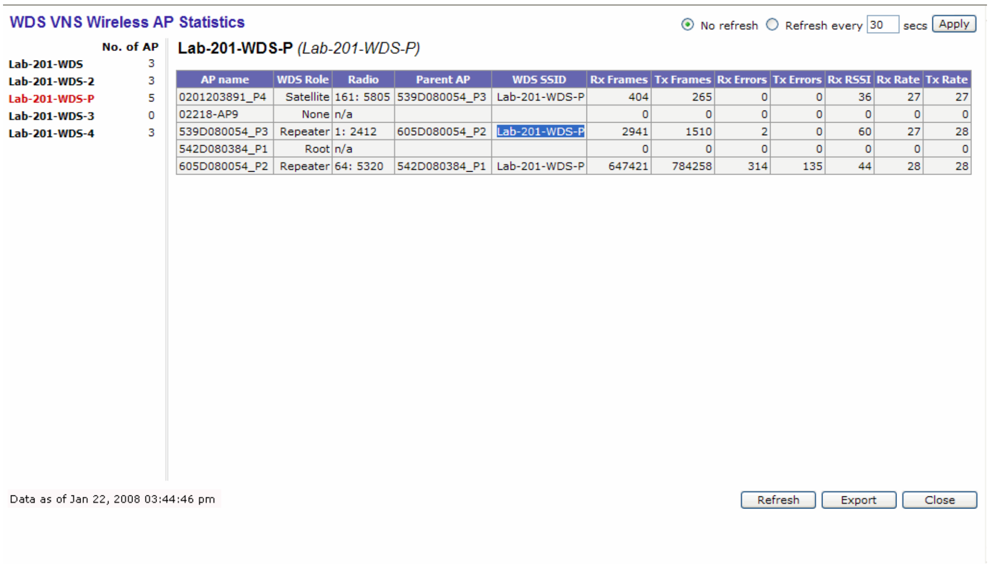
Active Users: 1 Search Client by User name ▾ Search

Data as of Dec 10, 2008 02:14:59 pm Selected clients: Add to Blacklist Disassociate Refresh Export Close

- Statistics are expressed in respect to the AP. Therefore, **Packets Sent** indicates the packets the AP has sent to a client and **Packets Rec’d** indicates the packets the AP has received from a client.
- The green check mark icon in the first column indicates that the client is authenticated.
- **Time Conn** is the time that a client has been on the system, not just on an AP. If the client roams from one AP to another, the session stays, therefore **Time Conn** does not reset.
- A client is displayed as soon as the client connects (or after a refresh of the screen). The client disappears as soon as it times out.
- The **RSS** (received signal strength) of a client is the average of the transmitted and received RSS on hardware platforms where both values are available.

To view WDS VNS Wireless AP Statistics:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.
2. Click the **WDS Wireless AP Statistics** display option. The **WDS VNS Wireless AP Statistics** display opens in a new browser window.



WDS VNS Wireless AP Statistics

● No refresh ○ Refresh every 30 secs Apply

	No. of AP
Lab-201-WDS	3
Lab-201-WDS-2	3
Lab-201-WDS-P	5
Lab-201-WDS-3	0
Lab-201-WDS-4	3

Lab-201-WDS-P *(Lab-201-WDS-P)*

AP name	WDS Role	Radio	Parent AP	WDS SSID	Rx Frames	Tx Frames	Rx Errors	Tx Errors	Rx RSSI	Rx Rate	Tx Rate
0201203891_P4	Satellite	161: 5805	539D080054_P3	Lab-201-WDS-P	404	265	0	0	36	27	27
02218-AP9	None	n/a			0	0	0	0	0	0	0
539D080054_P3	Repeater	1: 2412	605D080054_P2	Lab-201-WDS-P	2941	1510	2	0	60	27	28
542D080384_P1	Root	n/a			0	0	0	0	0	0	0
605D080054_P2	Repeater	64: 5320	542D080384_P1	Lab-201-WDS-P	647421	784258	314	135	44	28	28

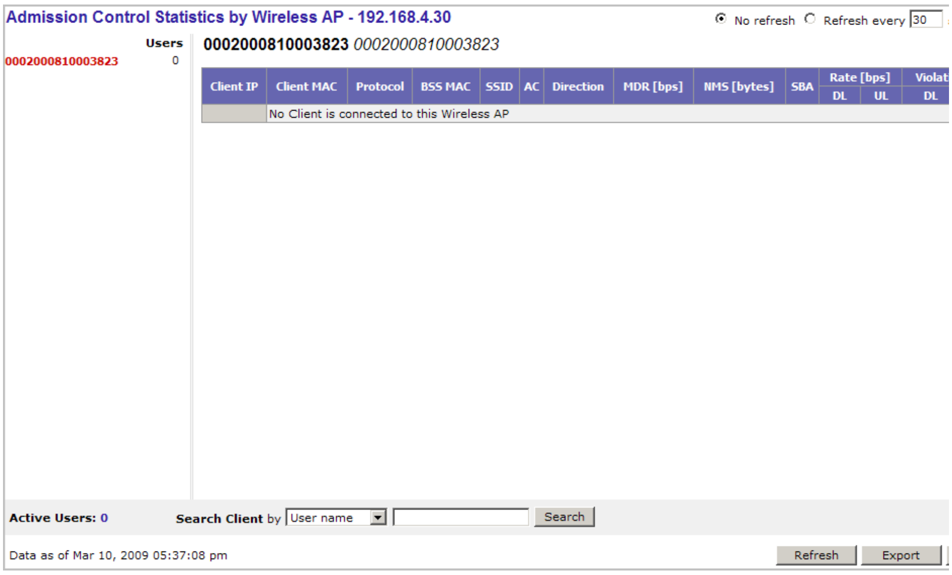
Data as of Jan 22, 2008 03:44:46 pm

Note: The **Rx RSSI** value on the **WDS VNS Wireless AP Statistics** display represents the received signal strength (in dBm).

To view Admission Control Statistics by Wireless AP:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.

2. Click the **Admission Control Statistics by Wireless AP** display option. The **Admission Control Statistics by Wireless AP** display opens in a new browser window.



Admission Control Statistics by Wireless AP - 192.168.4.30

● No refresh ○ Refresh every 30

	Users
0002000810003823	0

0002000810003823 *0002000810003823*

Client IP	Client MAC	Protocol	BSS MAC	SSID	AC	Direction	MDR [bps]	NMS [bytes]	SBA	Rate [bps]		Violat
										DL	UL	DL
	No Client is connected to this Wireless AP											

Active Users: 0

Search Client by User name ▾ Search

Data as of Mar 10, 2009 05:37:08 pm

3. In the **Admission Control Statistics by Wireless AP** display, click a registered Wireless AP to display its information:
4. The Admission Control Statistics by Wireless AP lists the TSPEC statistics associated with this Wireless AP:
   - **AC** – Access class where TSPEC is applied,
   - **Direction** – Uplink, Downlink or Bidirectional,
   - **MDR** – Mean Data Rate
   - **NMS** – Nominal Packet Size
   - **SBA** – Surplus Bandwidth (ratio)

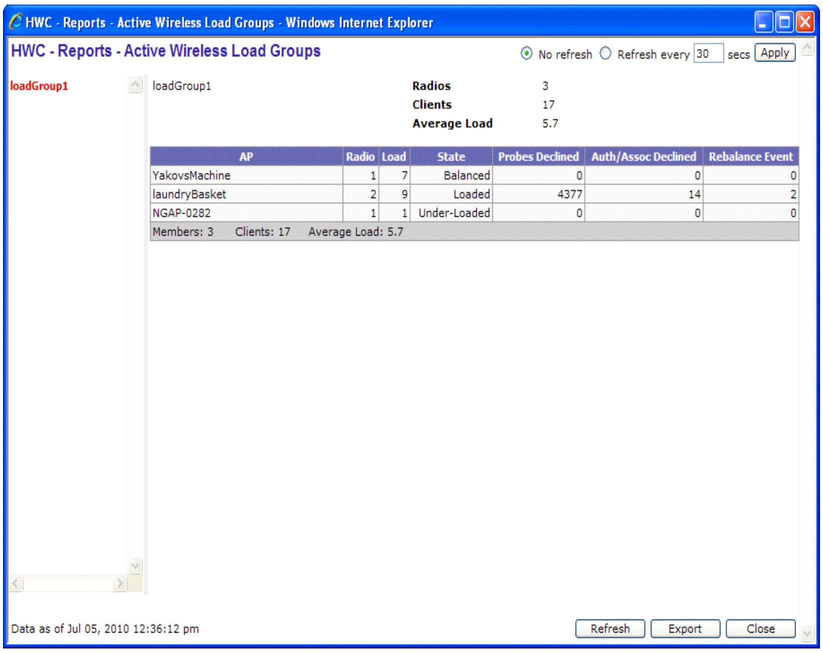
   The following statistics are of measured traffic:
   - **Rate** – Rate in 30 second intervals (uplink and downlink)
   - **Violation** – Number of bits in excess in the last 30 seconds (uplink and downlink)

11.5 Viewing load balance group statistics

The **Active Wireless Load Groups** report lists all load groups, and for the selected load group, all active AP radios.

To view the Active Wireless Load Groups report:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.
2. Click the **Active Wireless Load Groups** report. The **Active Wireless Load Groups** report opens in a new browser window.



HWC - Reports - Active Wireless Load Groups - Windows Internet Explorer

HWC - Reports - Active Wireless Load Groups

● No refresh ○ Refresh every 30 secs Apply

loadGroup1

loadGroup1

Radios	3
Clients	17
Average Load	5.7

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
YakovsMachine	1	7	Balanced	0	0	0
laundryBasket	2	9	Loaded	4377	14	2
NGAP-0282	1	1	Under-Loaded	0	0	0
Members: 3 Clients: 17 Average Load: 5.7						

Data as of Jul 05, 2010 12:36:12 pm

The statistics reported for each load balance group are:

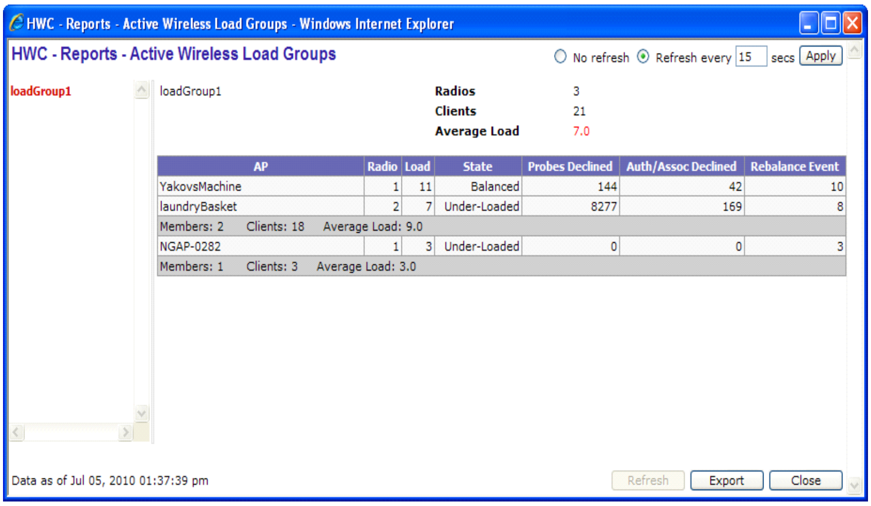
- **Radios** — Number of radio members
- **Clients** — Total number of clients for all radio members
- **Average Load** — Average load for the group

  The reported average load may not be correct in a failover situation. If some APs in the load balance group fail over the foreign controller, those APs will report to the foreign controller. The member APs will continue to use the member count for the whole group, but the member count displayed on the controller will be for only those APs that are reporting. Since the member count reported on the controller is not the complete set, the average will not be consistent with what the APs are using for the state determination.

The statistics reported for each member of the load balance group are:

- **AP** — AP name
- **Radio** — Radio number
- **Load** — Load value (number of clients currently associated with the AP)
- **State** — Load state
- **Probes Declined**
- **Auth/Assoc Requests Declined**
- **Rebalance Event** — Clients removed because of an over-loaded state

The report identifies SIAPP sub-groupings and provide separate group statistics for each sub-group.


HWC - Reports - Active Wireless Load Groups - Windows Internet Explorer

HWC - Reports - Active Wireless Load Groups

○ No refresh ● Refresh every 15 secs Apply

loadGroup1

loadGroup1

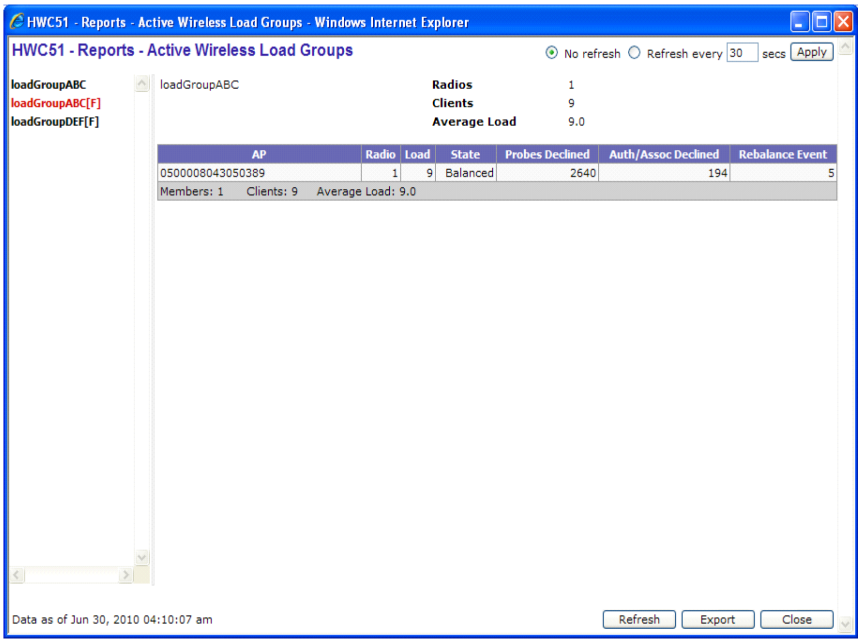
Radios	3
Clients	21
Average Load	7.0

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
YakovsMachine	1	11	Balanced	144	42	10
laundryBasket	2	7	Under-Loaded	8277	169	8
Members: 2 Clients: 18 Average Load: 9.0						
NGAP-0282	1	3	Under-Loaded	0	0	3
Members: 1 Clients: 3 Average Load: 3.0						

Data as of Jul 05, 2010 01:37:39 pm

When the load group includes sub-groups, **Average Load**, in red, is the average of the entire group. The average for each sub-group is also reported. The sub-group average is reported in red when group membership changes and not all members have been updated with the new member count.

Load balance group statistics are reported on the foreign controller when APs fail over with load groups from a different controller indicated with an “(F)” following the load group name.


HWC51 - Reports - Active Wireless Load Groups - Windows Internet Explorer

HWC51 - Reports - Active Wireless Load Groups

● No refresh ○ Refresh every 30 secs Apply

loadGroupABC
loadGroupABC[F]
loadGroupDEF[F]

loadGroupABC

Radios	1
Clients	9
Average Load	9.0

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
0500008043050389	1	9	Balanced	2640	194	5
Members: 1 Clients: 9 Average Load: 9.0						

Data as of Jun 30, 2010 04:10:07 am

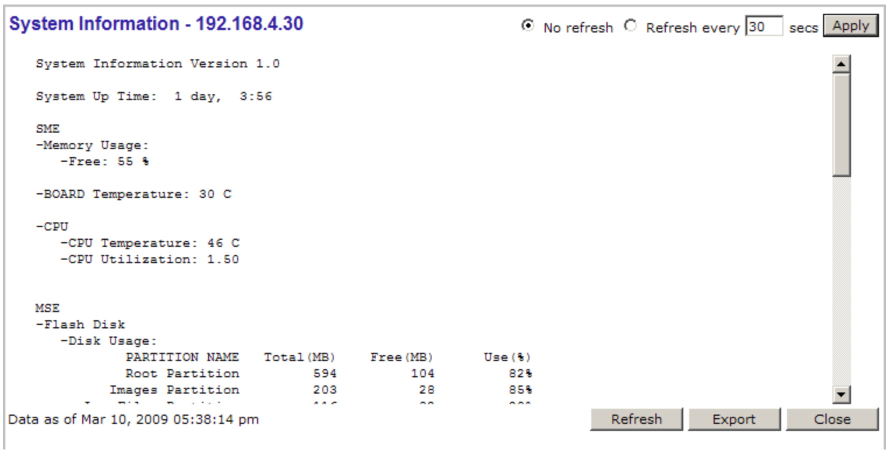
11.6 Viewing the System Information and Manufacturing Information displays

System Information – Displays system information including memory usage and CPU and board temperatures.

Manufacturing Information – Displays manufacturing information including the card serial number and CPU type and frequency.

To view system information:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.
2. Click the **System Information** display option. The **System Information** display opens in a new browser window.



System Information - 192.168.4.30

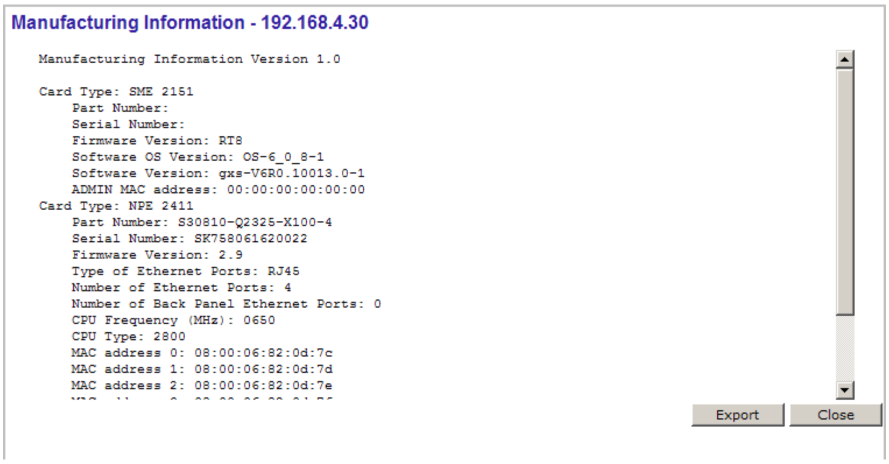
● No refresh ○ Refresh every 30 secs

```
System Information Version 1.0

System Up Time:  1 day,  3:56

SME
-Memory Usage:
   -Free: 55 %

-BOARD Temperature: 30 C

-CPU
   -CPU Temperature: 46 C
   -CPU Utilization: 1.50


MSE
-Flash Disk
   -Disk Usage:
           PARTITION NAME   Total(MB)    Free(MB)     Use(%)
           Root Partition         594         104        82%
         Images Partition         203          28        85%
```

Data as of Mar 10, 2009 05:38:14 pm

To view manufacturing information:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.
2. Click the **Manufacturing Information** display option. The **Manufacturing Information** display opens in a new browser window.



Manufacturing Information - 192.168.4.30

```
Manufacturing Information Version 1.0

Card Type: SME 2151
    Part Number:
    Serial Number:
    Firmware Version: RT8
    Software OS Version: OS-6_0_8-1
    Software Version: gxs-V6R0.10013.0-1
    ADMIN MAC address: 00:00:00:00:00:00
Card Type: NPE 2411
    Part Number: S30810-Q2325-X100-4
    Serial Number: SK758061620022
    Firmware Version: 2.9
    Type of Ethernet Ports: RJ45
    Number of Ethernet Ports: 4
    Number of Back Panel Ethernet Ports: 0
    CPU Frequency (MHz): 0650
    CPU Type: 2800
    MAC address 0: 08:00:06:82:0d:7c
    MAC address 1: 08:00:06:82:0d:7d
    MAC address 2: 08:00:06:82:0d:7e
```

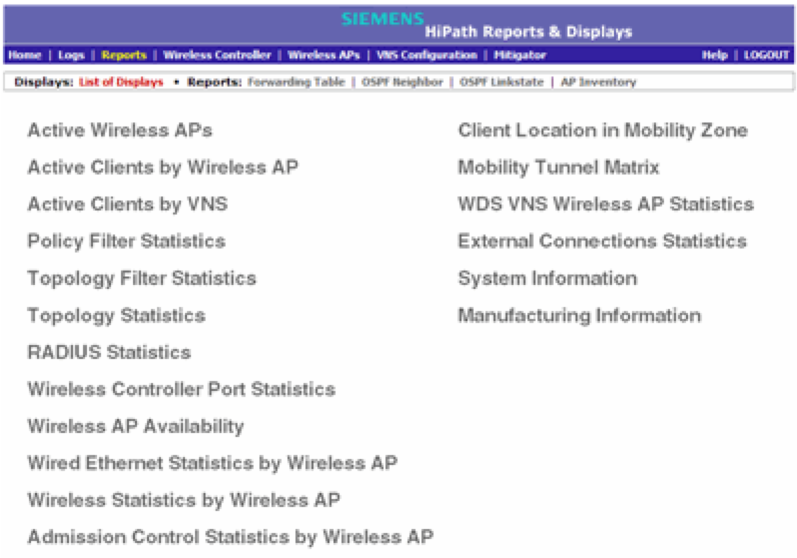
Note: In the latest models of the HiPath Wireless Controller C2400, the IXP2800 Network Processor in the NPE Card has been replaced by the new IXP2805 Network Processor. Consequently, the **Manufacturing Information** in all such latest models displays **CPU Type** as **2805**.

11.7 Viewing displays for the mobility manager

When a HiPath Wireless Controller has been configured as a mobility manager, two additional displays appear as options on the **HiPath Reports & Displays** screen:

- **Client Location in Mobility Zone** – Displays the active wireless clients and their status
- **Mobility Tunnel Matrix** – Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain

Note: The **Client Location in Mobility Zone** and **Mobility Tunnel Matrix** displays only appear if the mobility manager function has been enabled for the controller. Otherwise, the **Agent Mobility Tunnel Matrix** display is listed.


SIEMENS
HiPath Reports & Displays
Home | Logs | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | AP Inventory

Active Wireless APs

Active Clients by Wireless AP

Active Clients by VNS

Policy Filter Statistics

Topology Filter Statistics

Topology Statistics

RADIUS Statistics

Wireless Controller Port Statistics

Wireless AP Availability

Wired Ethernet Statistics by Wireless AP

Wireless Statistics by Wireless AP

Admission Control Statistics by Wireless AP

Client Location in Mobility Zone

Mobility Tunnel Matrix

WDS VNS Wireless AP Statistics

External Connections Statistics

System Information

Manufacturing Information

To view mobility manager displays:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.
2. Click the appropriate mobility manager display:
   - Client Location in Mobility Zone
   - Mobility Tunnel Matrix

The colored status indicates the following:

- **Green** – The mobility manager is in communication with an agent and the data tunnel has been successfully established.
- **Yellow** – The mobility manager is in communication with an agent but the data tunnel is not yet successfully established.
- **Red** – The mobility manager is not in communication with an agent and there is no data tunnel.

Client Location in Mobility Zone

You can do the following:

- Sort this display by home or foreign controller
- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box
- Define the refresh rates for this display
- Export this information as an xml file

Mobility Tunnel Matrix

- Provides connectivity matrix of mobility state
- Provides a view of:
  - Tunnel state
  - If a tunnel between controllers is reported down, it is highlighted in red
  - If only a control tunnel is present, it is highlighted in yellow
  - If data and control tunnels are fully established, it is highlighted in green
  - Tunnel Uptime
  - Number of clients roamed (Mobility loading)
  - Local controller loading
  - Mobility membership list

A HiPath Wireless Controller is only removed from the mobility matrix if it is explicitly removed by the administrator from the Mobility permission list. If a particular link between controllers, or the controller is down, the corresponding matrix connections are identified in red color to identify the link.

The Active Clients by VNS report for the controller on which the user is home (home controller) will display the known user characteristics (IP, statistics, etc.). On the foreign controller, the Clients by VNS report does not show users that have roamed from other controllers, since the users remain associated with the home controller's VNS.

The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP.

Note: Although you can set the screen refresh period less than 30 seconds, the screen will not be refreshed quicker than 30 seconds. The screen will be refreshed according to the value you set only if you set the value above 30 seconds.

11.8 Viewing reports

The following reports are available in the HiPath Wireless Controller, Access Points and Convergence Software system:

- Forwarding Table (routes defined on the **Routing Protocols** screens)
- OSPF Neighbor (if OSPF is enabled on the **Routing Protocols** screens)

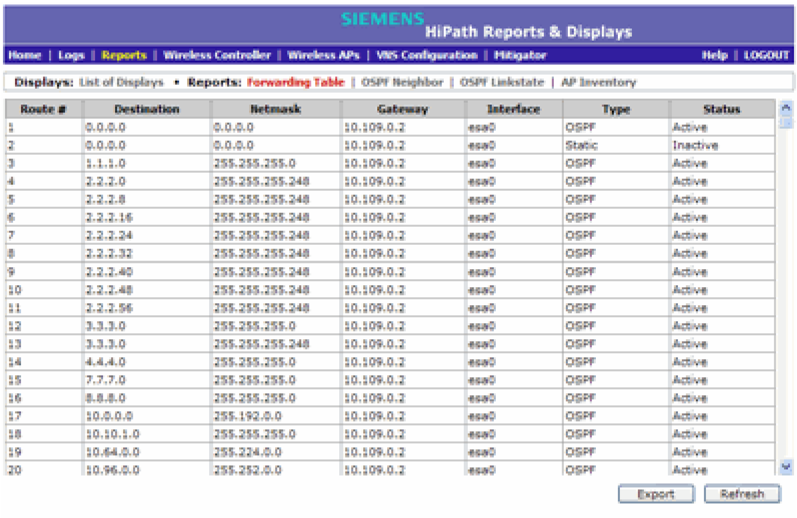
- OSPF Linkstate (if OSPF is enabled on the **Routing Protocols** screens)
- AP Inventory (a consolidated summary of Wireless AP setup)

To view reports:

1. From the main menu, click **Reports & Displays**. The **HiPath Reports & Displays** screen is displayed.
2. In the **Reports** list, click the report you want to view.

Note: The **AP Inventory** report opens in a new browser window. All other reports appear in the current browser window.

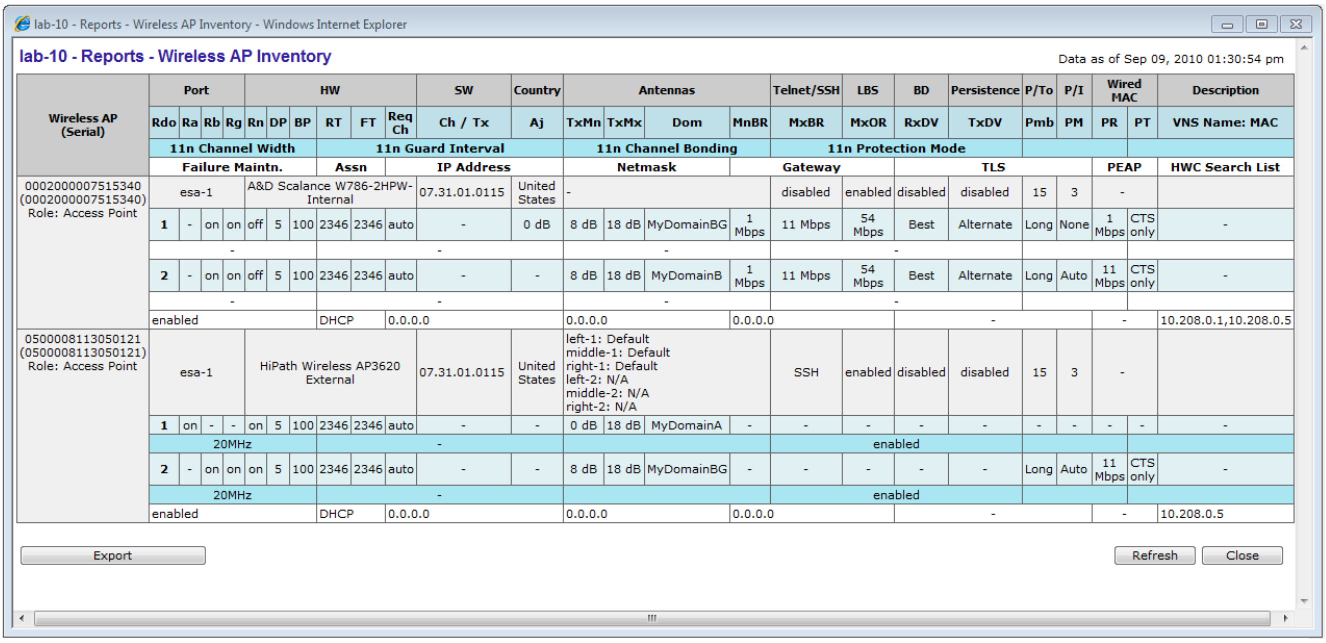
The following is an example of a **Forwarding Table** report:


SIEMENS
HiPath Reports & Displays
Home | Logs | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mitigator
Help | LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | AP Inventory

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.109.0.2	esa0	OSPF	Active
2	0.0.0.0	0.0.0.0	10.109.0.2	esa0	Static	Inactive
3	1.1.1.0	255.255.255.0	10.109.0.2	esa0	OSPF	Active
4	2.2.2.0	255.255.255.248	10.109.0.2	esa0	OSPF	Active
5	2.2.2.8	255.255.255.248	10.109.0.2	esa0	OSPF	Active
6	2.2.2.16	255.255.255.248	10.109.0.2	esa0	OSPF	Active
7	2.2.2.24	255.255.255.248	10.109.0.2	esa0	OSPF	Active
8	2.2.2.32	255.255.255.248	10.109.0.2	esa0	OSPF	Active
9	2.2.2.40	255.255.255.248	10.109.0.2	esa0	OSPF	Active
10	2.2.2.48	255.255.255.248	10.109.0.2	esa0	OSPF	Active
11	2.2.2.56	255.255.255.248	10.109.0.2	esa0	OSPF	Active
12	3.3.3.0	255.255.255.0	10.109.0.2	esa0	OSPF	Active
13	3.3.3.0	255.255.255.248	10.109.0.2	esa0	OSPF	Active
14	4.4.4.0	255.255.255.0	10.109.0.2	esa0	OSPF	Active
15	7.7.7.0	255.255.255.0	10.109.0.2	esa0	OSPF	Active
16	8.8.8.0	255.255.255.0	10.109.0.2	esa0	OSPF	Active
17	10.0.0.0	255.192.0.0	10.109.0.2	esa0	OSPF	Active
18	10.10.1.0	255.255.255.0	10.109.0.2	esa0	OSPF	Active
19	10.64.0.0	255.224.0.0	10.109.0.2	esa0	OSPF	Active
20	10.96.0.0	255.252.0.0	10.109.0.2	esa0	OSPF	Active

Note: If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually time out.

The following is an example of the Wireless AP Inventory report:


lab-10 - Reports - Wireless AP Inventory - Windows Internet Explorer

lab-10 - Reports - Wireless AP Inventory

Data as of Sep 09, 2010 01:30:54 pm

Wireless AP (Serial)	Port				HW						SW	Country	Antennas				Telnet/SSH	LBS	BD	Persistence	P/To	P/I	Wired MAC		Description
	Rdo	Ra	Rb	Rg	Rn	DP	BP	RT	FT	Req Ch	Ch / Tx	Aj	TxMn	TxMx	Dom	MnBR	MxBR	MxOR	RxDV	TxDV	Pmb	PM	PR	PT	VNS Name: MAC
	11n Channel Width							11n Guard Interval					11n Channel Bonding				11n Protection Mode								
	Failure Maintn.							Assn		IP Address			Netmask			Gateway			TLS				PEAP		HWC Search List
0002000007515340 (0002000007515340) Role: Access Point	esa-1				A&D Scalance W786-2HPW-Internal						07.31.01.0115	United States	-				disabled	enabled	disabled	disabled	15	3	-		
	1	-	on	on	off	5	100	2346	2346	auto	-	0 dB	8 dB	18 dB	MyDomainBG	1 Mbps	11 Mbps	54 Mbps	Best	Alternate	Long	None	1 Mbps	CTS only	-
	-							-					-				-								
	2	-	on	on	off	5	100	2346	2346	auto	-	-	8 dB	18 dB	MyDomainB	1 Mbps	11 Mbps	54 Mbps	Best	Alternate	Long	Auto	11 Mbps	CTS only	-
	-							-					-				-								
	enabled							DHCP		0.0.0.0			0.0.0.0			0.0.0.0			-				-		10.208.0.1,10.208.0.5
0500008113050121 (0500008113050121) Role: Access Point	esa-1				HiPath Wireless AP3620 External						07.31.01.0115	United States	left-1: Default middle-1: Default right-1: Default left-2: N/A middle-2: N/A right-2: N/A				SSH	enabled	disabled	disabled	15	3	-		
	1	on	-	-	on	5	100	2346	2346	auto	-	-	0 dB	18 dB	MyDomainA	-	-	-	-	-	-	-	-	-	-
	20MHz							-									enabled								
	2	-	on	on	on	5	100	2346	2346	auto	-	-	8 dB	18 dB	MyDomainBG	-	-	-	-	-	Long	Auto	11 Mbps	CTS only	-
	20MHz							-									enabled								
	enabled							DHCP		0.0.0.0			0.0.0.0			0.0.0.0			-				-		10.208.0.5

Table 38 lists the column names and abbreviations found in the **AP Inventory** report:

Column Name	Description
Port	Ethernet port and associated IP address of the interface on the HiPath Wireless Controller through which the Wireless AP communicates.
HW	Hardware version of the Wireless AP.
SW	Software version executing on theWireless AP.
Country	Country in which the AP is deployed
Antennas	Antennas used
Telnet/SSH	Telnet or SSH access (enabled or disabled)
LBS	Location based service (enabled or disabled)
BD	Broadcast disassociation (enabled or disabled).
Persistence	Enabled or disabled
P/To	Poll timeout. If polling is enabled, a numeric value.
P/I	Poll interval. If polling is enabled, a numeric value.
Wired MAC	The physical address of the Wireless AP's wired Ethernet interface.
Description	As defined on the **AP Properties** screen.
Rdo	Radios: **1** or **2**.
Ra	802.11a radio. The data entry for an Wireless AP indicates whether the **a** radio is on or off.

Table 38 AP Inventory report columns

Column Name	Description
Rb	802.11b protocol enabled. Possible values are **on** or **off**.
Rg	802.11g protocol enabled. Possible values are **on** or **off**.
Rn	802.11n protocol enabled. Possible values are **on** or **off**.
DP	DTIM period
BP	Beacon Period
RT	RTS Threshold
FT	Fragmentation Threshold
Req Ch	Channel served by the corresponding radio.
Ch / Tx	Channel Tx
Aj	Tx power level, in decibels
TxMn	Minimum Tx power, in decibels
TxMx	Maximum Tx power, in decibels
Dom	RF domain
MnBR	Minimum Basic Rate (For more information, see the Wireless AP radio configuration tabs.)
MxBR	Maximum Basic Rate
MxOR	Maximum Operational Rate
RxDV	Receive Diversity
TxDV	Tx Diversity
Pmb	Preamble (long, short)
PM	Protection Mode
PR	Protection Rate
PT	Protection Type
VNS Name: MAC	Also called BSSID, this is the MAC address of a (virtual) wireless interface on which the Wireless AP serves a BSS/ VNS. There could be 8 per radio.
11n Channel Width	20MHz, 40MHz, or auto
11n Guard Interval	If 11n Channel Width is 40MHz, long or short
11n Channel Bonding	Enabled only if 11n Channel Width is 40MHz
11n Protection Mode	Protects high throughput transmissions on primary channels from non-11n APs and clients. Enabled or disabled.
Failure Maintn.	Maintain MU sessions on Wireless AP when the Wireless AP loses the connection to the HiPath Wireless Controller.
Assn	Assignment (address assignment method)
IP Address	Wireless AP's IP address if statically configured (same as the **Static Values** radio button on the **AP Static Configuration** screen).
Netmask	If the Wireless AP's IP address is configured statically, the net mask that is statically configured for the Wireless AP.

Table 38 AP Inventory report columns (Continuation)

Column Name	Description
Gateway	If the Wireless AP's IP address is configured statically, the IP address of the gateway router that the Wireless AP will use.
TLS	802.1x EAP-TLS authentication configuration
PEAP	802.1x PEAP authentication configuration
HWC Search List	The list of IP addresses that the Wireless AP is configured to try to connect to in the event that the current connection to the HiPath Wireless Controller is lost.

Table 38 AP Inventory report columns (Continuation)

To export and save a report in XML:

1. On the report screen, click **Export**. A Windows **File Download** dialog is displayed.
2. Click **Save**. A Windows **Save As** dialog is displayed.

> **Note:** If your default XML viewer is Internet Explorer or Netscape, clicking **Open** will open the exported data to your display screen. You must right-click to go back to the export display. The XML data file will not be saved to your local drive.

3. Browse to the location where you want to save the exported XML data file, and in the **File name** box enter an appropriate name for the file.
4. Click **Save**. The XML data file is saved in the specified location.

11.9 Call Detail Records (CDRs)

You can configure the HiPath Wireless Controller to generate Call Detail Records (CDRs), which contain usage information about each wireless session per VNS. For more information on how to configure the HiPath Wireless Controller to generate CDRs, refer to Section 6.9.3.2, “Defining accounting methods for a WLAN Service”, on page 348.

CDRs are located in a CDR directory on the HiPath Wireless Controller. To access the CDR file, you must first back up the file on the local drive, and then upload it to a remote server. After the CDR file is uploaded to a remote server, you can work with the file to view CDRs or import the records to a reporting tool.

You can back up and upload the file on the remote server either via the HiPath Wireless Assistant (GUI) or CLI.

11.9.1 CDR files naming convention

CDRs are written to a file on the HiPath Wireless Controller. The filename is based on the creation time of the CDR file with the following format: YYYYMMDDhhmmss.<ext>

- **YYYY** — Four digit year
- **MM** — Two digit month, padded with a leading zero if the month number is less than 10
- **DD** — Two digit day of the month, padded with a leading zero if the day number is less than 10
- **hh** — Two digit hour, padded with a leading zero if the hour number is less than 10
- **mm** — Two digit minute, padded with a leading zero if the minute number is less than 10
- **ss** — Two digit second, padded with a leading zero if the second number is less than 10
- **<ext>** — File extension, either **.work** or **.dat**

11.9.2 CDR file types

Two types of CDR files exist in the CDR directory on the HiPath Wireless Controller C2400:

- **.work** — The active file that is being updated by the accounting system. The file is closed and renamed with the **.dat** extension when it attains its maximum size (16 MB) or it has been open for the maximum allowed duration (12 hours). You can back up and copy the **.work** file from the HiPath Wireless Controller to a remote server.
- **.dat** — The inactive file that contains the archived account records. You can back up and copy the **.dat** file from the HiPath Wireless Controller to a remote server.

Note: The CDR directory on the HiPath Wireless Controller only has two files — a **.work** file and a **.dat** file. When the **.work** file attains its maximum size of 16 MB, or it has been open for 12 hours, it is saved as a **.dat** file. This new **.dat** file overwrites the existing **.dat** file. If you want to copy the existing **.dat** file, you must do so before it is overwritten by the new **.dat** file.

11.9.3 CDR file format

A CDR file contains a sequence of CDR records. The file is a standard ASCII text file. Records are separated by a sequence of dashes followed by a line break. The individual fields of a record are reported one per line, in “field=value’ format.

The following table describes the records that are displayed in a CDR file.

Note: Most of the CDR records are typical RADIUS server attributes. For more information, refer to the user manual of your RADIUS server.

CDR Records	Description
Acct-Session-ID	A unique CDR ID
User-Name	The name of the user, who was authenticated.
Filter-ID	The name of the filter list for the user.
Acct-Interim-Interval	The number of seconds between interim accounting updates.
Session-Timeout	The maximum number of seconds of service to be provided to the user before termination of the session.
Class	This field is copied from the Access-Accept message sent by the RADIUS server during authentication.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
Acct-Delay-Time	Indicates how many seconds the client tried to authenticate send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS (AAA), Local (Internal CP) or Remote (External CP). The field displays one of the following values: • 1 – AAA authentication • 2 – Internal CP authentication • 3 – External CP authentication
Framed-IP-Address	Indicates the address to be configured for the user
Connect-Info	This field is sent from the NAS to indicate the nature of the users’ connection — 802.11b for Radio **b/g** or 802.11a for radio **a**.
NAS-Port-Type	Indicates RADIUS NAS Port Type is Wireless 802.11
Called-Station-ID	The Wireless AP’s MAC address.
Calling-Station-ID	The client’s MAC address.
Siemens-AP-Serial	The Wireless AP’s serial number.
Siemens-AP-Name	The Wireless AP’s name.

Table 39 CDR Records and their description

CDR Records	Description
Siemens-VNS-Name	The VNS name on which the session took place.
Siemens-SSID	The SSID name on which the session took place.
Acct-Session-Time	The number of seconds the user has received the service.
Acct-Output-Packets	The number of packets that were sent to the port in the course of delivering this service to a framed user.
Acct-Input-Packets	The number of packets that have been received from the port over the course of this service being provided to a Framed User.
Acct-Output-Octets	The number of octets that were sent to the port in the course of delivering the service.
Acct-Input-Octets	The number of octets that were received from the port over the course of the service.
Acct-Terminate-Cause	Indicates how the session was terminated. The field displays one of the following values: • **1** – User Request **4** – Idle Timeout • **5** – Session Timeout • **6** – Admin Reset • **11** – NAS Reboot • **16** – Callback • **17** – User Error
Authenticated_time	Indicates the time at which the client was authenticated. The time is in the following format: **Date hh:mm:ss**. For example, **April 21 2008 14:50:24**
Disassociation_time	Indicates the time at which the client was disassociated from the Wireless AP. The time is in the following format: **Date hh:mm:ss**. For example, **April 21 2008 14:57:20**.

Table 39 CDR Records and their description (Continuation)

11.9.4 Viewing CDRs

The following is a high-level overview of how to view CDRs:

1. Back up the CDR files on the local drive of the HiPath Wireless Controller.
2. Copy the CDR files from the HiPath Wireless Controller to the remote server.
3. Unzip the file.
4. Download the CDR files from the remote server to view CDRs.

Note: You cannot access the CDR files directly from the CDR directory.

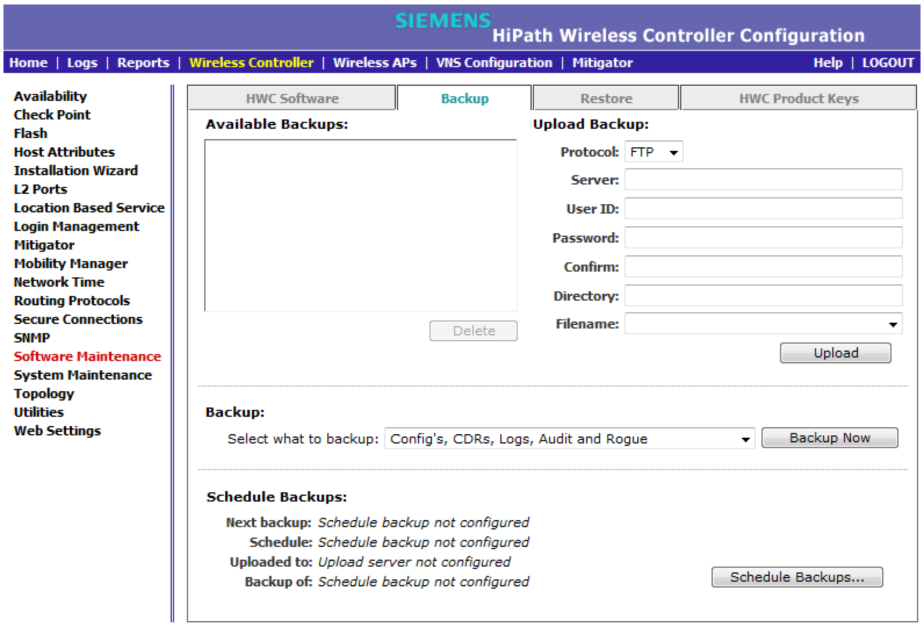
When you back up CDRs, both the **.work** and **.dat** files are zipped into a single .zip file. This .zip file is uploaded on the remote server. You can unzip this file from the remote server to extract the **.work** and **.dat** files.

You can back up and upload the files on the remote server either via the HiPath Wireless Assistant (GUI) or CLI.

This section describes how to back up and copy the CDR files to a remote server via the HiPath Wireless Assistant (GUI). For more information on how to copy the CDR file to the remote server via CLI, refer to the *HiPath Wireless Controller, Access Points and Convergence Software CLI Reference Guide*.

To back up and copy the CDR files to a remote server:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Software Maintenance**. The **Software Maintenance** screen is displayed.
3. Click the **Backup** tab.

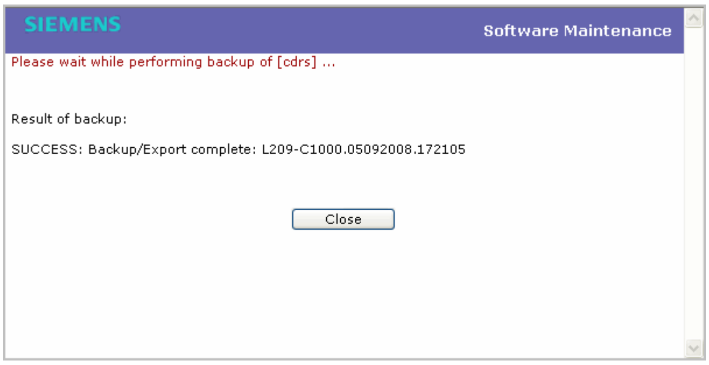


Protocol: FTP
Server:
User ID:
Password:
Confirm:
Directory:
Filename:

Backup:
Select what to backup: Config's, CDRs, Logs, Audit and Rogue

Schedule Backups:
Next backup: *Schedule backup not configured*
Schedule: *Schedule backup not configured*
Uploaded to: *Upload server not configured*
Backup of: *Schedule backup not configured*

4. From the **Select what to backup** drop-down menu, click **CDRs only**, and then click **Backup Now**. The following window displays the backup status.



Please wait while performing backup of [cdrs] ...

Result of backup:

SUCCESS: Backup/Export complete: L209-C1000.05092008.172105

5. To close the window, click **Close**. The backed up file is displayed in the **Available Backups** box.

Note: The **.work** and **.dat** files are zipped into a single file.

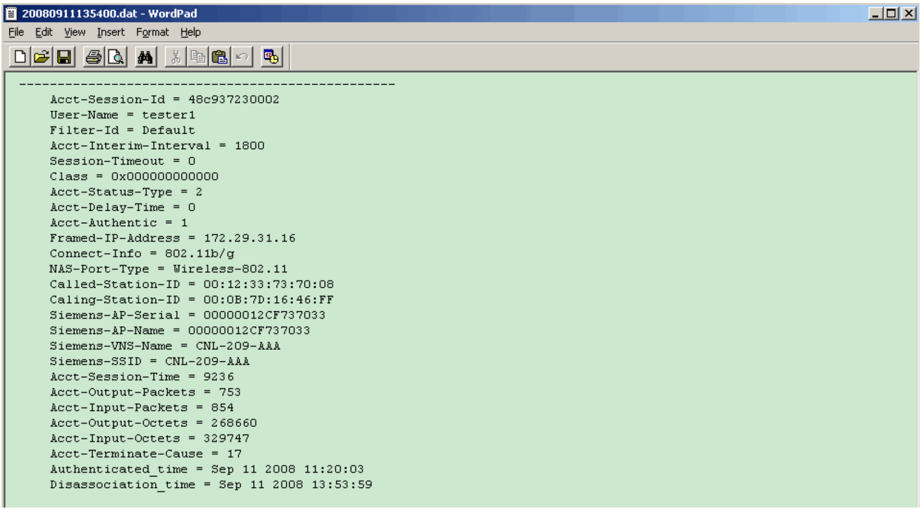
---

6. To upload a backup, in the **Upload Backup** section, do the following:
   - **Protocol** – Select the file transfer protocol you want to use to upload the backup file, **SCP** or **FTP**.
   - **Server** – Type the IP address of the server where the backup will be stored.
   - **User ID** – Type the user ID to log in to the server.
   - **Password** – The password to log in to the server.
   - **Confirm** – The password to confirm the password.
   - **Directory** – The directory in which you want to upload the CDR file.
   - **Filename** – Type the zipped CDR file name.

Note: After you back up CDRs, the zipped CDR file name is selected by default in the **Filename** box.

---

7. In the **Upload Backup** section, click **Upload**. The .zip file is uploaded on to the server.
8. Unzip the file. The two CDR files — **.work** and **.dat** — are visible on the server.
9. To view CDRs, download the files.



```
-------------------------------------------------
    Acct-Session-Id = 48c937230002
    User-Name = tester1
    Filter-Id = Default
    Acct-Interim-Interval = 1800
    Session-Timeout = 0
    Class = 0x000000000000
    Acct-Status-Type = 2
    Acct-Delay-Time = 0
    Acct-Authentic = 1
    Framed-IP-Address = 172.29.31.16
    Connect-Info = 802.11b/g
    NAS-Port-Type = Wireless-802.11
    Called-Station-ID = 00:12:33:73:70:08
    Caling-Station-ID = 00:0B:7D:16:46:FF
    Siemens-AP-Serial = 00000012CF737033
    Siemens-AP-Name = 00000012CF737033
    Siemens-VNS-Name = CNL-209-AAA
    Siemens-SSID = CNL-209-AAA
    Acct-Session-Time = 9236
    Acct-Output-Packets = 753
    Acct-Input-Packets = 854
    Acct-Output-Octets = 268660
    Acct-Input-Octets = 329747
    Acct-Terminate-Cause = 17
    Authenticated_time = Sep 11 2008 11:20:03
    Disassociation_time = Sep 11 2008 13:53:59
```

Figure 28 Sample .dat file

12 Performing system administration

This chapter describes system administration processes, including:

- Performing Wireless AP client management
- Defining HiPath Wireless Assistant administrators and login groups
- Configuring Web session timeouts

12.1 Performing Wireless AP client management

There are times when for business, service, or security reasons you want to cut the connection with a particular wireless device. You can view all the associated wireless devices, by MAC address, on a selected Wireless AP and do the following:

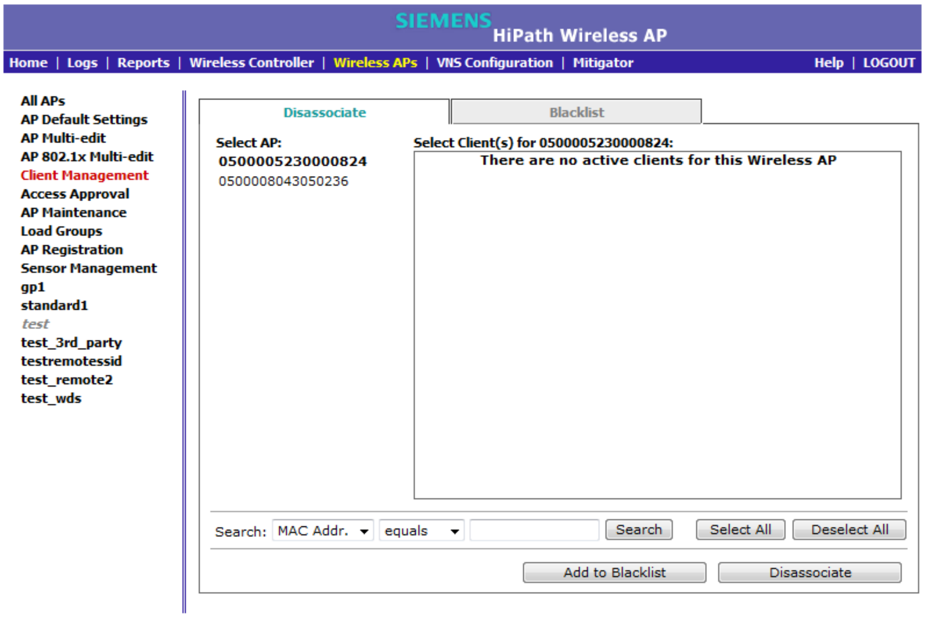
- Disassociate a selected wireless device from its Wireless AP.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the Wireless AP.
- Backup and restore the HiPath Wireless Controller database. For more information, see the *HiPath Wireless Controller, Access Points and Convergence Software Maintenance Guide*.

12.1.1 Disassociating a client

In addition to the following procedure below, you can also disassociate wireless users directly from the **Active Clients by VNS** screen. For more information, see Chapter 11, “Working with reports and displays”.

To disassociate a wireless device client:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.



Select AP:
0500005230000824
0500008043050236

Select Client(s) for 0500005230000824:
There are no active clients for this Wireless AP

Search: MAC Addr. equals

3. In the **Select AP** list, click the AP that is connected to the client that you want to disassociate.

4. In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate.

Note: You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the **Search** box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.

5. Click **Disassociate**. The client's session terminates immediately.

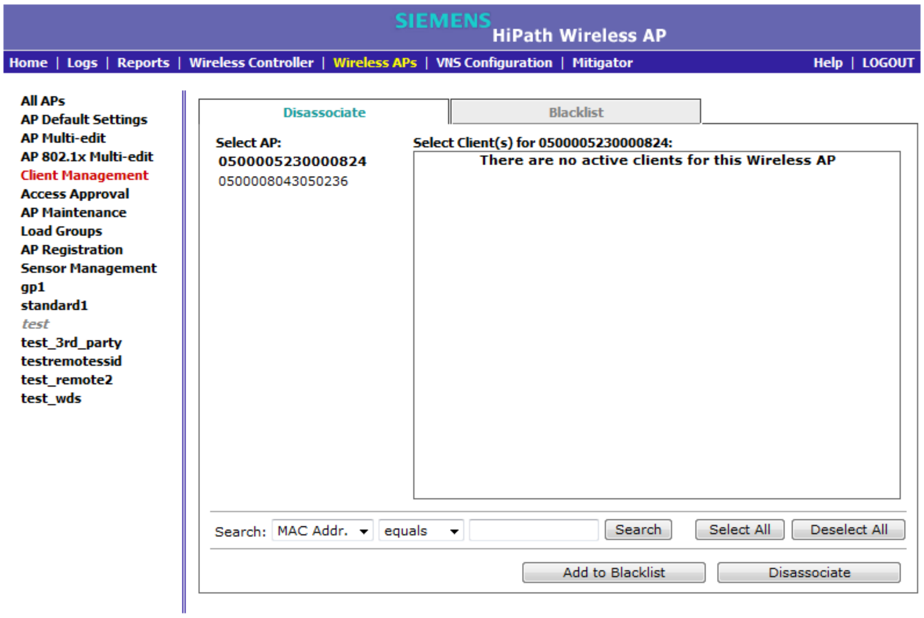
12.1.2 Blacklisting a client

The **Blacklist** tab displays the current list of MAC addresses that are not allowed to associate. A client is added to the blacklist by selecting it from a list of associated APs or by typing its MAC address.

To blacklist a wireless device client:

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

2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.



Select AP:
0500005230000824
0500008043050236

Select Client(s) for 0500005230000824:
There are no active clients for this Wireless AP

3. In the **Select AP** list, click the AP that is connected to the client that you want to blacklist.

4. In the **Select Client(s)** list, select the checkbox next to the client you want to blacklist, if applicable.

Note: You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the **Search** box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.

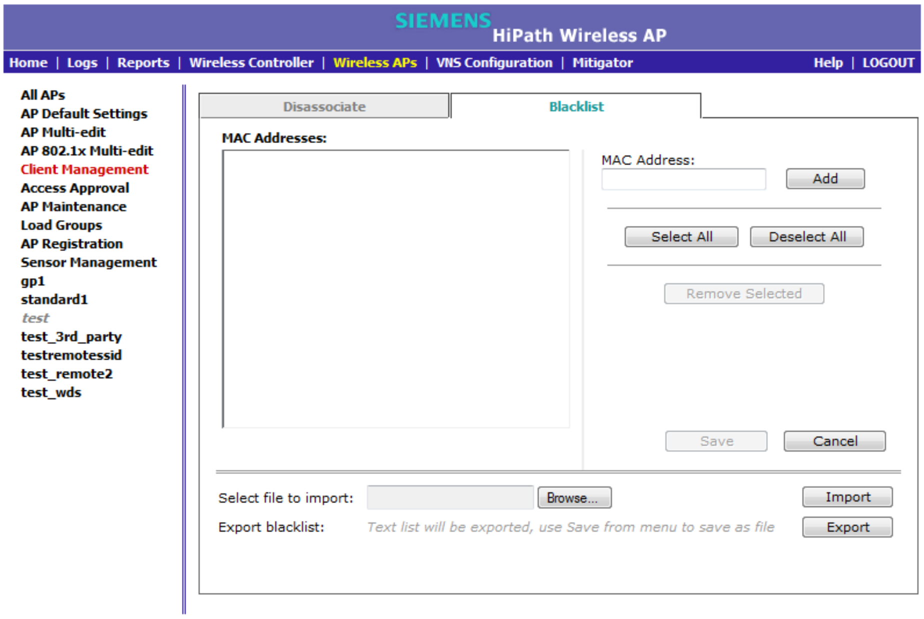
5. Click **Add to Blacklist**. The selected wireless client's MAC address is added to the blacklist.

To blacklist a wireless device client using its MAC address:

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

2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3. Click the **Blacklist** tab.



4. To add a new MAC address to the blacklist, in the **MAC Address** box type the client’s MAC address.

5. Click **Add**. The client is displayed in the **MAC Addresses** list.

Note: You can use the **Select All** or **Clear All** buttons to help you select multiple clients.

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

To clear an address from the blacklist:

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

2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3. Click the **Blacklist** tab.

4. To clear an address from the blacklist, select the corresponding checkbox in the **MAC Addresses** list.

5. Click **Remove Selected**. The selected client is removed from the list.

Note: You can use the **Select All** or **Clear All** buttons to help you select multiple clients.

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

To import a list of MAC addresses for the blacklist:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.
3. Click the **Blacklist** tab.
4. Click **Browse** and navigate to the file of MAC addresses you want to import and add to the blacklist.
5. Click the file, and then click **Import**. The list of MAC addresses is imported.

To export a list of MAC addresses for the blacklist:

1. From the main menu, click **Wireless AP Configuration**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.
3. Click the **Blacklist** tab.
4. Click **Export**. The saved blacklist file is exported.
5. To export the current blacklist, use the browser's save option to save the file as a text (.txt) file. It is recommend that a descriptive file name is used.

12.2 Defining HiPath Wireless Assistant administrators and login groups

You can define the login user names and passwords for administrators that have access to the HiPath Wireless Assistant. You can also assign them to a login group — as full administrators, read-only administrators, or as GuestPortal managers. For each user added, you can define and modify a user ID and password.

- **Full administrators** – Users assigned to this login group have full administrator access rights on the HiPath Wireless Controller. Full administrators can manage all aspects of the HiPath Wireless Controller, including GuestPortal user accounts.
- **Read-only administrators** – Users assigned to this login group have read-only access rights on the HiPath Wireless Controller, including the GuestPortal user accounts.

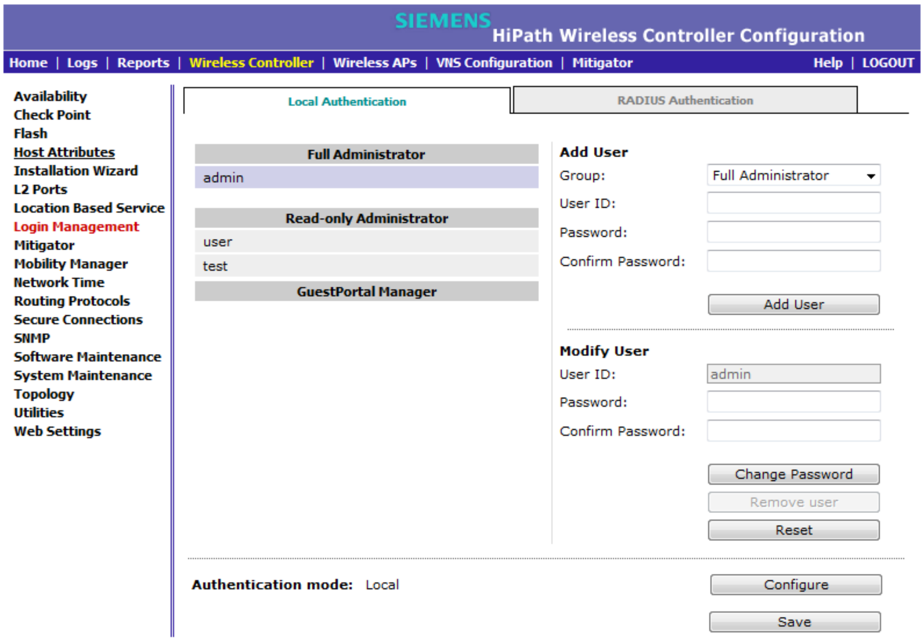
- **GuestPortal managers** – Users assigned to this login group can only manage GuestPortal user accounts. Any user who logs on to the HiPath Wireless Controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the HiPath Wireless Assistant.

Note: When adding or modifying a user, note the following password character constraints:
• Allowed characters include A-Z a-z 0-9 ~!@#$%^&*()_+|-=\{}[];<>?,.
• Characters not allowed include / ` ' " : and space is not valid.

To add a HiPath Wireless Controller administrator to a login group:

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

2. In the left pane, click **Login Management**. The **Local Authentication** tab is displayed.



3. In the **Group** drop-down list, click one of the following:

   - **Full Administrator** – Users assigned to this login group have full administrator access rights on the HiPath Wireless Controller.

     Full administrators can manage GuestPortal user accounts.

   - **Read-only Administrator** – Users assigned to this login group have read-only access rights on the HiPath Wireless Controller.

     Read-only administrators have read access to the GuestPortal user accounts.

- **GuestPortal Manager** – Users assigned to this login group can only manage GuestPortal user accounts. Any user who logs on to the HiPath Wireless Controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the HiPath Wireless Assistant. For more information, see Section 12.2.1, “Working with GuestPortal Guest administration”, on page 485.

4. In the **User ID** box, type the user ID for the new user. A user ID can only be used once, in only one category.
5. In the **Password** box, type the password for the new user.
6. In the **Confirm Password**, re-type the password.
7. Click **Add User**. The new user is added to the appropriate login group list.

To modify a HiPath Wireless Controller administrator’s password:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Login Management**. The **Local Authentication** tab is displayed.
3. Click the user whose password you want to modify.
4. In the **Password** box, type the new password for the user.
5. In the **Confirm Password**, re-type the new password.
6. To change the password, click **Change Password**.

To remove a HiPath Wireless Controller administrator:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Login Management**. The **Local Authentication** tab is displayed.
3. Click the user you want to remove.
4. Click **Remove user**. The user is removed from the list.

12.2.1 Working with GuestPortal Guest administration

A GuestPortal provides wireless device users with temporary guest network services. A GuestPortal is serviced by a GuestPortal-dedicated VNS. The GuestPortal-dedicated VNS is configured by an administrator with full administrator access rights. For more information, see Section 6.5, “Working with a GuestPortal VNS”, on page 307.

A GuestPortal administrator is assigned to the GuestPortal Manager login group and can only create and manage guest user accounts — a GuestPortal administrator cannot access any other area of the HiPath Wireless Assistant. For more information, see Section 12.2, “Defining HiPath Wireless Assistant administrators and login groups”, on page 483.

From the **GuestPortal Guest Administration** page of the HiPath Wireless Assistant, you can add, edit, configure, and import and export guest accounts.

12.2.1.1 Adding new guest accounts

To add a new guest account:

1. Do one of the following:

   - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.

   - If you have full administrator rights:

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

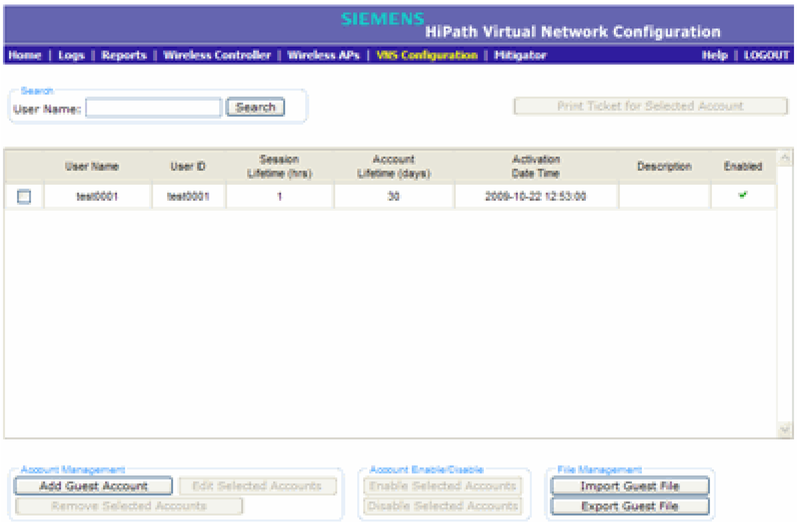
     b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

     c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

     d) In the **GuestPortal** section, click **Manage Guest Users**.

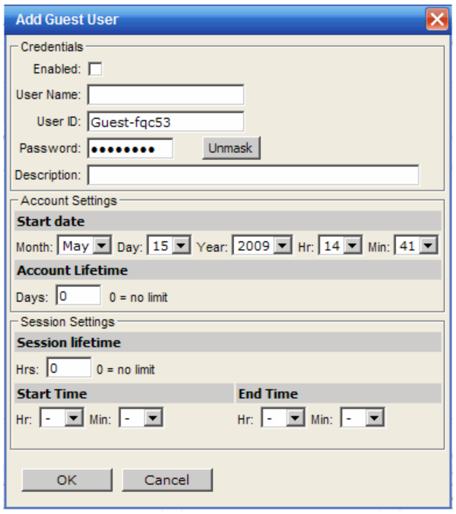
   The **GuestPortal Guest Administration** screen is displayed.

   Note: You have 3 minutes to add new guest user accounts. If that time expires, close the **GuestPortal Guest Administration** screen and click **Manage Guest Users** again. You can also increase the **Start date** time to be within 3 minutes of the current network time.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the **Account Management** section, click **Add Guest Account**. The **Add Guest User** screen is displayed.



Enabled: □

User Name:

User ID: Guest-fqc53

Password: ••••••••

Description:

Month: May Day: 15 Year: 2009 Hr: 14 Min: 41

Days: 0 0 = no limit

Hrs: 0 0 = no limit

Start Time Hr: - Min: -

End Time Hr: - Min: -

3. To enable the new guest account, select the **Enabled** checkbox. For more information, see Section 12.2.1.2, “Enabling or disabling guest accounts”, on page 488.

4. In the **Credentials** section, do the following:

    - **User Name** – Type a user name for the person who will use this guest account.
    - **User ID** – Type a user ID for the person who will use this guest account. The default user ID can be edited.
    - **Password** – Type a password for the person who will use this guest account. The default password can be edited.

Toggle between **Mask**/**Unmask** to hide or see the password.

- **Description** – Type a brief description for the new guest account.

5. In the **Account Settings** section, do the following:
   - **Start date** – Specify the start date and time for the new guest account.
   - **Account lifetime** – Specify the account lifetime, in days, for the new guest account. The default **0** value does not limit the account lifetime.
6. In the **Session Settings** section, do the following:
   - **Session lifetime** – Specify a session lifetime, in hours, for the new guest account. The default **0** value does not limit a session lifetime. The session lifetime is the allowed cumulative total in hours spent on the network during the account lifetime.
   - **Start Time** – Specify a start time for the session for the new guest account.
   - **End Time** – Specify an end time for the session for the new guest account.
7. To save your changes, click **OK**.

12.2.1.2 Enabling or disabling guest accounts

A guest account must be enabled in order for a wireless device user to use the guest account to obtain guest network services.

When a guest account is disabled, it remains in the database. A disabled guest account cannot provide access to the network.

To enable or disable guest accounts:

1. Do one of the following:
   - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.
   - If you have full administrator rights:

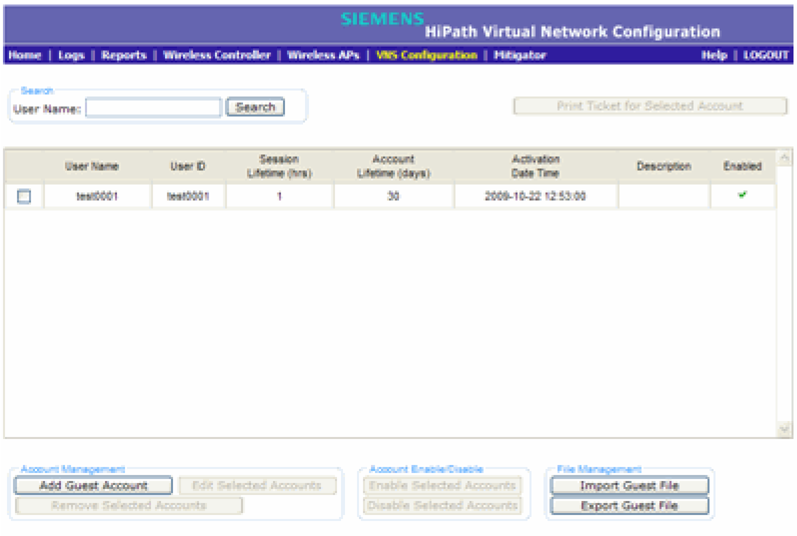
     a) From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

     b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

     c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

     d) In the **GuestPortal** section, click **Manage Guest Users**.

The **GuestPortal Guest Administration** screen is displayed.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the guest account list, select the checkbox next to the user name of the guest account that you want to enable or disable.

3. In the **Account Enable/Disable** section, click **Enable Selected Accounts** or **Disable Selected Accounts** accordingly. A dialog is displayed requesting you to confirm your selection.

4. Click **Ok**. A confirmation message is displayed in the **GuestPortal Guest Administration** screen footer.

12.2.1.3 Editing guest accounts

An already existing guest account can be edited.

To edit a guest account:

1. Do one of the following:

   - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.

   - If you have full administrator rights:

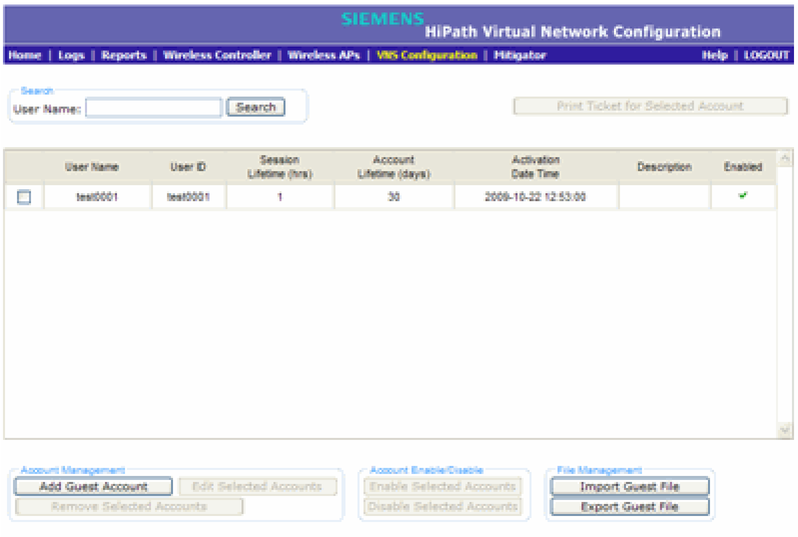
     a) From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

     b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

d) In the **GuestPortal** section, click **Manage Guest Users**.

The **GuestPortal Guest Administration** screen is displayed.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the guest account list, select the checkbox next to the user name of the guest account that you want to edit.

3. In the **Account Management** section, click **Edit Selected Accounts**. The **Edit Guest User** screen is displayed.

4. Edit the guest account accordingly. For more information on guest account properties, see Section 12.2.1.1, “Adding new guest accounts”, on page 486.

5. To save your changes, click **OK**. A confirmation message is displayed in the **GuestPortal Guest Administration** screen footer.

12.2.1.4 Removing guest accounts

An already existing guest account can be removed from the database.

To remove a guest account:

1. Do one of the following:

    - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.
    - If you have full administrator rights:

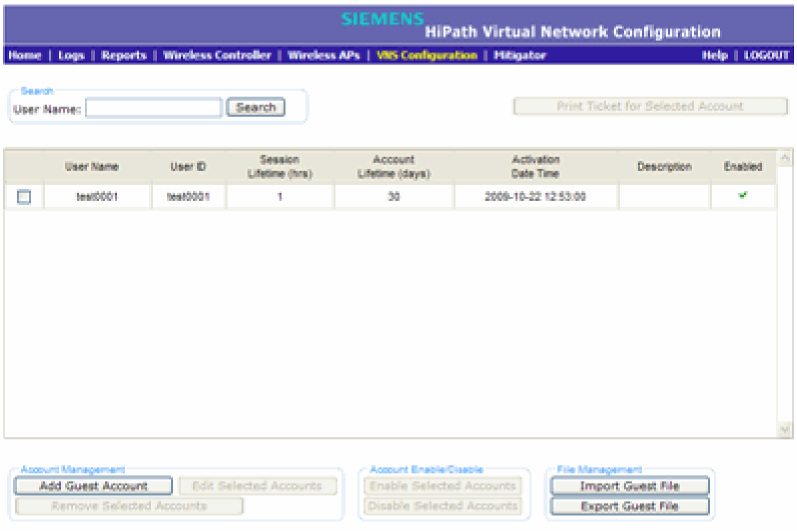
        a) From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

        b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

        c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

        d) In the **GuestPortal** section, click **Manage Guest Users**.

    The **GuestPortal Guest Administration** screen is displayed.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the guest account list, select the checkbox next to the user name of the guest account that you want to remove.
3. In the **Account Management** section, click **Remove Selected Accounts**. A dialog is displayed requesting you to confirm your removal.
4. Click **OK**. A confirmation message is displayed in the **GuestPortal Guest Administration** screen footer.

12.2.1.5 Importing and exporting a guest file

To help administrators manage large numbers of guest accounts, you can import and export .csv (comma separated value) guest files for the HiPath Wireless Controller.

The following describes the column values of the .csv guest file.

Column	Value
A	User ID
B	User name
C	Password
D	Description
E	Account activation date
F	Account lifetime, measured in days
G	Session lifetime, measured in hours
H	Is the account enabled (1) or disabled (0)
I	Time of day, start time
J	Time of day, duration
K	Total time of the session lifetime that has been used, measured in minutes
L	Is the guest user account synchronized on a secondary HiPath Wireless Controller in an availability pair, yes (1) no (0)

Table 40 Guest account import and export .csv file values

To export a guest file

1. Do one of the following:

   - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.

   - If you have full administrator rights:

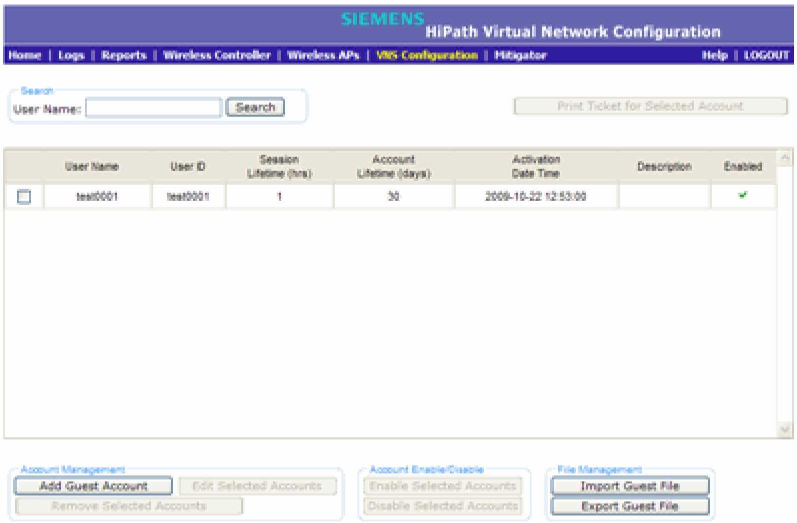
     a) From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

     b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

     c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

     d) In the **GuestPortal** section, click **Manage Guest Users**.

   The **GuestPortal Guest Administration** screen is displayed.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the **File Management** section, click **Export Guest File**. A **File Download** dialog is displayed.

3. Click **Save**. The **Save As** dialog is displayed.

4. Name the guest file, and then navigate to the location where you want to save the file. By default, the exported guest file is named **exportguest.csv**.

5. Click **Save**. The **File Download** dialog is displayed as the file is exported.

6. Click **Close**. A confirmation message is displayed in the **GuestPortal Guest Administration** screen footer.

To import a guest file

1. Do one of the following:

   - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.

   - If you have full administrator rights:

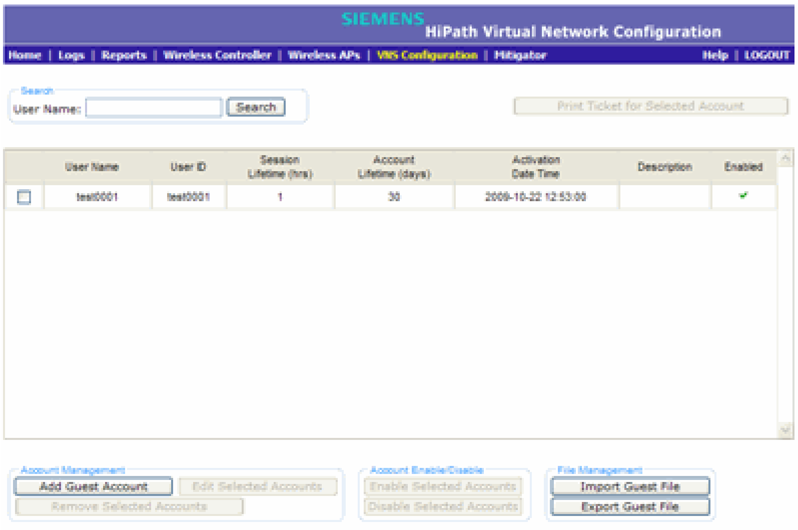
     a) From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

     b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

     c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

     d) In the **GuestPortal** section, click **Manage Guest Users**.

   The **GuestPortal Guest Administration** screen is displayed.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the **File Management** section, click **Import Guest File**. The **Import Guest File** dialog is displayed.

3. Click **Browse** to navigate to the location of the .csv guest file that you want to import, and then click **Open**.

4. Click **Import**. The file is imported and a confirmation message is displayed in the **Import Guest File** dialog.

5. Click **Close**.

12.2.1.6 Viewing and printing a GuestPortal account ticket

You can view and print a GuestPortal account ticket from the **GuestPortal Guest Administration** screen. A GuestPortal account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account.

The HiPath Wireless Controller is shipped with a default template for the GuestPortal account ticket. The template is an html page that is augmented with system placeholders that display information about the user.

You can also upload a custom GuestPortal ticket template for the HiPath Wireless Controller. To upload a custom GuestPortal ticket template you need full administrator access rights on the HiPath Wireless Controller. The filename of a custom GuestPortal ticket template must be .html. For more information, see Section 12.2.1.7, “Working with the GuestPortal ticket page”, on page 496.

To view print a GuestPortal account ticket:

1. Do one of the following:

   - If you have GuestPortal Manager rights, log onto the HiPath Wireless Controller.
   - If you have full administrator rights:

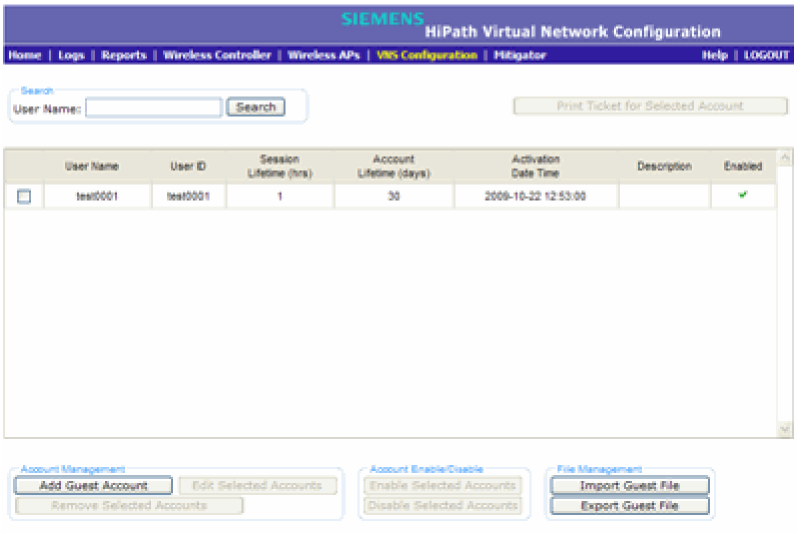
     a) From the main menu, click **Virtual Network Configuration**. The **Virtual Network Configuration** screen is displayed.

     b) In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.

     c) Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.

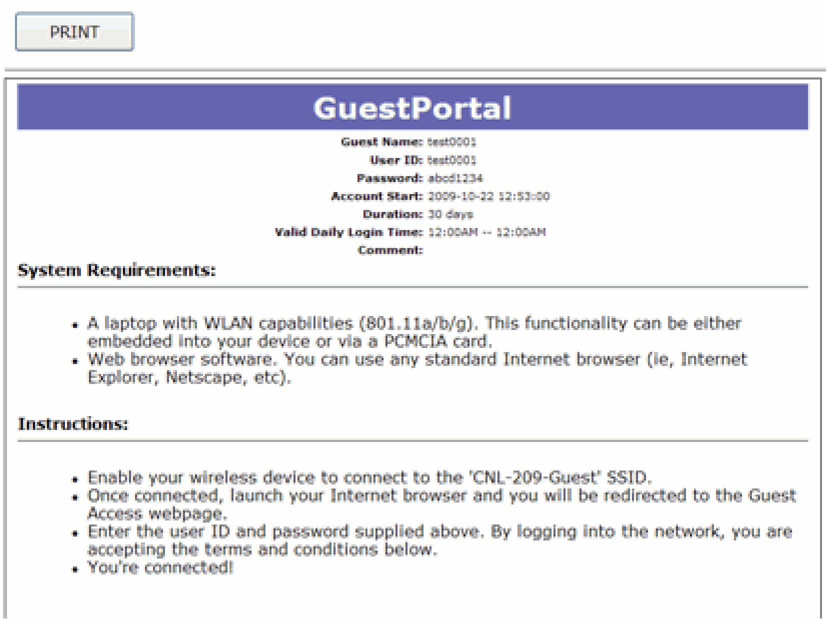
     d) In the **GuestPortal** section, click **Manage Guest Users**.

   The **GuestPortal Guest Administration** screen is displayed.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
□	test0001	test0001	1	30	2009-10-22 12:53:00		✓

2. In the guest account list, select the checkbox next to the user name whose guest account ticket you want to print a ticket, and then click **Print Ticket for Selected Account**. The **GuestPortal** ticket is displayed.



GuestPortal

Guest Name: test0001

User ID: test0001

Password: abcd1234

Account Start: 2009-10-22 12:53:00

Duration: 30 days

Valid Daily Login Time: 12:00AM -- 12:00AM

Comment:

System Requirements:

- A laptop with WLAN capabilities (801.11a/b/g). This functionality can be either embedded into your device or via a PCMCIA card.
- Web browser software. You can use any standard Internet browser (ie, Internet Explorer, Netscape, etc).

Instructions:

- Enable your wireless device to connect to the 'CNL-209-Guest' SSID.
- Once connected, launch your Internet browser and you will be redirected to the Guest Access webpage.
- Enter the user ID and password supplied above. By logging into the network, you are accepting the terms and conditions below.
- You're connected!

3. Click **Print**. The **Print** dialog is displayed.

4. Click **Print**.

Note: The default GuestPortal ticket page uses placeholder tags. For more information, see Appendix E, “Default GuestPortal source code”

12.2.1.7 Working with the GuestPortal ticket page

Working with the GuestPortal ticket page can include activating a GuestPortal ticket page, uploading a customized GuestPortal ticket page to the HiPath Wireless Controller, and deleting a customized GuestPortal ticket page.

Note: The default GuestPortal ticket page cannot be deleted.

To work with the GuestPortal account ticket page, you need full administrator rights. You can work with the guest account ticket page from the **Settings** screen. A guest account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account.

Working with a custom GuestPortal ticket page

A customized GuestPortal ticket page can be uploaded to the HiPath Wireless Controller. When designing your customized GuestPortal ticket page, be sure to use the guest account information placeholder tags that are depicted in the default GuestPortal ticket page. For more information, see Appendix E, “Default GuestPortal source code”.

To activate a GuestPortal ticket page:

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, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
3. Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen is displayed.
4. In the **GuestPortal** section, click **Configure Ticket Page**. The **Ticket Settings** dialog is displayed.
5. In the **Active Template** list, click the GuestPortal ticket page you want to activate, and then click **Apply**.

   This list includes all GuestPortal ticket pages that have been uploaded to the HiPath Wireless Controller.

To upload a custom GuestPortal ticket page:

1. On the **Ticket Settings** dialog, click **Browse**. The **Choose file** dialog is displayed.
2. Navigate to the .html GuestPortal ticket page file that you want to upload to the HiPath Wireless Controller, and then click **Open**. The file name is displayed in the **Upload Template** box.
3. Click **Apply**. The file is uploaded to the HiPath Wireless Controller.

   The **Active Template** list includes all GuestPortal ticket pages that have been uploaded to the HiPath Wireless Controller.

To delete a custom GuestPortal ticket page:

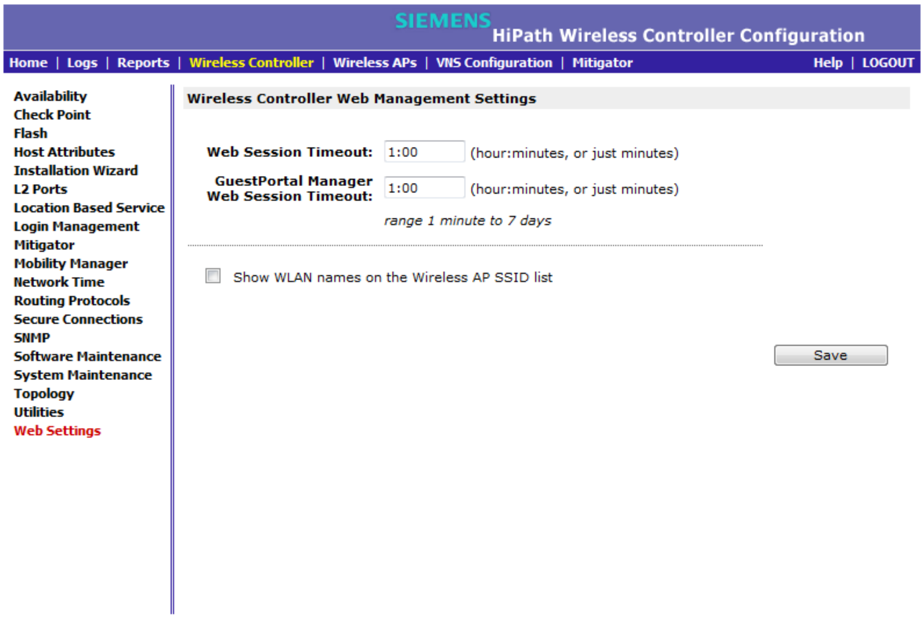
1. On the **Ticket Settings** dialog, in the **Active Template** list, click the GuestPortal ticket page you want to delete, and then click **Delete**. A dialog prompts you to confirm you want to delete the GuestPortal ticket page.
2. To delete the file, click **OK**, and then click **Apply**.,

12.3 Configuring Web session timeouts

You can configure the time period to allow Web sessions to remain inactive before timing out.

To configure Web session timeouts:

1. From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Web Settings** The **Wireless Controller Web Management Settings** screen is displayed.



Wireless Controller Web Management Settings

Web Session Timeout: 1:00 (hour:minutes, or just minutes)

GuestPortal Manager Web Session Timeout: 1:00 (hour:minutes, or just minutes)

range 1 minute to 7 days

□ Show WLAN names on the Wireless AP SSID list

3. In the **Web Session Timeout** box, type the time period to allow the Web session to remain inactive before it times out. This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.
4. In the **GuestPortal Manager Web Session Timeout** box, type the time period to allow the GuestPortal Web session to remain inactive before it times out. This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.
5. Select the **Show WLAN names on the Wireless AP SSID list** checkbox to allow the names of the WLAN services to appear in the SSID list for Wireless APs.
6. To save your settings, click **Save**.

Note: Screens that auto-refresh will time-out unless a manual action takes place prior to the end of the timeout period.

13 Glossary

13.1 Networking terms and abbreviations

Term	Explanation
AAA	Authentication, Authorization and Accounting. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.
Access Point (AP)	A wireless LAN transceiver or ‘base station’ that can connect a wired LAN to one or many wireless devices.
Ad-hoc mode	An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). (Compare Infrastructure Mode)
AES	Advanced Encryption Standard (AES) is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits. AES was created by the National Institute of Standards and Technology (NIST). AES is a privacy transform for IPSec and Internet Key Exchange (IKE). AES has a variable key length - the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key. For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.
AES-CCMP	AES uses the Counter-Mode/CBC-MAC Protocol (CCMP). CCM is 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 and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.
ARP	Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.
Association	A connection between a wireless device and an Access Point.
asynchronous	Asynchronous transmission mode (ATM). A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.
BSS	Basic Service Set. A wireless topology consisting of one Access Point connected to a wired network and a set of wireless devices. Also called an infrastructure network. *See also* IBSS.
Captive Portal	A browser-based authentication mechanism that forces unauthenticated users to a Web page. Sometimes called a ‘reverse firewall’.

Term	Explanation
CDR	Call Data (Detail) Record In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call. In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database
CHAP	Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.
CLI	Command Line Interface.
Collision	Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.
Datagram	A datagram is ”a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” (RFC1594). The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports.
dBm	An abbreviation for the power ratio in decibels (dB) of the measured power referenced to one milliwatt.
Decapsulation	*See* tunnelling.
Device Server	A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers and network time servers are examples of device servers.
DHCP	Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. (IETF RFC1531.) Option 78 specifies the location of one or more SLP Directory Agents. Option 79 specifies the list of scopes that a SLP Agent is configured to use.(RFC2610 - DHCP Options for Service Location Protocol)

Term	Explanation
Directory Agent (DA)	A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request. For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent. (SLP version 2, RFC2608, updating RFC2165)
Diversity antenna and receiver	The AP has two antennae. Receive diversity refers to the ability of the AP to provide better service to a device by receiving from the user on which ever of the two antennae is receiving the cleanest signal. Transmit diversity refers to the ability of the AP to use its two antenna to transmit on a specific antenna only, or on a alternate antennae. The antennae are called diversity antennae because of this capability of the pair.
DNS	Domain Name Server
DSSS	Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare FHSS)
DTIM	DTIM delivery traffic indication message (in 802.11 standard)
Dynamic WEP	The IEEE introduced the concept of user-based authentication using per-user encryption keys to solve the scalability issues that surrounded static WEP. This resulted in the 802.1x standard, which makes use of the IETF's Extensible Authentication Protocol (EAP), which was originally designed for user authentication in dial-up networks. The 802.1x standard supplemented the EAP protocol with a mechanism to send an encryption key to a Wireless AP. These encryption keys are used as dynamic WEP keys, allowing traffic to each individual user to be encrypted using a separate key.
EAP-TLS EAP-TTLS	EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames. In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication. EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys. EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. (*See also* PEAP)

Term	**Explanation**
ELA (OPSEC)	Event Logging API (Application Program Interface) for OPSEC, a module in Check Point used to enable third-party applications to log events into the Check Point VPN-1/FireWall-1 management system.
Encapsulation	*See* tunnelling.
ESS	Extended Service Set (ESS). Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (*See* BSS and SSID.)
FHSS	Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that ‘hops’ in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare DSSS)
Fit, thin and fat APs	A thin AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required. A fit AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management. A fat (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.
FQDN	Fully Qualified Domain Name. A ‘friendly’ designation of a computer, of the general form computer.[subnetwork.].organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a Domain Name Server.
FTM	Forwarding Table Manager
FTP	File Transfer Protocol
Gateway	In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.
Gigabit Ethernet	The high data rate of the Ethernet standard, supporting data rates of 1 gigabit (1,000 megabits) per second.
GUI	Graphical User Interface
Heartbeat message	A heartbeat message is a UDP data packet used to monitor a data connection, polling to see if the connection is still alive. In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.
Host	(1) A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines. (2) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

Term	Explanation
HTTP	Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.
IBSS	Independent Basic Service Set. *See* BSS. An IBSS is the 802.11 term for an adhoc network. *See* adhoc network.
ICMP	Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.
ICV	ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (*See* WPA and MIC)
IE	Internet Explorer.
IEEE	Institute of Electrical and Electronics Engineers, a technical professional association, involved in standards activities.
IETF	Internet Engineering Task Force, the main standards organization for the Internet.
Infrastructure Mode	An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (*See* ad-hoc mode and BSS.)
Internet or IP telephony	IP or Internet telephony are communications, such as voice, facsimile, voice-messaging applications, that are transported over the Internet, rather than the public switched telephone network (PSTN). IP telephony is the two-way transmission of audio over a packet-switched IP network (TCP/IP network). An Internet telephone call has two steps: (1) converting the analog voice signal to digital format, (2) translating the signal into Internet protocol (IP) packets for transmission over the Internet. At the receiving end, the steps are reversed. Over the public Internet, voice quality varies considerably. Protocols that support Quality of Service (QoS) are being implemented to improve this.
IP	Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (host) on the Internet has at least one IP address that uniquely identifies it. Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
IPC	Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.

Term	Explanation
IPsec IPsec-ESP IPsec-AH	Internet Protocol security (IPSec) Internet Protocol security Encapsulating Security Payload (IPsec-ESP). The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram.Internet Protocol security Authentication Header (IPsec-AH). AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver.IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.
isochronous	Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.
ISP	Internet Service Provider.
IV	IV (Initialization Vector), part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (*See* WPA and TKIP)
LAN	Local Area Network.
License installation	
LSA	Link State Advertisements 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. *See* also OSPF.
MAC	Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.
MAC address	Media Access Control address. A hardware address that uniquely identifies each node of a network.
MIB	Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. A MIB is a collection of definitions defining the properties of a managed object within a device. Every managed device keeps a database of values for each of the definitions written in the MIB. Definition of the MIB conforms to RFC1155 (Structure of Management Information).
MIC	Message Integrity Check or Code (MIC), also called ‘Michael’, is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks. Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (*See* WPA, TKIP and ICV).

Term	Explanation
MTU	Maximum Transmission Unit. The largest packet size, measured in bytes, that a network interface is configured to accept. Any messages larger than the MTU are divided into smaller packets before being sent.
MU	Mobile Unit, a wireless device such as a PC laptop.
multicast, broadcast, unicast	Multicast: transmitting a single message to a select group of recipients. Broadcast: sending a message to everyone connected to a network. Unicast: communication over a network between a single sender and a single receiver.
NAS	Network Access Server, a server responsible for passing information to designated RADIUS servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC2138)
NAT	Network Address Translator. A network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
Netmask	In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the "255.255.255.0" netmask allows the specific host computer address to be visible.
NIC	Network Interface Card. An expansion board in a computer that connects the computer to a network.
NMS	Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.
NTP	Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC1305)
OFDM	Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels. OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.
OID	Object Identifier.
OPSEC	OPSEC (Open Platform for Security) is a security alliance program created by Check Point to enable an open industry-wide framework for interoperability of security products and applications. Products carrying the 'Secured by Check Point' seal have been tested to guarantee integration and interoperability.
OS	Operating system.
OSI	Open System Interconnection. An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.

Term	Explanation
OSI Layer 2	At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sublayers: • the Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking • The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.
OSI Layer 3	The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
OSPF	Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts 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. (RFC2328)
OUI	Organizationally Unique Identifier (used in MAC addressing).
Packet	The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into packets. Each packet is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).
PAP	Password Authentication Protocol is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (*See* CHAP).
PDU	Protocol Data Unit. A data object exchanged by protocol machines (such as management stations, SMUX peers, and SNMP agents) and consisting of both protocol control information and user data. PDU is sometimes used as a synonym for “packet".
PEAP	PEAP (Protected Extensible Authentication Protocol) is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (*See* also EAP-TLS).
PHP server	Hypertext Preprocessor
PKI	Public Key Infrastructure
PoE	Power over Ethernet. The Power over Ethernet standard (802.3af) defines how power can be provided to network devices over existing Ethernet connection, eliminating the need for additional external power supplies.
POST	Power On Self Test, a diagnostic testing sequence performed by a computer to determine if its hardware elements are present and powered on. If so, the computer begins its boot sequence.

Term	Explanation
push-to-talk (PTT)	The push-to-talk (PTT) is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic. A PTT call is initiated by selecting a channel and pressing the 'talk' key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.
QoS	Quality of Service. A term for a number of techniques that intelligently match the needs of specific applications to the network resources available, using such technologies as Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, setting traffic priorities across the network. Quality-of-Service (QoS): A set of service requirements to be met by the network while transporting a flow. (RFC2386)
RADIUS	Remote Authentication Dial-In User Service. An authentication and accounting system that checks User Name and Password and authorizes access to a network. The RADIUS specification is maintained by a working group of the IETF (RFC2865 RADIUS, RFC2866 RADIUS Accounting, RFC2868 RADIUS Attributes for Tunnel Protocol Support).
RF	Radio Frequency, a frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF) -- 0-3 Hz to Extremely high frequency (EHF) -- 30GHz - 300 GHz. The middle ranges are: Low frequency (LF) -- 30 kHz - 300 kHz, Medium frequency (MF) -- 300 kHz - 3 MHz, High frequency (HF) -- 3MHz - 30 MHz, Very high frequency (VHF) -- 30 MHz - 300 MHz, Ultra-high frequency (UHF)-- 300MHz - 3 GHz.
RFC	Request for Comments, a series of notes about the Internet, submitted to the Internet Engineering Task Force (IETF) and designated by an RFC number, that may evolve into an Internet standard. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.
Roaming	In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.
RP-SMA	Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas
RSN	Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).
RSSI	RSSI received signal strength indication (in 802.11 standard)
RTS / CTS	RTS request to send, CTS clear to send (in 802.11 standard)
Segment	In Ethernet networks, a section of a network that is bounded by bridges, routers or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.

Term	Explanation
SLP	Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request. For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent. (SLP version 2, RFC2608, updating RFC2165)
SMI	Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC1155 and RFC1442 (SNMPv2).
SMT (802.11)	Station ManagemenT. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are: • dot11smt - objects related to station management and local configuration • dot11mac - objects that report/configure on the status of various MAC parameters • dot11res - Objects that describe available resources • dot11phy - Objects that report on various physical items.
SNMP	Simple Network Management Protocol. A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set.
SNMP trap	An event notification sent by the SNMP managed agent to the management system to identify the occurrence of conditions (such as a threshold that exceeds a predetermined value).
SSH	Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. SSH is a suite of three utilities - slogin, ssh, and scp - secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
SSID	Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. In 802.11 networks, each Access Point advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named Access Point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID. Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

Term	Explanation
SSL	Secure Sockets Layer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. URLs that require an SSL connection start with https: instead of http. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The ‘sockets’ part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.
Subnet mask	(*See* netmask)
Subnets	Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.
SVP	SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.
Switch	In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.
syslog	A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them. Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC3164)
TCP / IP	Transmission Control Protocol. TCP, together with IP (Internet Protocol), is the basic communication language or protocol of the Internet. Transmission Control Protocol manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. Internet Protocol handles the address part of each packet so that it gets to the right destination. TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.
TFTP	Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.
TKIP	Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. TKIPs’ enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (rekeyed) automatically and authenticated between devices after the rekey interval (either a specified period of time, or after a specified number of packets has been transmitted).
TLS	Transport Layer Security. (*See* EAP, Extensible Authentication Protocol)

Term	Explanation
ToS / DSCP	ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service (QoS) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.
TSN	Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).
Tunnelling	Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.
UDP	User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive packets over an IP network. It is used primarily for broadcasting messages over a network.
U-NII	Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.
URL	Uniform Resource Locator. the unique global address of resources or files on the World Wide Web. The URL contains the name of the protocol to be used to access the file resource, the IP address or the domain name of the computer where the resource is located, and a pathname -- a hierarchical description that specifies the location of a file in that computer.
VLAN	Virtual Local Area Network. A network of computers that behave as if they are connected to the same wire when they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. When a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration. The standard is defined in IEEE 802.1Q - Virtual LANs, which states that 'IEEE 802 Local Area Networks (LANs) of all types may be connected together with Media Access Control (MAC) Bridges, as specified in ISO/IEC 15802-3. This standard defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure.”
VNS	Virtual Network Services (VNS). A Siemens specific technique that provides a means of mapping wireless networks to a wired topology.
VoIP	Voice Over Internet Protocol. An internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet and is reassembled when it reaches the destination.
VPN	Virtual Private Network. A private network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
VSA	Vendor Specific Attribute, an attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

Term	Explanation
Walled Garden	A restricted subset of network content that wireless devices can access.
WEP	Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.
Wi-Fi	Wireless fidelity. A term referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Used in reference to the Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.
WINS	Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.
WLAN	Wireless Local Area Network.
WMM	Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is compliant with the IEEE 802.11e Quality of Service (QoS) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.
WPA	Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEPs' basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1x for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael. WPA requires that all computers and devices have WPA software.
WPA-PSK	Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the Wireless AP or router and the WPA clients. This preshared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic rekeying.

13.2 Controller, Access Points and Convergence Software terms and abbreviations

Term	Explanation
CTP	CAPWAP Tunnelling Protocol (CTP). The Wireless AP uses a UDP (User Datagram Protocol) based tunnelling protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate the 802.11 packets and forward them to the HiPath Wireless Controller. The CTP protocol defines a mechanism for the control and provisioning of Wireless APs (CAPWAP) through centralized access controllers. In addition, it provides a mechanism providing the option to tunnel the mobile client data between the access point and the access controller.
DRM (dynamic radio/RF management)	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 power levels to balance coverage if another Wireless AP, which is assigned to the same SSID and is on the same channel, is added to or leaves the network. • Allows wireless clients to be moved to another Wireless AP if the load is too high. • Scans automatically for a channel, using a channel selection algorithm. • Avoids other WLANs by reducing transmit power whenever other Wireless APs with the same channel, but different SSIDs are detected. 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. • 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.
HiPath Wireless Controller	The HiPath Wireless Controller is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It 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.
Langley	Langley is a Controller, Access Points and Convergence Software term for the inter-process messaging infrastructure on the HiPath Wireless Controller.
Mitigator	The Mitigator is a mechanism that assists in the detection of rogue access points. The feature has three components: (1) a radio frequency (RF) scanning task that runs on the Wireless AP, (2) an application called the Data Collector on the HiPath Wireless Controller that receives and manages the RF scan messages sent by the Wireless AP, (3) an Analysis Engine on the HiPath Wireless Controller that processes the scan data.
Mobility manager (and mobility agent)	The technique in Controller, Access Points and Convergence Software by which multiple HiPath Wireless Controllers on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different Wireless APs on different HiPath Wireless Controllers, to provide mobility to the wireless device user. One HiPath Wireless Controller on the network must be designated as the mobility manager. All other HiPath Wireless Controllers are designated as mobility agents. Relying on SLP, the mobility manager registers with the Directory Agent and the mobility agents discover the location of the mobility manager.

Term	Explanation
Data Collector	The Data Collector is an application on the HiPath Wireless Controller that receives and manages the Radio Frequency (RF) scan messages sent by the Wireless AP. This application is part of the Mitigator technique, working in conjunction with the scanner mechanism and the Analysis Engine to assist in detecting rogue access points.
Virtual Network Services (VNS)	The Virtual Network Services (VNS) technique is Siemens's means of mapping wireless networks to the topology of an existing wired network. When you set up Virtual Network Services (VNS) on the HiPath Wireless Controller, you are defining subnets for groups of wireless users. This VNS definition creates a virtual IP subnet where the HiPath Wireless Controller acts as a default gateway for wireless devices. 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. 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.
Wireless AP	The Wireless AP is a wireless LAN thin access point (IEEE 802.11) provided with unique software that allows it to communicate only with a HiPath Wireless Controller. (A thin access point handles the radio frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The Wireless AP also provides local processing such as encryption. The Wireless AP is a dual-band access point, with 802.11a/b/g/n radios.

A HiPath Wireless Controller’s physical description

This appendix describes the physical description and LEDs, SSD codes and their description of the following models of the HiPath Wireless Controller:

- HiPath Wireless Controller C5110
- HiPath Wireless Controller C4110
- HiPath Wireless Controller C2400
- HiPath Wireless Controller C20
- HiPath Wireless Controller C20N
- HiPath Wireless Controller CRBT8210/8110

A.1 HiPath Wireless Controller C5110

A.1.1 Front panel

Figure 29 depicts the front panel features of the HiPath Wireless Controller C5110. The following table describes the features by callout.

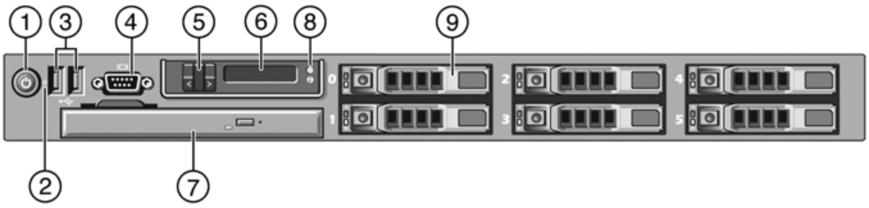


Figure 29 HiPath Wireless Controller C5110 front panel

Call out	Feature	Function
1	Power-on button	Controls the DC power supply output to the system.
2	NMI button	Not used in the current release.
3	USB connectors (2)	Connects USB 2.0-compliant devices to the system. For more information, see the **Note** following Figure 29.
3	Video connector	Not used in the current release.
5	LCD buttons	Controls the LCD display. Two navigation buttons allow you to scroll left and right through the display. The select button controls whether the LCD backlight is on or off.

Call out	Feature	Function
6	LCD display	Provides system ID, status information and system error messages. The LCD display lights during normal system operation. Both the systems management software and the identification buttons located on the front and back of the system can cause the LCD to flash blue to identify a particular system. The LCD display lights amber when the system needs attention due to a problem with power supplies, fans, system temperature or hard drives. When the controller is performing a software upgrade and configuration, the LCD panel will display the word "Upgrade." **Note**: If the system is connected to AC power and an error has been detected, the LCD displays amber lights regardless of whether the system has been powered on.
7	Slot for DVD drive	Not used in the current release.
8	System Identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of the buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
9	Hard drive	One 3.5 inch SATA 250 GB drive.

Note: The HiPath Wireless Controller C5110 is equipped with four USB connectors — two on each front and back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

A.1.2 Back panel

Figure 30 depicts the back panel features of the HiPath Wireless Controller C5110.

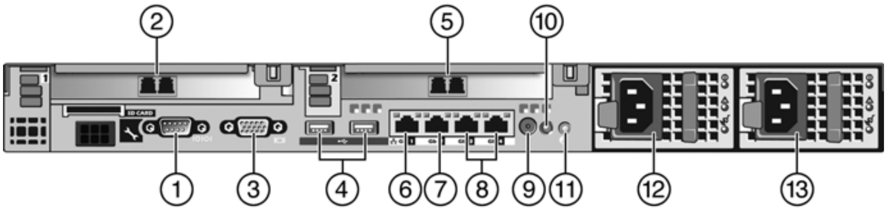


Figure 30 HiPath Wireless Controller C5110 back panel

Callout	Feature	Function
1	Serial port connector	Console Port – Used to get into **Rescue** mode.
2	NIC2 connector	Data port, 10 GbE SR-XFP single port NIC - esa1
3	Video connector	Not used in the current release
4	USB connectors (2)	Connects USB 2.0-compliant devices to the system.
5	10 GbE SR-XFP single port NIC connector	Data port - esa2
6	1 GbE RJ45 connector	Management port - Admin
7	1 GbE RJ45 connector	Data port – esa0
8	Not used	Not used in the current release.
9	System status indicator connector	Not used in the current release.
10	System status indicator	The blue-colored system status indicator blinks to indicate the location of a particular system within a rack. The indicator continues to blink until one of the system identification buttons is pushed again.
11	System identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
12	AC Power supply 1 (PS1)	AC Power Supply 1 and 2 combine to make a redundant power supply.
13	AC Power supply 2 (PS2)	

A.2 HiPath Wireless Controller C4110

For information on HiPath Wireless Controller C4110 hardware, see the *HiPath Wireless Controller C4110 Quick Reference* at http://www.enterasys.com/support/manuals.

A.3 HiPath Wireless Controller C2400

A.3.1 Front panel

The HiPath Wireless Controller C2400 is composed of the following three cards:

- Media/Persistent Storage Card
- Network Processor Card
- Host HiPath Wireless Controller Card

Figure 31 depicts the front panel features of the HiPath Wireless Controller C2400.

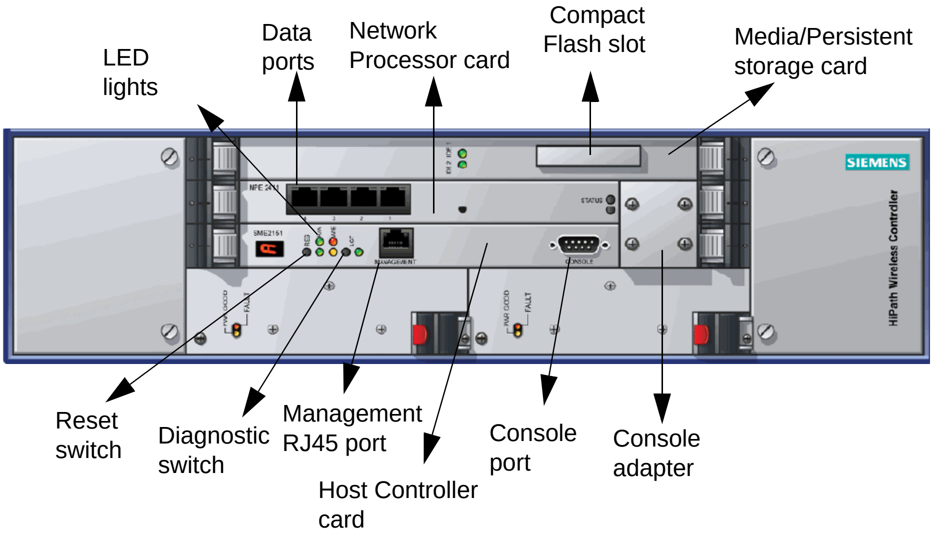


Figure 31 HiPath Wireless Controller C2400 front panel

The HiPath Wireless Controller C2400 has five LED lights and two switches on its front panel.

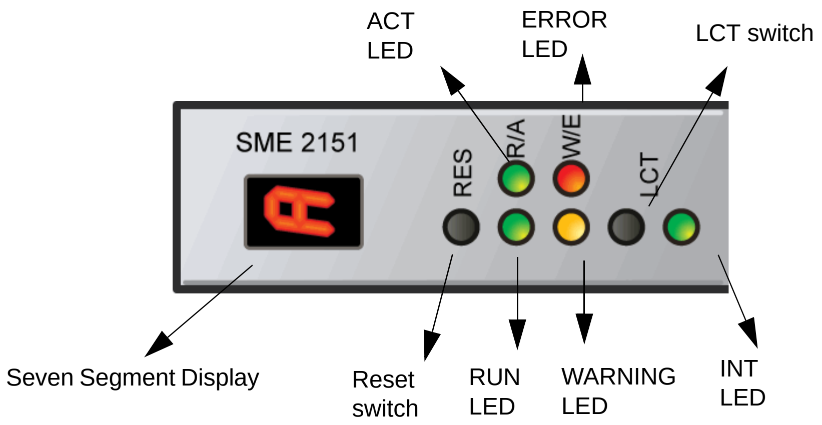


Figure 32 HiPath Wireless Controller’s C2400 LED lights and switches

The description of the LED states and switches is provided below:

- Reset Switch – Reboots the system.
- RUN LED – Indicates the CPU’s initialization has completed and the system is ready to provide application level services.
- ACT LED – Indicates the system’s software is in active running state.
- WARNING/ERROR LEDs – Indicate a problem in the running state of the system.
  - When any of the alarm LEDs is lit, the seven segment display provides the corresponding code point for the error indication. When the system is fully active and running, the console displays the letter **A** as seen in Figure 32.
- LCT Switch – The LCT button is used during the manufacturing process and is inactive otherwise.
- INT LED – Not used in the current release.

A.3.2 LED states and Seven Segment Display (SSD) codes

Table 41 lists LED states and SSD codes during firmware initialization. Table 42 lists LED states and SSD codes during application initialization. Table 43 lists LED states and SSD codes during warning conditions. Table 44 lists LED states and SSD codes during error conditions.

Active LED	Warning LED	Error LED	SSD Code	Condition
Green			0	The processor has started and the firmware has taken control.
Green			3	The Host Controller Card has failed to download Bootloader from Flash.
Green			4	The system is checking firmware consistency.
Green			5	The system is formatting memory.
Green			6	The system is initializing load device. **Note:** If the SSD code is stuck at 6 for more than a minute, it implies that the Network Processor Card is installed in wrong slot.
Green			9	The system is loading subsystem.
Green			b	The system is starting the operation system. The system is active.

Table 41 LED states and SSD codes during firmware initialization

Note: Although the Active LED will be lit Green during the firmware initialization, this LED state is irrelevant to the SSD display or the condition. Ignore the LED state during the firmware initialization.

Active LED	Warning LED	Error LED	SSD Code	Condition
Green			0	Application initialization started.
Green			C	System configuration in progress.
Green			1	Preparing Forwarding Engine initialization.
Green			2	Initializing Forwarding Engine.
Green			3	Completing application initialization.
Green			A	Application initialization complete. System active.
Green			H	System halted. Administrator requested halting of system.

Table 42 LED states and SSD codes during application initialization

Active LED	Warning LED	Error LED	SSD Code	Condition
Green	Yellow		1	High temperature reached.
Green	Yellow		2	Fan unit failure. Rotation counter indicates zero speed for one of the lateral trays. May be the result of fan tray removal.

Table 43 LED states and SSD codes during warning conditions

Active LED	Warning LED	Error LED	SSD Code	Condition
Green	Yellow		3	Power supply failure. Failed to detect one of the power supplies. May be the result of the removal of one of the power supplies.
Green	Yellow		4	FDD low sector count (40 backup sectors remaining).
Green	Yellow		5	FDD extremely low sector count (20 backup sectors remaining).

Table 43 LED states and SSD codes during warning conditions

Active LED	Warning LED	Error LED	SSD Code	Condition
Green		Red	1	Failed to identify FDD. Possibly due to removal of FDD card.
Green		Red	2	Failed to initialize NPE card.
Green		Red	3	Critical threshold reached (95C for NPE). The system will reboot.
Green		Red	4	Full fan assembly failure (both trays). The system will reboot.
Green		Red	5	Application initialization failure. Startup manager failed to initialize all the components of the system. The system will reboot.
Green		Red	6	Lost connectivity with ethernet interface. Possible failure of NPE card. The system will reboot.
Green		Red	7	MF 1000 card failure. Backup sectors exhausted.
Green		Red	8	NP 4000 card initialization failure. Firmware self test (BIST) has detected failure in one or more components (memory, bus, interconnects).

Table 44 LED states and SSD codes during error conditions

A.3.3 Back panel

Figure 33 depicts the back panel features of the HiPath Wireless Controller C2400.

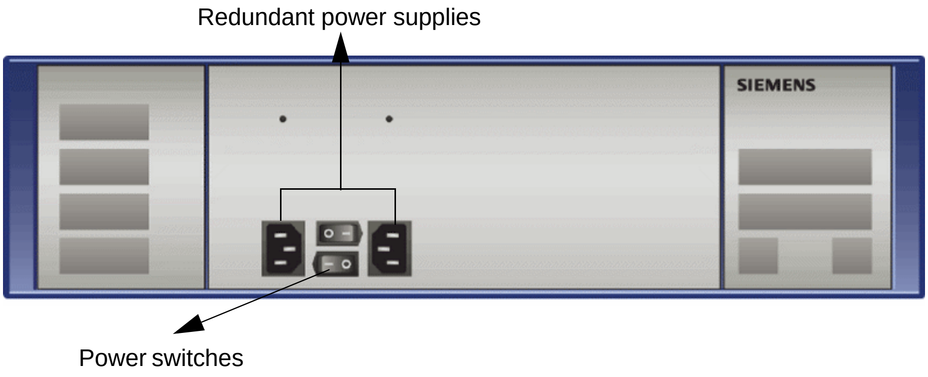


Figure 33 HiPath Wireless Controller C2400 back panel

A.4 HiPath Wireless Controller C20

A.4.1 Front panel

Figure 34 depicts the front panel features of the HiPath Wireless Controller C20

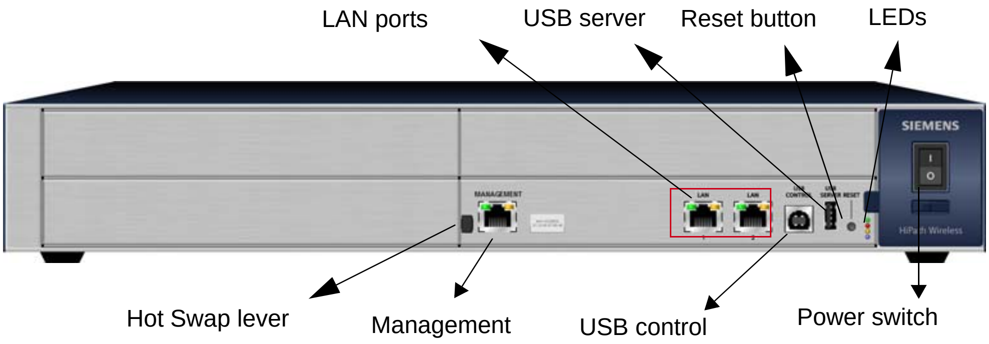


Figure 34 HiPath Wireless Controller C20 front panel

Note: The hot swap lever is not enabled in the current release. Pulling the hot swap lever will not affect the normal operation if the HiPath Wireless Controller C20 is already running. However, if you attempt to reboot the HiPath Wireless Controller C20 with the hot swap lever pulled out, the controller will fail to reboot. If you pull the hot swap lever while the HiPath Wireless Controller C20 is in operation, the Hot Swap LED will light up.

The HiPath Wireless Controller C20 has four lights on its front panel.

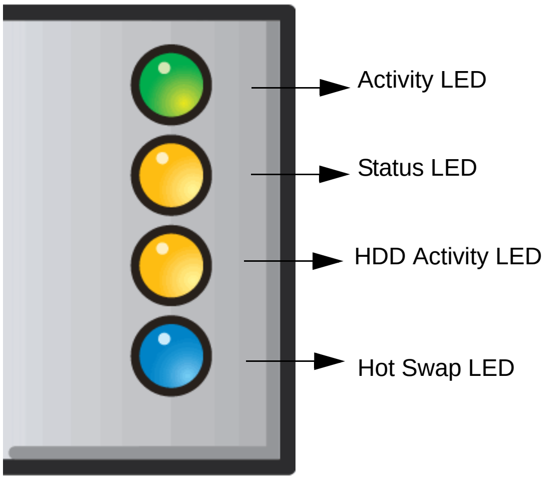


Figure 35 HiPath Wireless Controller C20 LED lights

The functional definitions of the HiPath Wireless Controller C20 LEDs are provided below:

- ACTIVITY LED – Indicates the CPU activity, including the amount of traffic carried to and from the Wireless APs.
- STATUS LED – Indicates the normal state of the HiPath Wireless Controller as seen by the system’s software. This LED covers all stages of the HiPath Wireless Controller, ranging from restarting to shutting-down. As long as the HiPath Wireless Controller is running normally, this LED will remain lit.

Note: When the system configuration is in progress, the **Activity** and **Status** LEDs are set to Amber and blink on a two-second interval.

- HDD Activity LED – Reports Hard Drive Device (HDD) activity.
- Hot Swap LED – Indicates that the hot swap lever on the HiPath Wireless Controller is pulled out.

A.4.2 LED states

The description of the HiPath Wireless Controller C20 LED status and activity states is provided below.

Status LED	Activity LED	Condition
Blinking Amber	Green	Power up (BIOS, POST)
Blinking Amber (2 second rate)	Blinking Amber (2 second rate)	System configuration in progress
Off	Green	System booting (failed to boot)
Off	Green	Start up manager: task started
Solid Green	Blinking Green	Start up manager: task completes startup – all components active
Solid Amber	Blinking Green	A component fails to start or needs restarting. (startup manager task retrying that component)
Green	Blinking Red	Possible hardware failure (no more retries)
Solid Red	Off	A component fails (no more retries)
Blinking Red	Off	System about to reset by watchdog
Solid Red	Solid Red	System shutdown / halt (requires a manual reboot)

Table 45 HiPath Wireless Controller C20 LED states and their description

- LED 3 – HDD Activity LED – Orange/Amber
- HDD Activity LED is off when HDD is not in use
- HDD Activity LED is on when HDD is in use
- LED 4 – Hot Swap LED – Blue
- Solid Blue when the hot swap button is pulled out

A.4.3 Back panel

Figure 36 depicts the back panel features of the HiPath Wireless Controller C20.

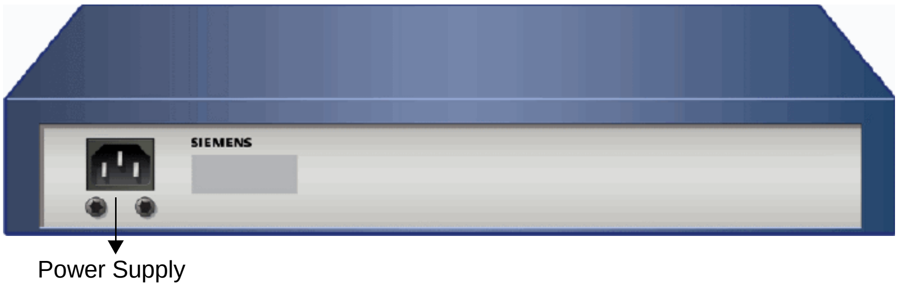


Figure 36 HiPath Wireless Controller C20 back panel

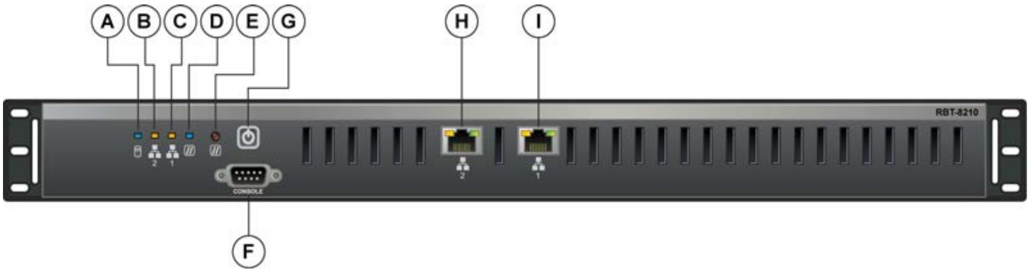
A.5 HiPath Wireless Controller C20N

For information on HiPath Wireless Controller C20N hardware, see the *HiPath Wireless Controller Module for Enterasys Matrix ® N-Series, Hardware Installation Guide*, at http://www.enterasys.com/support/manuals.

A.6 HiPath Wireless Controller CRBT8210/8110

A.6.1 Front panel

Figure 37 depicts the front panel features of the HiPath Wireless Controller CRBT8210/8110. Table 46 describes the control button functions and Table 47 describes the LED status.



A. Hard drive activity LED

B. NIC 2 activity LED

C. NIC 1 activity LED

D. Status/Power LED

E. Reset button

F. Console port connector

G. Power button

H. NIC2 connector (10/100/1000 Mbit) CRBT8110
NIC2 RJ-45 connector (10/100/1000 Base-T) CRBT8210

I. NIC1 connector (10/100/1000 Mbit)
NIC1 RJ-45 connector (10/100/1000 Base-T) CRBT8210

Figure 37 HiPath Wireless Controller CRBT8210/8110 front panel

Button	Function
Power	Toggles the system power on/off.
Reset	Performs a soft system reboot.

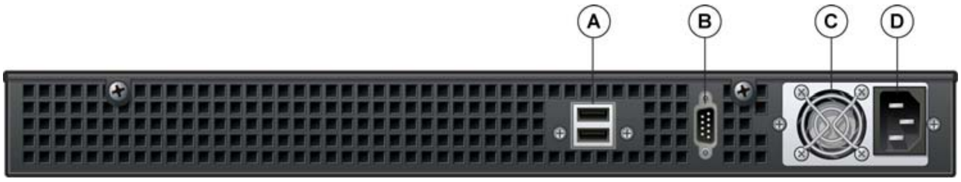
Table 46 Control button functions

LED	Function
NIC1 activity NIC2 activity	• A continuous amber light indicates a link between the system and the network to which it is connected. • A blinking amber light indicates network activity.
Status/Power	• A continuous blue light indicates that the system has power applied to it. • No light indicates that the system does not have power applied to it.
Hard drive disk status	• A continuous blue light indicates a hard drive disk fault. • A blinking blue light indicates hard drive activity.

Table 47 LED indicator status

A.6.2 Back panel

Figure 38 depicts the back panel features of the HiPath Wireless Controller CRBT8110.



A. USB connectors

B. Video connector

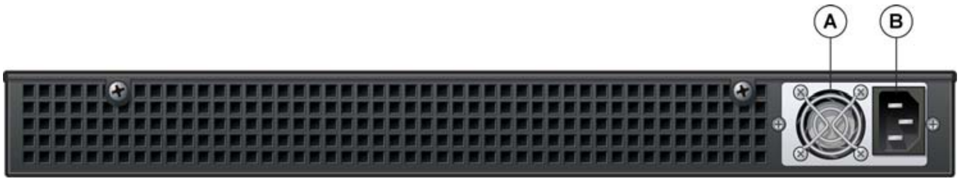
C. Power supply

D. Power connector

Figure 38 HiPath Wireless Controller CRBT8110 back panel

Note: The HiPath Wireless Controller CRBT8110 is equipped with two USB connectors on the back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

Figure 39 depicts the back panel features of the HiPath Wireless Controller CRBT8210.



A. Power supply

B. Power connector

Figure 39 HiPath Wireless Controller CRBT8210 back panel

B Regulatory information

Warning: Warnings identify essential information. Ignoring a warning can lead to problems with the application.

This appendix provides regulatory information for the HiPath Wireless Controller C20N/C20/C2400/C4110/C5110 and the HiPath Wireless AP models:

- AP 2610/2620 (AP26XX series)
- AP 3605/3610/3620 (AP36XX series)

Note: Throughout this appendix, the term ‘Wireless AP’ refers to both AP models (AP26XX series and AP36XX series). Specific AP models are only identified in this appendix where it is necessary to do so.

Note: For technical specifications and certification information for the HiPath Wireless Outdoor AP, models AP 2650/2660, see the *HiPath Wireless Outdoor AP Installation Guide.*

Configuration of the Wireless AP frequencies and power output are controlled by the regional software license and proper selection of the country during initial installation and set-up. Customers are only allowed to select the proper country from their licensed regulatory domain related to that customer’s geographic location, thus allowing the proper set-up of access points in accordance with local laws and regulations. The Wireless AP must not be operated until properly configured with the correct country setting or it may be in violation of the local laws and regulations.

Warning: Changes or modifications made to the HiPath Wireless Controller or the Wireless APs which are not expressly approved by Siemens could void the user's authority to operate the equipment.

Only authorized Siemens service personnel are permitted to service the system. Procedures that should be performed only by Siemens personnel are clearly identified in this guide.

Note: The HiPath Wireless Controllers and the Wireless APs are in compliance with the European Directive 2002/95/EC on the restriction of the use of certain hazardous substances (RoHS) in electrical and electronic equipment.

B.1 HiPath Wireless Controller C20N/C20/C2400/C4110/C5110

Conformance standards and directives

Safety

- UL 60950-1 (U.S)
- CSA C22.2 No.60950-01-03 (Canada)
- 2006/95/EC Low Voltage Directive (LVD)
- EN 60950-1 (Europe)
- IEC 60950-1 with applicable National Differences
- AS/NZS 60950.1 (Australia/New Zealand)

EMC (Emissions / Immunity)

- FCC Part 15, Subpart B, Class A (North America)
- ICES-003, Class A (Canadian Emissions)
- 2004/108/EC EMC Directive
- EN 55022: Class A (European Emissions)
- ENEN 55024: includes EN 61000-4-2,3,4,5,6,11 (European Immunity)
- EN 61000-3-2: (Harmonics)
- EN 61000-3-3: (Flicker)
- IEC/CISPR 22: Class A (International Emissions)
- IEC/CISPR 24: includes IEC/EN 61000-4-2,3,4,5,6,11 (International Immunity)
- Australia/New Zealand AS/NZS 3548 via EU standards (ACMA)

RoHS

- European Directive 2002/95/EC

B.1.1 Rack mounting your system

Refer to the following guidelines when setting up your HiPath Wireless Controllers and Wireless APs.

Elevated operating ambient

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Reduced air flow

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical loading

Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit overloading

Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable earthing

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

B.2 Wireless APs 26XX and 36XX

This device is suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code, and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1.

B.2.1 Wi-Fi certification

The AP26XX is Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g. The AP2610/20 Wireless APs with internal and external antennas are designed and intended to be used indoors.

The AP36XX is Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g/n. The AP36XX Wireless APs with internal and external antennas are designed and intended to be used indoors.

Wireless AP model	Wi-Fi certification ID
AP2605	WFA7482
AP2610	WFA7432
AP2620	WFA7387
AP2650	WFA7386
AP2660	WFA7431
AP3605	WFA9173
AP3610	WFA6025
AP3620	WFA5917

Table 48 Wireless AP Wi-Fi certification ID

Note: Operation in the European Community and rest of the world may be dependant on securing local licenses, certifications, and regulatory approvals.

B.2.2 AP2620 external antenna AP

Approved external antennas

The AP2620 external antenna APs can also be used with optional certified external antennas:

- The external antennas on the AP2620 must be identical.
- Any unused antenna ports must be terminated when an external antenna is used with the AP2620.

Antenna diversity

There are some limitations for using different antennas and Tx/Rx diversity:

- If **Alternate** antenna diversity is used for Tx or Rx, then the same antenna model must be used as left and right antennas. In addition, if cables are used to connect external antennas, the cables must be of the same length and similar attenuation. If these rules are not respected, antenna diversity will not function properly and there will be degradation in the link budget in both directions.
- You can choose to install only one antenna provided that both Tx and Rx diversity are configured to use that antenna and only that antenna. You can choose to install one antenna for 11b/g band and one antenna for 11a band, provided that the antenna diversity is configured appropriately on both radios.

Sensor support

Changing the antenna on sensors is not supported (at this stage) for the following reasons:

- The sensor factors the antenna gain and pattern in its calculations and therefore it needs to know the antenna type and gain.
- The sensor operating in mitigation mode becomes a transmitter and must obey the same CTLs as the normal AP software.
- Neither the sensor nor the HiPath Wireless Manager HiGuard support configuring the antenna.

B.2.3 AP3620 external antenna AP

Approved external antennas

The AP3620 external antenna APs can also be used with optional certified external antennas:

- Any unused antenna ports must be terminated when an external antenna is used with the AP3620.

B.2.4 United States

B.2.4.1 FCC Declaration of Conformity Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential and business environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause harmful interference, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment or devices.
- Connect the equipment to an outlet other than the receiver's.
- Consult a dealer or an experienced radio/TV technician for suggestions.

B.2.4.2 USA conformance standards

This equipment meets the following conformance standards:

Safety

- UL 60950-1
- UL 2043 Plenum Rated as part of UL 60950-1. Suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code.

EMC

- FCC CFR 47 Part 15, Class B

Radio transceiver

- CFR 47 Part 15.247, Subpart C
- CFR 47 Part 15.407, Subpart E

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

Warning: The Wireless APs must be installed and used in strict accordance with the manufacturer's instructions as described in this guide and related documentation for the device to which the Wireless AP is connected. Any other installation or use of the product violates FCC Part 15 regulations.

Operation of the Wireless AP is restricted for indoor use only, specifically in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(e).

This Part 15 radio device operates on a non-interference basis with other devices operating at the same frequency when using antennas provided or other Siemens certified antennas. Any changes or modification to the product not expressly approved by Siemens could void the user's authority to operate this device.

For the product available in the USA market, only channels 1 to 11 can be operated. Selection of other channels in the 2.4 GHz band is not possible.

B.2.4.3 FCC RF Radiation Exposure Statement

The Wireless AP complies with FCC RF radiated exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device has been tested and has demonstrated compliance when simultaneously operated in the 2.4 GHz and 5 GHz frequency ranges. This device must not be co-located or operated in conjunction with any other antenna or transmitter.

Caution: The radiated output power of the Wireless AP is below the FCC radio frequency exposure limits as specified in “Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields” (OET Bullet 65, Supplement C). This equipment should be installed and operated with a minimum distance of 25 cm between the radiator and your body or other co-located operating antennas. When using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 34cm.

B.2.4.4 External antennas

The AP2620/AP3620 external antenna APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see Section B.2.8, “AP2620/AP3620 approved external antennas”.

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

When using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 34cm.

B.2.5 Canada

B.2.5.1 Industry Canada Compliance Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of Industry Canada.

Cet appareil numerique respecte les limites de bruits radioelectriques applicables aux appareils numeriques de Classe B prescrites dans la norme sur le materiel brouilleur: "Appareils Numeriques," NMB-003 edictee par le Industrie Canada.

This device complies with Part 15 of the FCC Rules and Canadian Standard RSS-210. Operation is subject to the following conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.
- This Class B digital apparatus complies with Canadian ICES-003.
- Operation in the 5150-5250 MHz band is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
- Please note that high power radars are allocated as primary users (meaning they have priority) and can cause interference in the 5250-5350 MHz and 5470-5725 MHz bands of LE-LAN devices.
- For the product available in the Canadian market, only channels 1 to 11 can be operated. Selection of other channels in the 2.4 GHz band is not possible.

B.2.5.2 Canada conformance standards

This equipment meets the following conformance standards:

Safety

- C22.2 No.60950-1-03
- UL 2043 Plenum Rated as part of UL 60950-1. Suitable for use in environmental air space in accordance with Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1

EMC

- ICES-003, Class B

Radio transceiver

- RSS-210 (2.4 GHz and 5GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

B.2.5.3 External antennas

The AP2620/AP3620 external antenna APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see Section B.2.8, “AP2620/AP3620 approved external antennas”.

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

When using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 34cm.

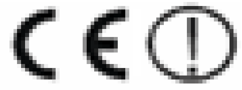
B.2.6 European community

The Wireless APs are designed for use in the European Union and other countries with similar regulatory restrictions where the end user or installer is allowed to configure the Wireless AP for operation by entry of a country code relative to a specific country. Upon connection to the controller, the software will prompt the user to select a country code. After the country code is selected, the controller will set up the Wireless AP with the proper frequencies and power outputs for that country code.

Although outdoor use may be allowed and may be restricted to certain frequencies and/or may require a license for operation, the Wireless AP is intended for indoor use and must be installed in a proper indoor location. Use the installation utility provided with the controller software to ensure proper set-up in accordance with all European spectrum usage rules. Contact local Authority for procedure to follow and regulatory information. For more details on legal combinations of frequencies, power levels and antennas, contact Siemens.

Declaration of Conformity with R&TTE Directive of the European Union 1999/5/ EC

The following symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).



B.2.6.1 Declaration of Conformity in Languages of the European Community

English

Hereby, Siemens, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Finnish

Valmistaja Siemens vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Dutch

Hierbij verklaart Siemens dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Bij deze verklaart Siemens dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.

French

Par la présente Siemens déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Par la présente, Siemens déclare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.

Swedish

Härmed intygar Siemens att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Danish

Undertegnede Siemens erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

German

Hiermit erklärt Siemens die Übereinstimmung des "WLAN Wireless Controller bzw. Access Points" mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG.

Greek

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Siemens ΔΗΛΩΝΕΙ ΟΤΙ Radio LAN device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Icelandic

Siemens lysir her med yfir að thessi bunadur, Radio LAN device, uppfyllir allar grunnkrofur, sem gerdar eru i R&TTE tilskipun ESB nr 1999/5/EC.

Italian

Con la presente Siemens dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Spanish

Por medio de la presente Siemens declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Portuguese

Siemens declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Malti

Hawnhekk, Siemens, jiddikjara li dan Radio LAN device jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

New Member States requirements of Declaration of Conformity

Estonian — Käesolevaga kinnitab Siemens seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Hungary — Alulírott, Siemens nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

Slovak — Siemens týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Czech — Siemens tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."

Slovenian — Šiuo Siemens deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Latvian — Ar šo Siemens deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem

Lithuanian — Siemens deklaruoja, kad Radio LAN device atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".

Polish — Niniejszym, Siemens, deklaruję, że Radio LAN device spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

B.2.6.2 European conformance standards

This equipment meets the following conformance standards:

Safety

- 2006/95/EC Low Voltage Directive (LVD)
- IEC/EN 60950-1 + National Deviations

EMC (Emissions / Immunity)

- 2004/108/EC EMC Directive
- EN 55011/CISPR 11, Class B, Group 1 ISM
- EN 55022/CISPR 22, Class B
- EN 55024/CISPR 24, includes IEC/EN 61000-4-2,3,4,5,6,11
- EN 61000-3-2 and -3-3 (Harmonics and Flicker)
- EN 60601-1-2 (EMC immunity for medical equipment)
- EN 50385 (EMF)
- ETSI/EN 301 489-1 & -17

Radio transceiver

- R&TTE Directive 1999/5/EC
- ETSI/EN 300 328 (2.4 GHz)
- ETSI/EN 301 893 (5 GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

RoHS

- European Directive 2002/95/EC

B.2.6.3 External antennas

The AP2620/AP3620 external antenna APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see Section B.2.8, “AP2620/AP3620 approved external antennas”.

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

When using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 34cm.

B.2.6.4 Conditions of use in the European community

The Wireless APs with internal and external antennas are designed and intended to be used indoors. Some EU countries allow outdoor operation with limitations and restrictions, which are described in this section. It is the responsibility of the end user to ensure operation in accordance with these rules, frequencies, and transmitter power output. The Wireless AP must not be operated until properly configured for the customer’s geographic location.

Caution: The user or installer is responsible to ensure that the Wireless AP is operated according to channel limitations, indoor / outdoor restrictions, license requirements, and within power level limits for the current country of operation. A configuration utility has been provided with the HiPath Wireless Controller to allow the end user to check the configuration and make necessary configuration changes to ensure proper operation in accordance with the spectrum usage rules for compliance with the European R&TTE directive 1999/5/EC.

The Wireless APs with internal and external antennas are designed to be operated only indoors within all countries of the European Community. Some countries require limited channels of operation. These restrictions are described in this section.

Caution: The Wireless AP is completely configured and managed by the HiPath Wireless Controller connected to the network. Please follow the instructions in this user guide to properly configure the Wireless AP.

• The Wireless APs require the end user or installer to ensure that they have a valid license prior to operating the Wireless AP. The license contains the region and the region exposes the country codes which allow for proper configuration in conformance with European National spectrum usage laws

• There is a default group of settings that each Wireless AP receives when it connects to the controller. There is the ability to change these settings. The user or installer is responsible to ensure that each Wireless AP is properly configured.

• The software within the controller will automatically limit the allowable channels and output power determined by the selected country code. Selecting the incorrect country of operation or identifying the proper antenna used, may result in illegal operation and may cause harmful interference to other systems.

• This device employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.

• The 5 GHz Turbo Mode feature is not enabled for use on the Wireless APs.

• The 5150- 5350 MHz band, channels 36, 40, 44, 48, 52, 56, 60, or 64, are restricted to indoor use only.

• The external antenna APs must only use antennas that are certified by Siemens.

• The 2.4 GHz band, channels 1 - 13, may be used for indoor or outdoor use but there may be some channel restrictions.

• In Greece and Italy, the end user must apply for a license from the national spectrum authority to operate outdoors.

• In France, outdoor operation is not permitted in the 2.4 GHz band.

B.2.6.5 European spectrum usage rules

The AP configured with approved internal or external antennas can be used for indoor and outdoor transmissions throughout the European community as displayed in Table 49. Some restrictions apply in Belgium, France, Greece, and Italy.

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116, 132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Austria	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Belgium	Indoor only	Indoor only	Indoor or outdoor *	Indoor or outdoor
Bulgaria	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Denmark	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Croatia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Cyprus	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Czech Rep.	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Estonia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Finland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
France	Indoor only	Indoor only	Indoor or outdoor	Indoor only
Germany	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Greece	Indoor only	Indoor only	Indoor (Outdoor w/License)	Indoor (Outdoor w/license)
Hungary	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Iceland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Ireland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Italy	Indoor only	Indoor only	Indoor or outdoor	Indoor (Outdoor w/license)
Latvia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Liechtenstein	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Lithuania	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Luxembourg	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Netherlands	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Malta	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Norway	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Poland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Portugal	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Romania	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Slovak Rep.	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Slovenia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor

Table 49 European spectrum usage rules

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116, 132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Spain	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Sweden	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Switzerland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Turkey	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
U.K	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor

Table 49 European spectrum usage rules (Continuation)

Note: * Belgium requires notifying the spectrum agency if deploying > 300 meter wireless links in outdoor public areas.

B.2.7 Certifications of other countries

The Wireless APs have been certified for use in various other countries. When the Wireless AP is connected to the Siemens HiPath Wireless Controller, the user is prompted to select a country code. Once the correct country code is selected, the controller automatically sets up the Wireless AP with the proper frequencies and power outputs for that country code.

Note: It is the responsibility of the end user to select the proper country code for the country the device will be operated within or run the risk violating local laws and regulations.

Approved external antennas

The external antenna Wireless APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see Section B.2.8, “AP2620/AP3620 approved external antennas”.

Other country specific compliance standards, approvals and declarations

- IEC 60950-1 CB Scheme + National Deviations
- AS/NZS 60950.1 (Safety)
- AS/NZS 3548 (Emissions via EU standards – ACMA)
- AS/NZS 4288 (Radio via EU standards)

- EN 300 328 (2.4 GHz)
- EN 301 893 (5 GHz)
- EN 301 489-1 & -17 (RLAN)
- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

B.2.8 AP2620/AP3620 approved external antennas

The AP2620/AP3620 external antenna APs can be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested and approved for use with the external antenna models.

Model	**Application**	**Shape**	**Gain (dBi)**	**Frequency (MHz)**	**Connector Type**
WS-ANT01	outdoor	omni	4	2400-2500 5150-5900	RPSMA
WS-AO-DS05360	outdoor	omni	5	2400-2500 5150-5350	Reverse Polarity Type-N
WS-AIO-5S12060	indoor	panel	12	2400-2500 4900-5990	Reverse Polarity Type-N
WS-AI-2S03360	indoor	omni	3.5	2400-2500	RPSMA
WS-AI-DS06360	indoor	omni	5 6	2300-2700 4900-6000	RPSMA
WS-AIO-DS05120	indoor/outdoor	panel	5	2400-2500	Reverse Polarity Type-N
WS-AIO-2S07060	indoor/outdoor	panel	7.5	2300-2600 4900-6000	Reverse Polarity Type-N
WS-AIO-5S17017	indoor/outdoor	panel	17	5470-5850	Reverse Polarity Type-N
WS-AIO-2514090	indoor/outdoor	panel	14	2400-2485	Reverse Polarity Type-N
WS-AIO-5S15090	indoor/outdoor	panel	15	4900-6000	Reverse Polarity Type-N
WS-AIO-2S18018	indoor/outdoor	panel	18	2300-2500	Reverse Polarity Type-N

Table 50 List of FCC/IC/ETSI approved antennas — AP2620

Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Connector Type
WS-ANT02	indoor	omni	4	2400-2500 5150-5900	RPSMA
WS-AO-DS05360	outdoor	omni	5	2400-2500 5150-5350	Reverse Polarity Type-N
WS-AO-D16060	outdoor	60 degree sector directional, 2 inputs	16	5150-5875	Reverse Polarity Type-N
WS-AO-5D23009	outdoor	panel, 2 inputs	23	5150-5875	Reverse Polarity Type-N
WS-AI-DT04360	indoor	omni, 3 inputs	3 4	2400-2500 4900-5990	RPSMA, 3ea.
WS-AI-DT05120	indoor	120 degree sector directional, 3 inputs	5	2300-2700 4900-6100	RPSMA

Table 51 List of FCC/IC/ETSI approved antennas — AP3620

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

When using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 34cm.

B.2.9 Certified 3rd party antennas

Table 52 lists the 3rd party antennas that are supported for AP2620, AP260-1, AP3620 and AP3620-1 models for ETSI and FCC. These antennas are supported only for existing customers prior to V7.11.

AP	Regulatory	Manufacturer	Part Number	Type	Usage	Frequency	Gain	Connector
2620	FCC/IC	Cushcraft	SR2405135D	Sector, 135 Deg Single Feed	Indoor	2.4	5	N-F
2620	FCC/IC	Cushcraft	S24493DS	Omni, Dual Feed	Indoor	2.4, 5	3	Reverse TNCx2
2620	FCC/IC	Cushcraft	SL24513P	Omni, Single Feed	Indoor	2.4, 5	3	SMA-F
2620	FCC/IC	Cushcraft	S24497P	60 Deg Sector, Single Feed	Indoor	2.4, 5	7	Reverse TNC
2620	FCC/IC	Hyperlink	HG2458CU	Omni, Single Feed	Indoor	2.4, 5	3	N-F

Table 52 Certified 3rd party antennas for use with AP2620, AP260-1, AP3620 and AP3620-1 models

AP	Regulatory	Manufacturer	Part Number	Type	Usage	Frequency	Gain	Connector
2620	FCC/IC	Maxrad	MDO24005PT	Omni, Dual Feed	Indoor	2.4	5.2	SMA, TNC, N
2620	ETSI	Huber and Suhner	SOA 2454/360/7/20/DF	Omni	Outdoor	2.4, 5	6 & 8	N-F
2620	ETSI	Huber and Suhner	SWA 2459/360/4/45/V	Omni	Outdoor	2.4, 5	4	N-F/SMA-F
2620	ETSI	Huber and Suhner	SPA 2456/75/9/0/DF	Plannar	Outdoor	2.4, 5	9	SMA-F/ TNC-F/ QN-F
2620	ETSI	Huber and Suhner	SOA 2400/360/4/0/DS	Omni	Outdoor	2.4, 5	3.5	N-F/TNC-F
2620	ETSI	Huber and Suhner	SWA 0859/360/4/10/V	Omni	Outdoor	2.4, 5	7	N-F/TNC-F
2620	ETSI	Huber and Suhner	SPA 2400/80/9/0/DS	Plannar	Outdoor	2.4	8.5	SMA-F/ TNC-F/ QMA-F
2620	ETSI	Huber and Suhner	SPA 2400/40/14/0/DS	Plannar	Outdoor	2.4	13.5	N-F/TNC-F
3620	FCC/IC	Cushcraft	SR249120D	120 Deg, Sector, Single Feed	Indoor	2.4, 5	5	RPSMA
3620	FCC/IC	Cushcraft	S24493TS	Omni, Triple Feed	Indoor	2.4, 5	3	RPSMA 3 ea.
3620	FCC/IC	Cushcraft	SL24513WP	Omni	Indoor	2.4, 5	3	RPSMA
3620	FCC/IC	Cushcraft	S24497P	60 Deg Sector, Single Feed	Indoor	2.4, 5	7 & 8	RPSMA
3620	FCC/IC	Hyperlink	HG2458CU	Omni	Indoor	2.4, 5	3	N-F
3620	FCC/IC	Maxrad	MDO24005PT	Omni, Dual Feed	Indoor	2.4	5.2	RPSMA
3620	ETSI	Huber and Suhner	SOA 2454/360/7/20/DF	Omni	Outdoor	2.4, 5	6 & 8	N-F
3620	ETSI	Huber and Suhner	SWA 2459/360/4/45/V	Omni	Outdoor	2.4, 5	4	N-F/SMA-F
3620	ETSI	Huber and Suhner	SPA 2456/75/9/0/DF	Plannar	Outdoor	2.4, 5	9	SMA-F/ TNC-F/ QN-F
3620	ETSI	Huber and Suhner	SOA 2400/360/4/0/DS	Omni	Outdoor	2.4, 5	3.5	N-F/TNC-F
3620	ETSI	Huber and Suhner	SWA 0859/360/4/10/V	Omni	Outdoor	2.4, 5	7	N-F/TNC-F
3620	ETSI	Huber and Suhner	SPA 2400/80/9/0/DS	Plannar	Outdoor	2.4	8.5	SMA-F/ TNC-F/ QMA-F
3620	ETSI	Huber and Suhner	SPA 2400/40/14/0/DS	Plannar	Outdoor	2.4	13.5	N-F/TNC-F

Table 52 *Certified 3rd party antennas for use with AP2620, AP260-1, AP3620 and AP3620-1 models*

C optiPoint WL2 Configuration

This appendix describes the recommended configuration for the optiPoint WL2 wireless telephone with the HiPath Wireless LAN Solution. In addition, corresponding configurations should be made on the PBX, if applicable.

Update your optiPoint WL2 wireless telephone software to the latest available firmware. The following information in this appendix refers to an optiPoint WL2 telephone running firmware version 50.002.43.00079.

Note: You can also use the VNS wizard to configure the HiPath Wireless Controller for use with optiPoint wireless telephones. For more information, see Section 6.4.2, “Creating a voice VNS using the VNS wizard”, on page 284.

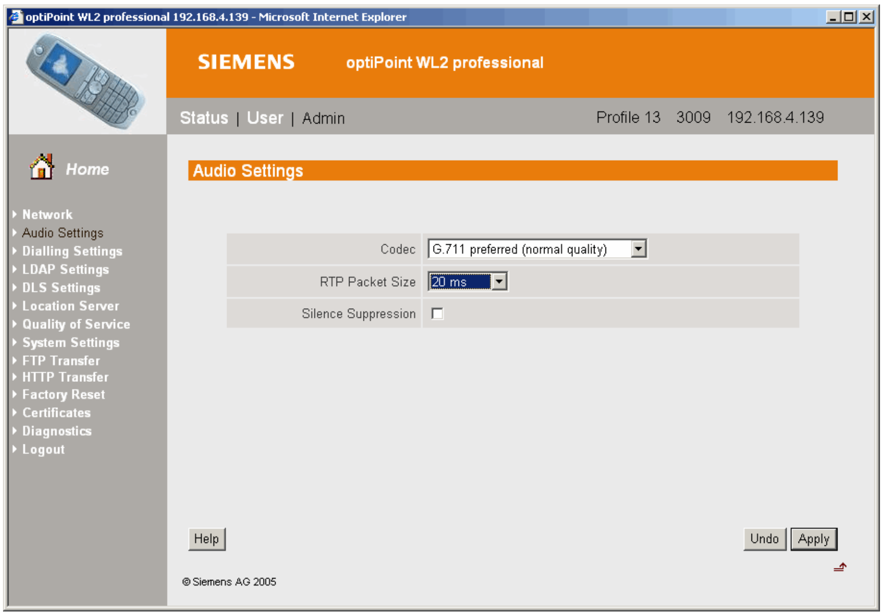
C.1 optiPoint WL2 wireless telephone configuration

To configure audio settings:

1. Launch your Web browser, and in the browser address bar type the optiPoint WL2’s IP address. The **optiPoint WL2 professional Handset** screen is displayed.
2. In the optiPoint WL2 professional menu, click **Admin**. The **Network: Profile Selection** screen is displayed.
3. In the left pane, click **Audio Settings**. The **Audio Settings** screen is displayed.
4. Configure the following audio settings:
   - In the **Codec** drop-down list, click **G.711 preferred (normal quality)**.

     The alternative **G729** codec would only provide a small increase in capacity at the expense of a significant increase in sensitivity to lost packets and degradation of quality.
   - In the **RTP Packet Size** drop-down list, click **20ms**.

     The **10ms** setting would not improve voice quality, but it would significantly decrease the per-AP voice capacity. The **30ms** setting would worsen the impact of lost packets while roaming.
   - Clear the **Silence Suppression** checkbox. The **Silence Suppression** option should be disabled.



Audio Settings

Codec	G.711 preferred (normal quality)
RTP Packet Size	20 ms
Silence Suppression	□

To configure Quality of Service protocol settings:

1. In the left pane, click **Quality of Service**. The **Quality of Service: Protocol Settings** screen is displayed.

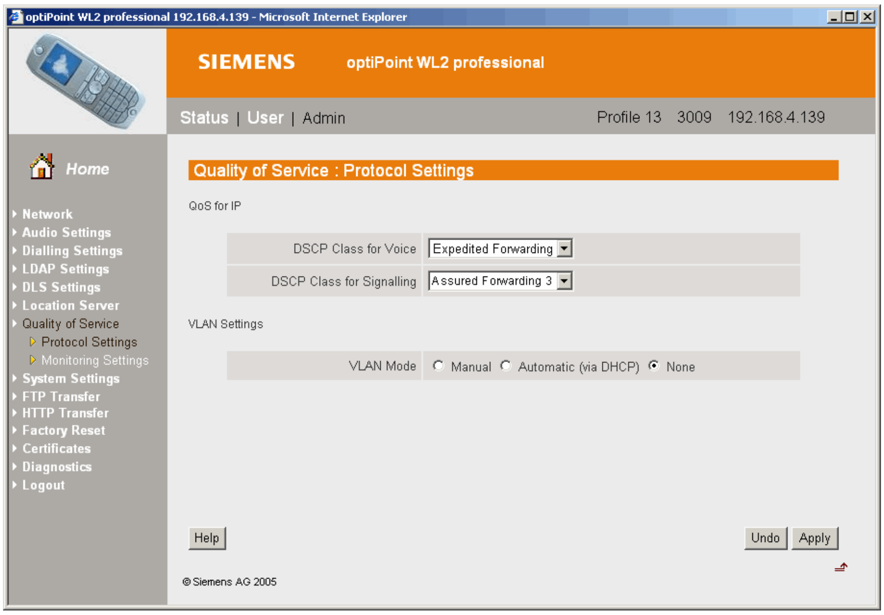
2. Configure the following Quality of Service settings:

   - In the **DSCP Class for Voice** drop-down list, click **Expedited Forwarding** to ensure maximum voice priority.

   - In the **DSCP Class for Signalling** drop-down list, click **Assured Forwarding 3**.

     Under normal conditions **Assured Forwarding 3** ensures a more reliable delivery for Signaling than for Voice (more retries) at the expense of a potential higher delay.

   - In the **VLAN Settings** section, select **None**.



Quality of Service : Protocol Settings

QoS for IP

DSCP Class for Voice	Expedited Forwarding
DSCP Class for Signalling	Assured Forwarding 3

VLAN Settings

VLAN Mode ○ Manual ○ Automatic (via DHCP) ● None

To configure WLAN settings:

1. In the left pane, click **Network**. The **Network: Profile Selection** screen is displayed.

2. In the **List of Profiles**, click **Edit** for the profile you want to configure. The **Network: Profile Name** screen is displayed.

3. In the left pane, click **WLAN**. The **Network: WLAN for profile** screen is displayed.

4. Configure the following WLAN settings:

   - In the **Output Power (in%)** drop-down list, click **100**.

     Use the maximum **100%** unless there is a reason to reduce it.

   - In the **Transmission Rate** drop-down, click **Auto**.

Note: When the **Transmission Rate** is set to a value, it does not force the phone to only use that particular PHY transmission rate. Instead, it forces the phone to only use PHY rates that are smaller or equal to the set rate.

   - In the **Fragmentation Threshold** box, ensure that the default value **2346** is used.

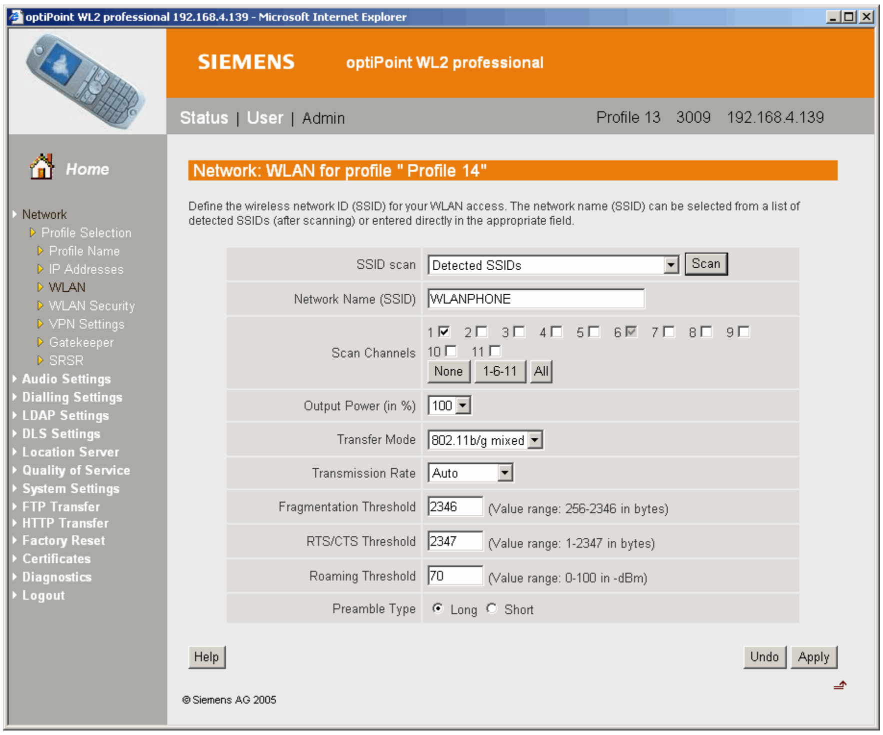
   - In the **RTS/CTS Threshold** box, ensure that the default value **2347** is used.

   - In the **Roaming Threshold** box, type a roaming threshold between the range of -75 dBm to -65 dBm, depending on the parameters of the deployment.

A larger value, for example -65 dBm will cause the phone to scan for alternate Wireless APs more often, which will result in more wireless traffic and slightly decreased battery life. A smaller value, for example -75 dBm will cause the phone to roam too late, causing voice interruptions during roaming.

- In the **Preamble Type** section, select **Short**. The short preamble provides for higher voice capacity.

  If legacy pre-11b devices are present in the coverage area or you are unsure if legacy pre-11b devices are present in the coverage area, select **Long**.



Network: WLAN for profile " Profile 14"

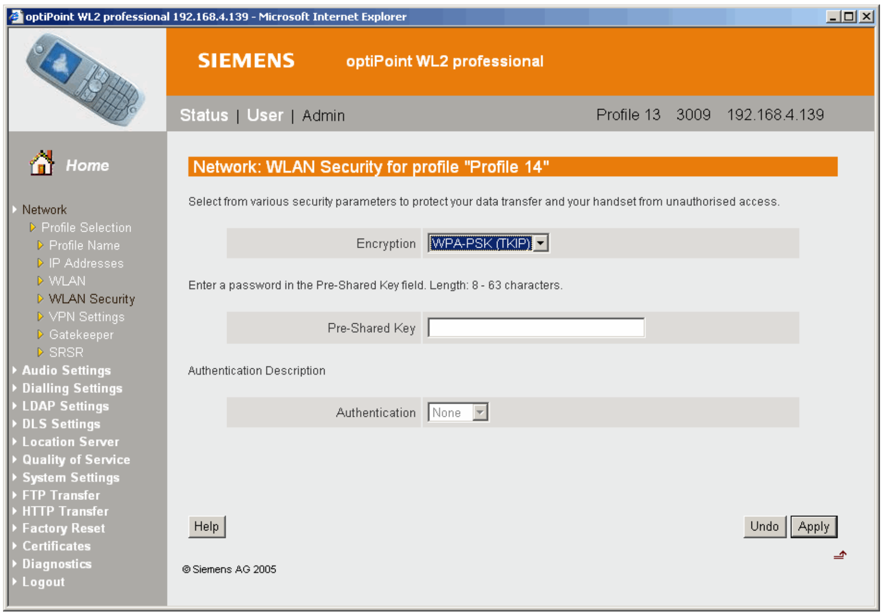
Define the wireless network ID (SSID) for your WLAN access. The network name (SSID) can be selected from a list of detected SSIDs (after scanning) or entered directly in the appropriate field.

SSID scan	Detected SSIDs ▾ [Scan]
Network Name (SSID)	WLANPHONE
Scan Channels	1 ☑ 2 □ 3 □ 4 □ 5 □ 6 ☑ 7 □ 8 □ 9 □ 10 □ 11 □ [None] [1-6-11] [All]
Output Power (in %)	100 ▾
Transfer Mode	802.11b/g mixed ▾
Transmission Rate	Auto ▾
Fragmentation Threshold	2346 (Value range: 256-2346 in bytes)
RTS/CTS Threshold	2347 (Value range: 1-2347 in bytes)
Roaming Threshold	70 (Value range: 0-100 in -dBm)
Preamble Type	● Long ○ Short

© Siemens AG 2005

To configure WLAN security settings:

1. In the left pane, click **Network**. The **Network: Profile Selection** screen is displayed.
2. In the left pane, click **WLAN Security**. The **Network: WLAN Security for profile** screen is displayed.
3. Configure the following WLAN security settings:
   - Click **WPA-PSK**.



Network: WLAN Security for profile "Profile 14"

Select from various security parameters to protect your data transfer and your handset from unauthorised access.

Encryption: WPA-PSK (TKIP)

Enter a password in the Pre-Shared Key field. Length: 8 - 63 characters.

Pre-Shared Key:

Authentication Description

Authentication: None

C.2 HiPath Wireless Controller configuration

The easiest way to configure a voice VNS is to use the VNS Creation Wizard. Refer to Section 6.4.2, “Creating a voice VNS using the VNS wizard”, on page 284.

The following settings must be configured on the HiPath Wireless Controller.

- A dedicated VNS must be used for WL2 phones. No other non-voice clients should be allowed in this VNS.
- The VNS must be a non-RADIUS VNS.

To configure a WL2 Voice Topology:

1. In the Layer 3 area, from the **DHCP** drop-down list, select **Local Server**, then click **Configure**.
2. Select the **Enable DLS DHCP Option** checkbox.
3. In the **DLS Address** box, type the IP address or the DNS name of the DLS. In the accompanying box, type the DLS port number. The default is **18443**.

For more information about configuring a Topology, see Section 6.8, “Configuring a Topology”, on page 319.

To configure a WL2 WLAN Service:

1. Click the **Privacy** tab.
2. Configure the following privacy settings:

- The privacy settings on the HiPath Wireless Controller must match those on the optiPoint WL2 phone.
- If the optiPoint WL2 phone is configured to use WPA-PSK, select the **WPA-PSK** option for the VNS.

3. Click the **QoS** tab.
4. Configure the following QoS policy settings:
   - For good voice quality and battery life, select **WMM**.
   - If the VNS is shared with legacy devices that require priority but do not support **WMM**, select **Legacy**.
   - If applicable, select **802.11e** or **Enable U-APSD**. (The next release of the optiPoint WL2 may require .11e support).

Note: The **Turbo Voice** and **Use Global Admission Control for Voice (VO)** options should be cleared. These options should not be used in the same VNS as the optiPoint WL2. These features are not currently supported on the optiPoint WL2.

- The **Priority Override** option (configured on the Advanced dialog) should normally be cleared. If the phone and PBX are configured properly, the default DSCP classification should work well. If you are unsure, sniff the packets over the air and check that the voice packets are sent with priority 6 or 7 in both UL and DL directions.

For more information about configuring a WLAN Service, see Section 6.9, “Configuring WLAN Services”, on page 331.

To configure Wireless AP radio properties:

1. From the main menu, click **Wireless AP Configuration**. The **HiPath Wireless AP** screen is displayed.
2. Click the applicable radio tab, In the **Radio Mode** drop-down list, click **g.**

Note: Enable 11b only if 11b devices are used on the same VNS as the optiPoint WL2 phone.

3. Click the **Advanced** button.
4. Configure the following radio settings:

- In the **DTIM Period** box, type **5**.

Note: A **DTIM Period** value of **1** may produce better results if significant RF interference exists in your environment. Use a **DTIM Period** value of **5** unless you notice a significant improvement when using a value of **1**.

- In the **Beacon Period** box, type **100** (ms).
- In the **RTS/CTS Threshold** box, ensure that the default value **2346** is used.
- In the **Frag. Threshold** box, ensure that the default value **2346** is used.
- In the **Rx Diversity** drop-down list, click **Best**.
- In the **Tx Diversity** drop-down list, click **Alternate**.

Note: If you experience variable or unstable signals, in the **Tx Diversity** drop-down list, click **Left**.

- In the **Min Basic Rate** drop-down list, click **1Mbps** if .11b is enabled.

Note: Use a **Min Basic Rate** of **6Mbps** if you are using only optiPoint WL2 phones on the VNS, as this will increase the number of concurrent calls per AP. Use a **Min Basic Rate** of **2Mbps** or **1Mbps** if your site has sparse RF coverage.

- In the **Max Basic Rate** drop-down list, click the default maximum possible basic rate. For example, click **12 Mbps** if you are using **6 Mbps** as the **Min Basic Rate**. Otherwise, click **24 Mbps**.
- In the **Max Operational Rate** drop-down list, click the default maximum rate. For example, **54 Mbps**.
- In the **Preamble** drop-down list, click **Short**. The short preamble provides for higher voice capacity.

  If legacy pre-11b devices are present in the coverage area or you are unsure if legacy pre-11b devices are present in the coverage area, click **Long**.
- In the **Total # of Tries for Background BK** drop-down list, click **adaptive (multi-rate)**.
- In the **Total # of Tries for Best Effort BE** drop-down list, click **adaptive (multi-rate)**.
- In the **Total # of Tries for Video VI** drop-down list, click **adaptive (multi-rate)**.

- In the **Total # of Tries for Voice VO** drop-down list, click **adaptive (multi-rate)**.
- In the **Total # of Tries for Turbo Voice TVO** drop-down list, click **adaptive (multi-rate)**.

Note: At a minimum, use **adaptive (multi-rate)** for **Total # of Tries for Best Effort BE** and **Total # of Tries for Voice VO** since this will significantly improve voice quality.

- In the **Protection Mode** drop-down list, click **Auto**.
- In the **Protection Rate** drop-down list, click **11 Mbps**.
- In the **Protection Type** drop-down list, click **CTS**. The CTS protection mode allows for higher voice capacity.

  If legacy pre-11b devices are present in the coverage area or you are unsure if legacy pre-11b devices are present in the coverage area, click **RTS CTS**. RTS CTS mode provides more robust protection.

D SpectraLink Wireless Telephones

The HiPath Wireless LAN Solution, consisting of the HiPath Wireless Controller, Wireless APs, and the HiPath Wireless Convergence Software, seamlessly integrates with SpectraLink Wireless Telephones to serve mobile voice and data requirements. The standards-based architecture of HiPath Wireless LAN provides an exceptional infrastructure for voice quality and handset-reliability to the SpectraLink telephones.

D.1 Network Topology

The following image depicts a typical network topology for SpectraLink telephones.

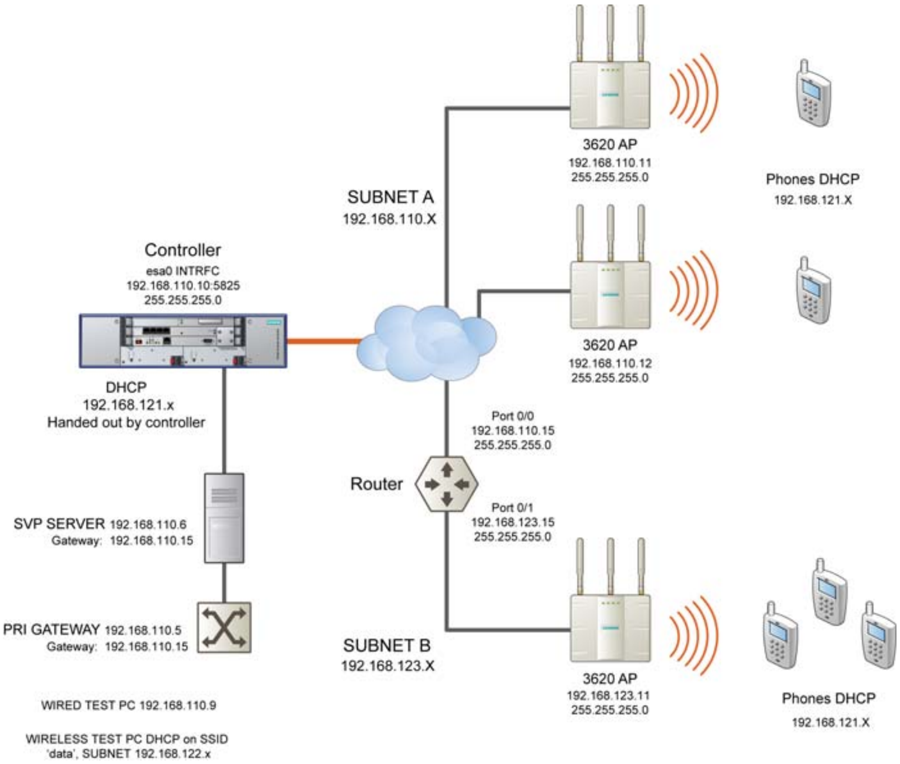


Figure 40 SpectraLink Network Topology

Note: The network topology depicted in Figure 40 is a dedicated network for SpectraLink Telephones. Other topologies are supported and can be used as required.

Note: For a successful deployment, all network elements in the SpectraLink network should be provisioned to prioritize voice data.

D.2 Configuring HiPath Wireless Controller for SpectraLink telephones

This section describes how to configure the HiPath Wireless Controller and Wireless APs for use with SpectraLink Wireless telephones.

You have to configure the following features in the HiPath Wireless Controller to set it up for SpectraLink telephones:

- Radio properties
- SSID
- Filters
- Multicast configuration
- Security
- Quality of Service (QoS)

The configuration process for SpectraLink telephones applies identically to HiPath Wireless APs, HiPath Wireless Outdoor APs and HiPath Wireless 802.11n APs, unless specified otherwise.

Note: You can also use the VNS wizard to configure the HiPath Wireless Controller for use with SpectraLink Wireless telephones. For more information, see Section 6.4.2, “Creating a voice VNS using the VNS wizard”, on page 284.

D.2.1 Setting up SSID

To set up the SSID:

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.
4. In 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.

5. 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.

Note: Siemens recommends that you choose **Bridge Traffic Locally at HWC** Topology Mode for SpectraLink network deployment.

6. In the Layer 3 area, 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 **Mask** box, type the appropriate values.
9. In the **Address Range** boxes (**from** and **to**), type the IP address range.
10. To save your changes, click **Save**.

D.2.2 Configuring filters

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 of SVP server in **IP/Subnet** and **port** boxes.
5. From the **Protocol** drop-down menu, select **UDP**.
6. Click **OK**. The new filtering rule for the SVP server is displayed in the centre pane.
7. Click **Up**. The filtering rule for the SVP server moves up, before the filter rule for **Default** filter.
8. Click Add again, then type the IP address of SpectraLink Gateway in **IP/Subnet** and **port** boxes, and then repeat steps 5 to 7.

9. Add the filtering rules for the IP addresses of all network elements as explained in steps 5 to 7.

Note: You must ensure that all the filtering rules, including the ones for SVP/ Gateway and other network elements, are moved up, before the filtering rule for the **Default** filter.

10. Select the **Allow** option of the **Default** filter.
11. To save your changes, click **Save**.

Note: You must complete the remaining configuration as explained in the subsequent sections, and then check if the deployment is working properly. If the deployment is working properly, you should deselect **Allow** option of the **Default** filter to secure the network
The secure setup in context of the network topology illustrated in Figure 40 on page 559 will be as follows:

- Allow 192.168.121.* UDP
- Allow 192.168.110.* UDP
- Allow 192.168.123.* UDP
- Disallow *.*.*.* N/A T

D.2.3 Setting up multicast configuration

Note: Before you set up multicast configuration, you must specify the physical port for routing multicast traffic on the **Wireless Controller configuration** screen.

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 SVP (224.0.1.116)** and then click **Add**.
5. Select the **Wireless Replication** checkbox.
6. To save your changes, click **Save**.

D.2.4 Setting up Security

To set up the security:

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. Select the **WPA v.2** option.
6. Under **WPA v.2** section, select **AES only** from the **Encryption** drop-down menu.

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

7. Enter the appropriate pass phrase in the **Pre-shared** key field.
8. To save your changes, click **Save**.

D.2.5 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:
   - Legacy
   - Turbo Voice

Note: If you are using HiPath Wireless APs and HiPath Wireless Outdoor APs, you must ensure that **Turbo Voice** QoS is selected to achieve best voice quality with the SpectraLink telephones.

Turbo Voice QoS does not have any effect on HiPath Wireless 802.11n APs as these APs provide best voice quality regardless of whether **Turbo Voice** QoS is selected or not.

Note: To achieve “higher call capacity”, you must ensure that **WMM** QoS is deselected.

Note: The HiPath Wireless 802.11n APs support only the **WMM** QoS. If you are using 802.11n APs, and you want to achieve “higher call capacity”, you must ensure that **WMM** QoS is deselected.
The **Turbo Voice** QoS does not have any effect on the 802.11n APs regardless of whether it is selected or not.

5. Click the **Advanced** button.
6. Under the **Priority Processing** section, select **Priority Override**.
7. Retain the default value in **Service Class** drop-down menu.
8. Retain the default value in **DSCP marking** drop-down menu.
9. To save your changes, click **Save**.

D.2.6 Setting up Radio Properties

To set up the radio for Voice Wireless LAN in HiPath Wireless AP (Models 2610/2620):

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 AP that is being used for the Voice WLAN.
3. On the **Wireless AP Configuration** screen, select the tab for the radio that is being used for Voice WLAN.
4. Click the **Advanced** button.
5. Under **Base Settings**, set the **DTIM Period** to **3**.

6. Under **Basic Radio Settings**, set the following parameters:
   - **Tx Diversity**: Set the **Tx Diversity** to either **Left** or **Right**.
   - **Total # of retries for Voice VO**: Set the **Total # of retries for Voice VO** to **adaptive (multi-rate)**.

Note: Siemens recommends that you set **Tx Diversity** to **Left**.

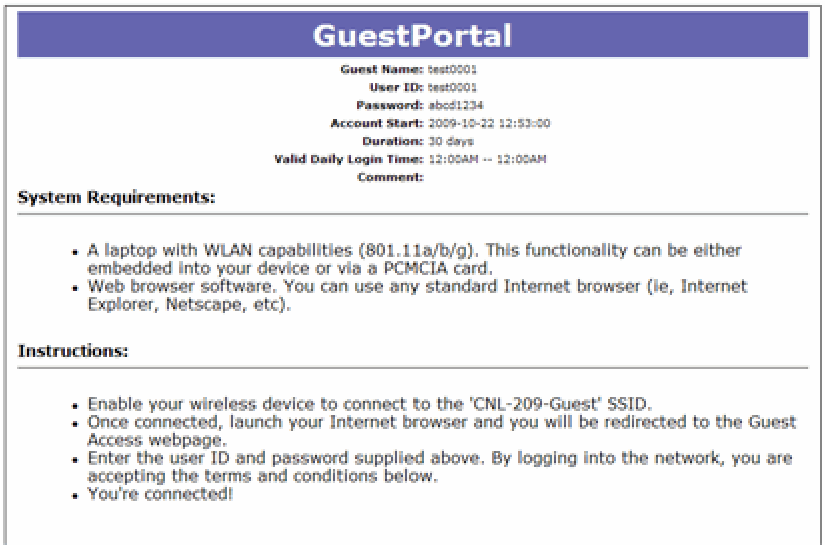
7. Retain the default values for all other parameters.
8. To save your changes, click **Save**.

To set up the radio for Voice Wireless LAN in HiPath Wireless 802.11n APs (Models AP3610/3620):

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 Voice WLAN.
3. On the **Wireless AP Configuration** screen, select the tab for the radio that is being used for the Voice WLAN.
4. Click the **Advanced** button.
5. Under **Base Settings**, set the **DTIM Period** to **3**.
6. Retain the default values for all other parameters.
7. To save your changes, click **Save**.

E Default GuestPortal source code

E.1 Ticket page



GuestPortal

Guest Name: test0001
User ID: test0001
Password: abcd1234
Account Start: 2009-10-22 12:53:00
Duration: 30 days
Valid Daily Login Time: 12:00AM -- 12:00AM
Comment:

System Requirements:

- A laptop with WLAN capabilities (801.11a/b/g). This functionality can be either embedded into your device or via a PCMCIA card.
- Web browser software. You can use any standard Internet browser (ie, Internet Explorer, Netscape, etc).

Instructions:

- Enable your wireless device to connect to the 'CNL-209-Guest' SSID.
- Once connected, launch your Internet browser and you will be redirected to the Guest Access webpage.
- Enter the user ID and password supplied above. By logging into the network, you are accepting the terms and conditions below.
- You're connected!

E.1.1 Placeholders used in the default GuestPortal ticket page

Placeholder tag	Description
!GuestName	Guest Name
!GuestComment	Guest Comment
!TimeOfDayStart	Time-of-day start
!TimeOfDayDuration	Time-of-day session duration
!SessionLifeTime	Maximum session time
!UserID	User ID for the guest
!Password	Password for the guest
!SSID	SSID to connect to
!AccountActivationTime	Account available time
!AccountLifeTime	Account life time

Table 53 Default GuestPortal ticket page template placeholders

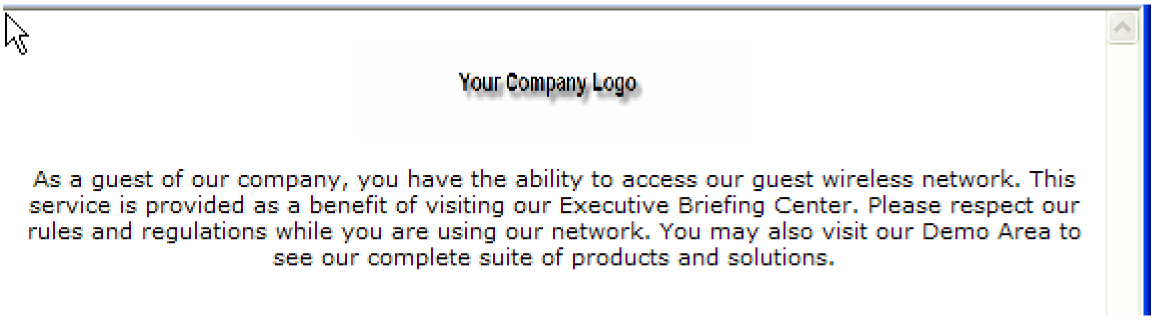
E.1.2 Default GuestPortal ticket page source code

Note: The GuestPortal account information placeholders used in the html code are preceded by the ! character.

```
<HTML>

<HEAD>

        <title></title>

        <meta content="text/html;charset=utf-8" http-
equiv="Content-Type"/>

</HEAD>

<body style="text-align:center">

        <table cellspacing="0" cellpadding="0" border="0"
align="center" width="790">

        <tr>

                <td style="background-
color:#6666b0;color:white;font-weight:bold;font-
size:30;padding:5px"



align="center" width="790">GuestPortal</td>

        </tr>

        </table>


        <table cellspacing="5" cellpadding="0" border="0"
style="margin:0 auto">

        <tr>

                <td align="right"><b>Guest Name:</b></td>

                <td align="left">!GuestName</td>

        </tr>

        <tr>

                <td align="right"><b>User ID:</b></td>

                <td align="left">!UserID</td>

        </tr>

        <tr>

                <td align="right"><b>Password:</b></td>

                <td align="left">!Password</td>

        </tr>

        <tr>

                <td align="right"><b>Account Start:</b></td>
                <td align="left">!AccountActivationTime</td>
        </tr>
        <tr>
                <td align="right"><b>Duration:</b></td>
                <td align="left">!AccountLifeTime</td>
        </tr>
        <tr>
                <td align="right"><b>Valid Daily Login Time:</
b></td>
                <td align="left">!TimeOfDayStart --
!TimeOfDayDuration</td>
        </tr>
        <tr>
                <td align="right"><b>Comment:</b></td>
                <td align="left">!GuestComment</td>
        </tr>
        </table>

         <div style="width:790px;margin:0 auto;text-align:left">
                <b>System Requirements:</b>
                <hr width=790 size=2 noshade>
                <div style="padding-left:30px">
                        <ul>
                                <li>A laptop with WLAN
capabilities (801.11a/b/g). This functionality can be either
embedded into your device or via a PCMCIA card.
                                <li>Web browser software. You
can use any standard Internet browser (ie, Internet Explorer,
Netscape, etc).
                        </ul>
                </div>
        </div>

        <div style="width:790px;margin:10px auto;text-
align:left">
                <b>Instructions:</b>
                <hr width=790 size=2 noshade>
                <div style="padding-left:30px;">
                        <ul>
                                <li>Enable your wireless device
to connect to the '!SSID' SSID.
```

```
                                <li>Once connected, launch your
Internet browser and you will be redirected to the Guest Access
webpage.
                                <li>Enter the user ID and
password supplied above. By logging into the network, you are
accepting the terms and conditions below.
                                <li>You're connected!
                        </ul>
                 </div>
         </div>

</div>
</body>
</HTML>
```

E.2 GuestPortal sample header page



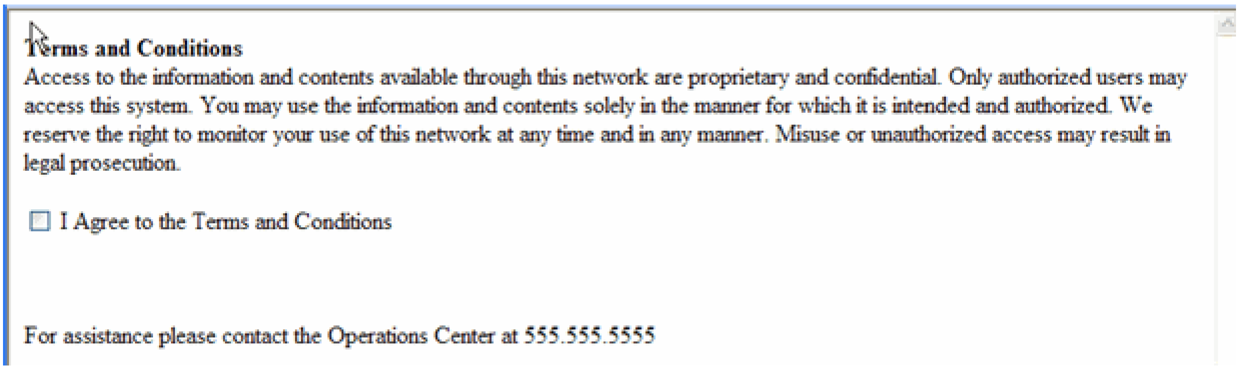
As a guest of our company, you have the ability to access our guest wireless network. This service is provided as a benefit of visiting our Executive Briefing Center. Please respect our rules and regulations while you are using our network. You may also visit our Demo Area to see our complete suite of products and solutions.

Sample header page source code

```
<HTML><HEAD><TITLE>your company name</TITLE>
<META http-equiv=Content-Type content="text/html;
charset=windows-1252">

<STYLE type=text/css>BODY {
FONT-SIZE: 11px; COLOR: #000000; FONT-FAMILY: Verdana, Arial,
Helvetica, sans-serif
}
TD {
FONT-SIZE: 11px; COLOR: #000000; FONT-FAMILY: Verdana, Arial,
Helvetica, sans-serif
}
H3 {
FONT-SIZE: 14px; COLOR: #000066; FONT-FAMILY: Verdana, Arial,
Helvetica, sans-serif
}
</STYLE>
<META content="Microsoft FrontPage 5.0" name=GENERATOR></HEAD>
<BODY>
<SPAN id=0 style="DISPLAY: none;">
<CENTER>
  <span id="1" style="DISPLAY: true;"><span id="1">
  <img border="0" src="your_logo.gif" width="198" height="49"></
span></span>
</CENTER>
<H3>Wireless Guest Access Login</H3>
<BR>
  Please enter the <strong>Username and Password</strong> you
were assigned from the Receptionist. <br>
  <INPUT type=hidden value=wba_login
name=fname>
  <TABLE cellPadding=3 border=0>
    <TBODY>
      <TR>
        <TD align=right>Username:</TD>
        <TD><INPUT maxLength=32 size=15 name=username></TD>
      </TR>
      <TR>
        <TD align=right>Password:</TD>
        <TD><INPUT type=password maxLength=32 size=15
name=key></TD>
      </TR>
      <TR>
        <TD align=right colSpan=2>
        </TD>
      </TR>
    </TBODY>
  </TABLE>
  <br>
  For assistance please contact our Operations Center at
555.555.5555
<BR>
</SPAN> <SPAN id=1 style="DISPLAY: true;">
  <p align="center"><span id="1">
  <img border="0" src="your_logo.gif" width="198" height="49"></
span><br>
```

```
  <br>
  As a guest of our company, you have the ability to access our
guest wireless network.
  This service is provided as a benefit of visiting our
Executive Briefing Center.
  Please respect our rules and regulations while you are using
our network. You may also visit our Demo Area to see our
complete suite of products and solutions.
  </p>
```

E.3 GuestPortal sample footer page



Terms and Conditions

Access to the information and contents available through this network are proprietary and confidential. Only authorized users may access this system. You may use the information and contents solely in the manner for which it is intended and authorized. We reserve the right to monitor your use of this network at any time and in any manner. Misuse or unauthorized access may result in legal prosecution.

□ I Agree to the Terms and Conditions

For assistance please contact the Operations Center at 555.555.5555

Sample footer page source code

```
<html>
<body>
    <strong>Terms and Conditions</strong><br>
    Access to the information and contents available through
this network are proprietary and confidential. Only authorized
users may access this system.
    You may use the information and contents solely in the
manner for which it is intended and authorized. We reserve the
right to monitor your use of this network at any time and in any
manner. Misuse or unauthorized access may result in legal
prosecution.
    <BR>
    <BR>
    <input type="checkbox" name="agree" value="on">
    I Agree to the Terms and Conditions <SPAN id=2
style="DISPLAY: none; FONT-WEIGHT: bold; FONT-SIZE: x-small;
COLOR: red">Required</SPAN>
    <br>
    <br>
    <br>
```

```
<br>
    For assistance please contact the Operations Center at 
555.555.5555
 </p>
</SPAN>


</BODY></HTML>
```