

To Create a Load Balance Groups

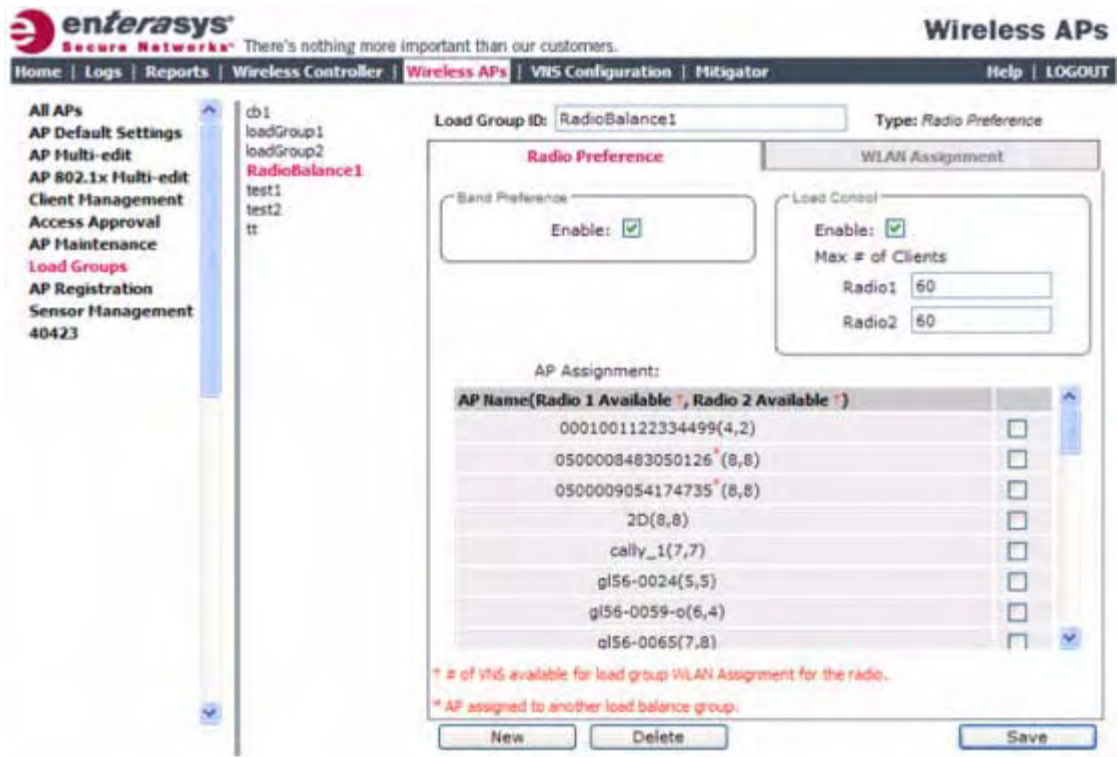
1. From the top menu, click **Wireless APs**. The Wireless AP screen is displayed.
2. In the left pane, click **Load Groups**. The **Wireless AP Load Groups** page displays.

The screenshot shows the Enterasys Wireless APs management interface. The top navigation bar includes Home, Logs, Reports, Wireless Controller, **Wireless APs**, VNS Configuration, and Mitigator. The left sidebar lists various management options, with **Load Groups** highlighted. The main content area displays the configuration for a Load Group with ID 'test' and Type 'Client Balancing'. It features two tabs: 'Radio Assignment' (active) and 'WLAN Assignment'. Under 'Radio Assignment', there is a dropdown for 'Select AP radios' and a table with columns for 'Radio 1(Available †)', 'Radio 2(Available †)', and 'AP Name'. The table contains one row with radio types 'a/n(7)' and 'b/g/n(7)', and AP name '0500008043050236'. A red note at the bottom states '† # of VNS available for load group WLAN Assignment for the radio.' Buttons for 'New', 'Delete', and 'Save' are at the bottom.

3. Click **New**. The **Add Load Group** window displays.

The 'Add Load Group' dialog box is shown. It has a title bar with a question mark and a close button. The 'Load Group ID' field contains 'RadioBalance1'. The 'Type' dropdown menu is open, showing 'Client Balancing' as the selected option and 'Radio Preference' as the option being clicked by the mouse. An 'Add' button is located at the bottom left of the dialog.

If you are adding a Radio Preference load balancing group, the Radio Preference tab becomes available.



Field/Button	Description
Load Group ID	Enter a unique name for the load group. You can create load groups with the same name on different Enterasys Wireless Controllers; however, the groups will be treated as separate groups according to the home controller where the group was originally created.
Type	The type of load group is displayed. Options include: <ul style="list-style-type: none"> Client Balancing - select to perform load balancing based on the number of clients across all APs in the load balance group and only for the WLANs assigned to the group. Radio Preference - select to perform band preference steering and enforce load control settings on this load group.
New	Click to create a new load group. The Add Load Group window.
Delete	Click to delete this load group.
Save	Click to save your changes.

Radio Assignment tab - this tab is available only for load groups assigned the Client Balancing type

Field/Button	Description
Select AP Radios	<p>From the drop-down menu, select the AP radios that you want to assign to the load group. Options include:</p> <ul style="list-style-type: none"> All radios Radio 1 Radio 2 Clear all radios <p>You can assign a radio to only one load balance group. A radio that is assigned to another load balance group will have an asterisk next to it. If you select a radio that has been assigned to another load balance group, the radio is reassigned to the new load balance group.</p> <p>Note: You can assign each radio of an AP to different load balance groups.</p>
Radio Preference tab - this tab is available only for load groups assigned the Radio Preference type	
Band Preference	<p>Select the Enable checkbox to enable band preference for this load group.</p> <p>For the AP36xx models only, you can apply band preference only to a VNS assigned in the load group. Enabling band preference enables you to move an 11a-capable client to an 11a radio to relieve congestion on an 11g radio. A client is considered 11a capable if the AP receives requests on an 11a VNS that already belongs to a load group with band preference enabled. After you configure band preference, if a client tries to reassociate with an 11g radio, it will be rejected if the AP determines that the client is 11a capable.</p>
AP Assignment	Select the APs on which you want to enforce the Band Preference and Load Control settings.
Load Control	Select the Enable checkbox to enable load control for this load group. Enabling load control causes the controller to enforce the limit you specify for the number of clients for each radio.
Max # of Clients:	Enter the maximum number of clients for Radio 1 and Radio 2. The default limit is 60. The valid range is: 5 to 60.
<ul style="list-style-type: none"> Radio 1 Radio 2 	
WLAN Assignment tab	
WLAN Name	<p>Click the checkbox of the one or more WLAN services that you want to assign to all member radios of the load balance group. You can select up to the radio limit of eight VNSs.</p> <p>When you assign a radio to a load group, WLAN service assignment can only be done from the WLAN Assignment tab on the Wireless AP Load Groups screen. On all other WLAN Assignment tabs associated with the member AP radios, the radio checkbox associated with the member AP radios will be grayed out. When you remove a radio from a load group, the load group's WLAN service will remain assigned to the radio, but you can now assign a different WLAN service to the radio.</p>

Field/Button	Description
Add Load Group Window	
Load Group ID	Enter a unique name for this load group.
Type	From the drop-down menu, select the type of load balancing to be used for this load group. Options are: <ul style="list-style-type: none"> • Client Balancing • Radio Preference
Add	Click to add this new load group. The new load group is the currently displayed load group in the Wireless AP Load Groups screen. After you add the new load group, navigate to the Radio Preference and WLAN Assignment tabs to assign radios and one or more WLAN services to the load group.
Cancel	Click to discard the new load group configuration

How Availability Affects Load Balancing

All radios assigned to a load group must belong to APs that are all controlled by the same Enterasys Wireless Controller. If you have enabled availability configuration of a load group is only possible from the home controller where the load group was created. Load balancing will continue to operate if member APs fail over to the foreign controller as long as the WLAN service assignment remains the same.

To ensure that load balancing works properly in availability, you should enable synchronization of the system configuration and the WLAN services used by the load group when you configure availability. If you do not enable synchronization, the radios on any AP that fails over may be removed from their assigned load groups. For more information, see [“Configuring Availability Using the Availability Wizard”](#) on page 11-3.

If you have not configured synchronization, in a failover situation you will be able to change the load balance group’s WLAN service assignment from the **VNS Configuration** screens and the **Wireless AP's WLAN Assignment** screens on the foreign controller.



Note: If you have configured synchronization, you cannot change the WLAN assignments from the foreign controller.

If you have not configured synchronization, you must configure the foreign controller to ensure that all AP radios in the load balance group have the same WLAN services assigned before the AP fails over, as originally configured for the load group. If the WLAN services assigned do not match when an AP fails over, the affected AP radios will be removed from the load group. If you change the WLAN services to match after the AP fails over, the AP radios still will not be allowed to be in the load group. You must reconnect the AP to the home controller to have the radios become part of the load group again.

Load Balance Group Statistics

You can view load balance group statistics through the **Active Wireless Load Groups** report. For more information, see [“Viewing Load Balance Group Statistics”](#) on page 15-8.

Configuring an AP Cluster

APs operating in both fit mode and standalone mode operate in a cluster setup. A cluster is a group of Wireless APs configured to communicate with each other. Mobile users (MU) can seamlessly roam between the APs participating in the cluster. The Enterasys Wireless AP extends basic cluster functionality with the following enhancements:

- Support for fast roaming
- Automatic Channel Selection (ACS) for all APs in the cluster
- Cluster member information is available to the user
- MU statistic history
- Pre-authentication

A cluster forms when APs operating are within the same subnet and multicast and IGMP snooping are enabled. The APs in the cluster use a default cluster ID (shared secret) or a cluster ID that you assign.

An AP cluster can exist at any point in your network. Each cluster member periodically (30 seconds) sends a secure SIAPP (Siemens Inter-AP Protocol) multicast message to update other cluster members. The SIAPP message includes:

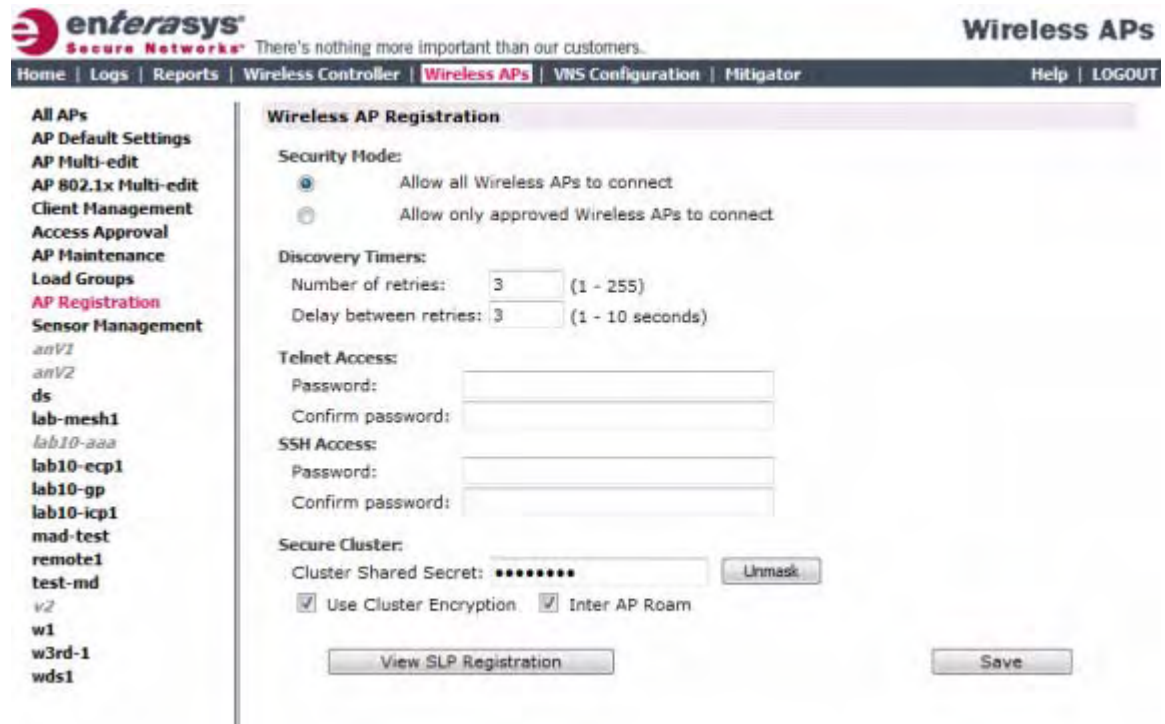
- The AP name
- The AP Ethernet MAC address
- The AP IP address
- The client count
- The base BSSIDs for both radios

Each AP caches locally stored information about other cluster members and maintains its own view of the cluster.

To Change an AP Cluster's Configuration:

1. From the top menu, click **Wireless APs**. The Wireless AP screen is displayed.

- In the left pane, click **AP Registration**. The **AP Registration** screen is displayed.



- In the **Secure Cluster** section, enter a cluster shared secret.
- Enable cluster encryption by clicking on the **User Cluster Encryption** checkbox. APs on which user cluster encryption is disabled cannot participate in the cluster.
- Enable or disable support for inter-AP roaming by clicking on the **Inter AP Roam** checkbox.
- Click **Save**.

Converting the Wireless AP to Standalone Mode

The Enterasys Wireless AP (AP3630/3640) by default operates in standalone (thick) AP mode. However, as long as the Wireless AP is running release V7.31 or V8.01, you can configure it to operate in fit mode in a controller-based deployment. Conversion from standalone to fit mode is seamless and can be performed from either the UI or CLI. Conversion from thin to standalone mode is performed from the UI or from the CLI.

To Convert the AP Operating in Fit Mode Back to Standalone Mode:

- From the top menu, click **Wireless APs**. The Wireless AP screen is displayed.

- In the left pane, click **Access Approval**. The **Access Approval** screen is displayed.

The screenshot shows the Enterasys Wireless APs management interface. The left navigation pane includes options like 'All APs', 'AP Default Settings', 'AP Multi-edit', 'AP 802.1x Multi-edit', 'Client Management', 'Access Approval' (highlighted), 'AP Maintenance', 'Load Groups', 'AP Registration', 'Sensor Management', and various CNL-91-0-0-ssid options. The main content area is titled 'Access Approval' and contains a table of Wireless APs:

Wireless APs	Home	Status
<input type="checkbox"/> 0500006072051204 00:0F:BB:09:06:F4	Local	Approved
<input type="checkbox"/> 1000005480080188 00:04:96:28:48:80	Local	Approved
<input type="checkbox"/> 7000000000000111 00:1A:E8:14:10:5F	Local	Approved

Below the table, there is a 'Perform action on selected Wireless AP' section with buttons for 'Approved', 'Pending', 'Release', 'Reboot', 'Delete', and 'Standalone Mode'. There is also a 'Sensor' dropdown menu and a 'Force Image Download' checkbox.

- Select one or more APs that you want to convert to standalone mode.



Note: If you try to convert an AP other than an AP3630/40, or an inactive or foreign AP to standalone mode, the system returns an error. Only an AP3630/40 running V7.31 or V8.01 can operate in both standalone and fit mode.

- In the **Perform Action on Selected Wireless AP** section, click the **Standalone Mode** button. The system warns you that the AP will be removed from the Enterasys Wireless Controller. Click **OK** to continue.



Note: After you convert the Wireless AP to standalone mode, you can no longer access it using the Wireless Assistant UI or CLI. Instead, you must access AP using the Wireless AP UI or CLI. Be sure to note the IP address of the AP before you convert it.

Configuring an AP as a Sensor

Only the Enterasys Wireless AP 2610/2620 and AP 3610/3620 can be configured as sensors.

A Wireless AP that is configured as a sensor performs scanning services and relays information to Wireless Advanced Services (WAS). When an AP is **Approved as Sensor**:

- The AP severs its connection to the Enterasys Wireless Controller
- The AP registers with Wireless Advanced Services (WAS)
- The AP performs scanning services
- The AP no longer performs RF services for the Enterasys Wireless Controller

When an AP is operating as a sensor, it has no interaction with the Enterasys Wireless Controller, and it does not perform like an AP: it does not allow devices to associate to it and traffic is not

forwarded through it. An AP operating as a sensor is managed by Enterasys Wireless Advanced Services (WAS). The WAS's sensor domain license (SDL) limit governs the number of sensors the customer can have.

When an AP is configured as a sensor, the AP's current configuration is retained in the controller database. If the sensor is later configured back to perform RF services, its previous configuration data is reassigned to it. For more information, see the *Enterasys Wireless Manager User Guide* and the *Enterasys Wireless Advanced Services User Guide*.

Before APs can be configured as sensors, you must first download the sensor image from a TFTP server to the Enterasys Wireless Controller:

To Download the Sensor Image from a TFTP Server to the Enterasys Wireless Controller:

1. From the top menu, click **Wireless APs**. The Wireless AP screen is displayed.
2. In the left pane, click **Sensor Management**. The **Wireless AP Sensor Management** screen is displayed.

The screenshot shows the 'Wireless AP Sensor Management' interface. On the left, a navigation menu includes 'All APs', 'AP Default Settings', 'AP Multi-edit', 'AP 802.1x Multi-edit', 'Client Management', 'Access Approval', 'AP Maintenance', 'Load Groups', 'AP Registration', 'Sensor Management' (highlighted), and 'Lab126-10-Int-CP 1112'. The main area is titled 'Wireless AP Sensor Management' and contains two sections: 'Local Sensor Images' and 'Download Sensor Images'. The 'Local Sensor Images' section lists 'AP26XX' and 'AP36XX', each with 'Image' and 'Version' input fields. The 'Download Sensor Images' section includes a 'Sensor Platform' dropdown menu (set to 'AP26XX'), and three input fields for 'TFTP Server', 'Directory', and 'Filename'. A 'Download' button is positioned at the bottom right of the form.

3. In the **Sensor Platform** field, select AP26xx or AP36xx.
4. Type the following:
 - **TFTP Server** — The IP address of the TFTP server the AP is to retrieve the sensor image file from.
 - **Directory** — The location of the AP26xx or AP36xx sensor image on the TFTP server.
 - **Filename** — The filename of the AP26xx or AP36xx sensor image on the TFTP server.
5. Click **Download**.
6. Once you have downloaded the sensor image, configure the appropriate Wireless AP as a sensor from either the **Wireless APs All APs** screen or the **Wireless APs Access Approval** screen.

To configure the Wireless AP as a sensor from the **Wireless APs All APs** screen:

- From the top menu, click **Wireless APs**. The Wireless AP screen is displayed.
- In the Wireless AP list, click the Wireless AP whose properties you want to modify. The **AP Properties** tab displays Wireless AP information.

The screenshot shows the Enterasys Wireless APs management interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', and 'Mitigator'. The 'Wireless APs' page is active, showing a list of APs on the left and the 'AP Properties' configuration form on the right. The 'AP Properties' form includes the following fields and values:

- Serial #:** 0500008043050236
- Host Name:** AP3620-0500008043050236
- Name:** 0500008043050236
- Location:** (empty)
- Description:** (empty)
- Port:** Unknown
- AP Environment:** Indoor
- Hardware Version:** Wireless AP3620 External
- Application Version:** 08.01.01.0184
- Status:** Approved
- Active Clients:** 0
- Role:** Access Point
- Country:** United States

Red warning messages are visible in the form:

- ¹ Change of name will cause interruption of service if DHCP is enable
- ² Change of Environment will cause interruption of service
- ³ Sensor role is not available since local Sensor image does not exist.
- ⁴ Change of Country may require AP to reboot

Buttons at the bottom include 'Copy to Defaults', 'Reset to Defaults', 'Add Wireless AP', and 'Save'.

- Select the AP that you want to configure as a sensor.
- In the **Role** field, select **Sensor**.
- Click **Save**.

To configure the Wireless AP as a sensor from the **Wireless APs Access Approval** screen:

- From the top menu, click **Wireless APs**. The Wireless AP screen is displayed.
- In the left pane, click **Access Approval**. The **Access Approval** screen is displayed, along with the registered Wireless APs and their status.
- Select the checkbox next to the Wireless AP that you want to configure as a sensor.
- Click **Sensor**.

Performing Wireless AP Software Maintenance

When a new version of AP software becomes you can install it from the Enterasys Wireless Controller.

You can configure each Wireless AP to upload the new software version either immediately, or the next time the Wireless AP connects to the controller. Part of the Wireless AP boot sequence seeks and install its software from the Enterasys Wireless Controller.

You can modify most of the radio properties on a Wireless AP without requiring a reboot of the AP.

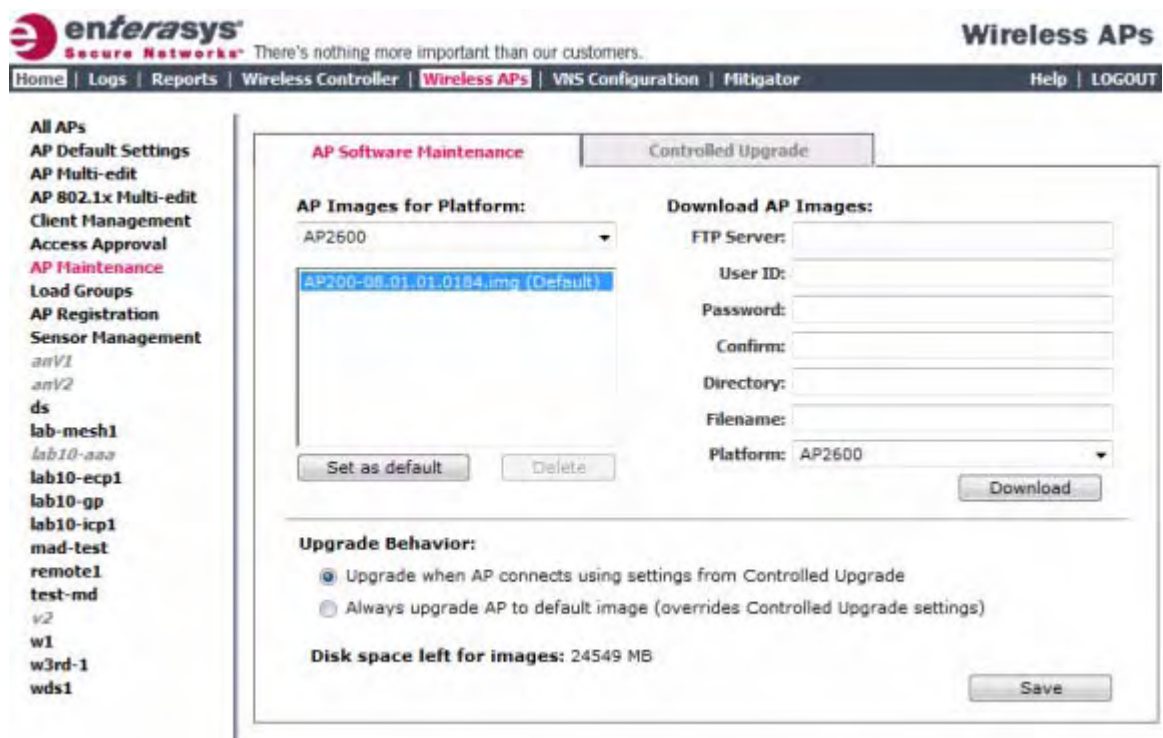
During upgrade, the Wireless AP keeps a backup copy of its software image. When a software upgrade is sent to the Wireless AP, the upgrade becomes the Wireless AP's current image and the previous image becomes the backup. In the event of failure of the current image, the Wireless AP will run the backup image.



Note: The Enterasys Wireless Controller does not ship with sensor software. You must download sensor software from a TFTP server to the local controller.

To Maintain the List of Current Wireless AP Software Images:

1. From the top menu, click **Wireless APs**. The **Wireless APs** screen is displayed.
2. In the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.



3. In the **AP Images for Platform** drop-down list, click the appropriate platform.
4. To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.
5. In the **Upgrade Behavior** section, select one of the following:
 - **Upgrade when AP connects using settings from Controlled Upgrade** — The **Controlled Upgrade** tab is displayed when you click **Save**. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
 - **Always upgrade AP to default image (overrides Controlled Upgrade settings)** — Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is

verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.

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

To Delete a Wireless AP Software Image:

1. From the top menu, click **Wireless APs**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
3. In the **AP Images for Platform** drop-down list, click the appropriate platform.
4. In the **AP Images** list, click the image you want to delete.
5. Click **Delete**. The image is deleted.

To Download a New Wireless AP Software Image:

1. From the top menu, click **Wireless APs**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
3. In the **Download AP Images** list, type the following:
 - **FTP Server** – The IP of the FTP server to retrieve the image file from.
 - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
 - **Password** – The corresponding password for the user ID.
 - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
 - **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
 - **Filename** – The name of the image file to retrieve.
 - **Platform** – The AP hardware type to which the image applies. There are several types of AP and they require different images.
4. Click **Download**. The new software image is downloaded.

To Define Parameters for a Wireless AP Controlled Software Upgrade:

1. From the top menu, click **Wireless APs**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
3. Click the **Controlled Upgrade** tab.



Note: The **Controlled Upgrade** tab is displayed only when the **Upgrade Behavior** is set to **Upgrade when AP connects using settings from Controlled Upgrade** on the **AP Software Maintenance** tab.

4. In the **Select AP Platform** drop-down list, click the type of AP you want to upgrade.
5. In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.
6. In the list of registered **Wireless APs**, select the checkbox for each Wireless AP to be upgraded with the selected software image.
7. Click **Apply AP image version**. The selected software image is displayed in the **Upgrade To** column of the list.

8. To save the software upgrade strategy to be run later, click **Save for later**.
9. To run the software upgrade immediately, click **Upgrade Now**. The selected Wireless AP reboots, and the new software version is loaded.



Note: The **Always upgrade AP to default image** checkbox on the **AP Software Maintenance** tab overrides the **Controlled Upgrade** settings.

Configuring Topologies

This chapter describes topology configuration, including:

For information about...	Refer to page...
Topology Overview	4-1
Configuring a Basic Topology	4-2
Enabling Management Traffic	4-3
Layer 3 Configuration	4-4
Exception Filtering	4-9
Multicast Filtering	4-13

Topology Overview

Topology configuration is independent of the WLAN services or Policies that are defined in the system. You can navigate to the Topologies configuration page from either Wireless Controller or VNS Configuration options of the Enterasys Wireless Assistant top menu. Also, the Policy definition page allows the user to edit or create a Topology definition at any time.

Topologies are not activated until they are referenced by a Policy. Creating an interface on a VLAN will not take effect until a Policy references its usage.

Topologies cannot be deleted while they are active (that is, referenced by a Policy).

On the **Topologies** configuration page, the key field is the **Mode**, which determines some of the other factors of the topology. When you have completed defining the topology for your VNS, save the topology settings. Once your topology is saved, you can then access the remaining VNS tabs and continue configuring your VNS.

On the **Topologies** configuration page, a number of parameters related to network topology can be defined:

- VLAN ID and associated L2 port
- L3 (IP) interface presence and the associated IP address and subnet range
- The rules for using DHCP
- Enabling or disabling the use of the associated interface for management/control traffic
- Selection of an interface for AP registration
- Multicast filter definition
- Exception filter definition

Starting with V7.0, the term “Physical Ports” refers to the data plane physical ports. The attributes of a physical port are:

- Administrative status (read-write)
- Name (read-only)
- MAC address (read-only)
- MTU size
- Multicast Support for Routed VNS

At most, one physical topology can be enabled for the multicast support for Routed VNS. This can be configured on the new physical port GUI.

Configuring a Basic Topology

The configuration procedure below is sufficient to create and be able to save a new topology. Optional configuration options are described in the following sections.

To Configure a Basic Topology:

1. From the top menu, click either **Wireless Controller** or **VNS Configuration**. Then, in the left pane, select **Topologies**. The Topologies window displays.
2. If you want to edit an existing topology, select the desired topology. If you want to create a new topology, click the **New** button. Depending on your selection, two or three tabs are displayed.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (selected), and Mitigator. The left sidebar shows a tree view with 'Topologies' selected. The main area displays a table of topologies with columns for Topology Name, VLAN ID, Tagged, Port, IP Address, and Mode. Below the table are buttons for 'New' and 'Delete Selected', and configuration fields for 'Internal VLAN ID' (set to 1) and 'Multicast Support' (set to esa0). A 'Save' button is located at the bottom right.

Topology Name	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	-	✗	Admin	192.168.3.110	Admin
<input type="checkbox"/> Bridged at AP untagged	-	✗	-	-	B@AP
<input type="checkbox"/> CNL-218-0-0	-	✗	-	172.29.160.1	Routed
<input type="checkbox"/> CNL-218-0-1	-	✗	-	172.29.160.9	Routed
<input type="checkbox"/> CNL-218-0-2	692	✓	esa1	10.218.2.1	B@HWC
<input type="checkbox"/> CNL-218-0-3	-	✗	-	172.29.160.25	Routed
<input type="checkbox"/> CNL-218-1-2-wds	-	✗	-	172.29.164.17	Routed
<input type="checkbox"/> CNL-218-1-4-wds	-	✗	-	-	B@AP
<input type="checkbox"/> CNL-218-1-5	-	✗	-	172.29.165.9	Routed

3. On the General tab, enter a name for the topology in the **Name** field.

4. Select a mode of operation from the **Mode** drop-down list. Choices are:
 - **Physical**
 - **Routed** – Routed topologies do not need any Layer 2 configuration, but do require Layer 3 configuration. See [“Layer 3 Configuration”](#) on page 4-4 for more information.
 - **Bridge Traffic Locally at AP** – Requires Layer 2 configuration. Does not require Layer 3 configuration. Bridge Traffic at the AP VNSs do not require the definition of a corresponding IP address since all traffic for users in that VNS will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port).
 - **Bridge Traffic Locally at HWC** – Requires Layer 2 configuration. May optionally have Layer 3 configuration. Layer 3 configuration would be necessary if services (such as DHCP, captive portal, etc.) are required over the configured network segment, or if controller management operations are intended to be done through the configured interface.
5. Configure the Layer 2 **VLAN Settings**, depending on the previously selected Mode.
 - For **Physical**, enter a VLAN identifier (1 - 4094), with at least one layer 2 member port (no mu associated).
 - For **Bridge Traffic Locally at HWC**, enter a VLAN identifier (1 - 4094) that is valid for your system and enter the port to which this VLAN is attached to, according to the networking deployment model pre-established during planning.
 - For **Bridge Traffic Locally at AP**, enter a VLAN identifier (1 - 4094) that is valid for your system.
 - Specify whether the VLAN configuration is **Tagged** or **Untagged**.
 - For **Port**, select the Physical (Ethernet) or Link Aggregation (LAG) data port. For more information, see [Viewing and Changing the L2 Ports Information](#).
6. To replicate topology settings, click **Synchronize** in the **Status** box.
7. Click **Save** to save your changes.

These steps are sufficient to create and save a topology. The following configuration options are optional and depend on the mode of the topology.

Enabling Management Traffic

If management traffic is enabled for a VNS, it overrides the built-in exception filters that prohibit traffic on the Enterasys Wireless Controller data interfaces. For more information, see [Filtering Rules](#).

To enable Management Traffic for a Topology:

1. From the top menu, click either **Wireless Controller** or **VNS Configuration**. Then, in the left pane, select **Topologies**. The Topologies window displays.
2. Select the desired physical or routed topology. If the Layer 3 parameters are not displayed, check the **Layer 3** checkbox.
3. Select the **Management Traffic** checkbox.
4. To save your changes, click **Save**.

Layer 3 Configuration

This section describes configuring IP addresses, DHCP options, Next Hop and OSPF parameters, for Physical port, Routed, and Bridge Traffic Locally at HWC topologies.

IP Address Configuration

The L3 (IP) address definition is only required for Physical port and Routed topologies. For Bridge Traffic Locally at HWC topologies, L3 configuration is optional. L3 configuration would be necessary if services such as DHCP, captive portal, AP registration (with up to 4 topologies) are required over the configured network segment or if controller management operations are intended to be done through the configured interface.

Bridge Traffic Locally at AP VNSs do not require the definition of a corresponding IP address since all traffic for users in that VNS will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port).

To Define the IP Address for the Topology:

1. From the top menu, click **Wireless Controller** and then from the left pane select **Topologies**. Alternatively, from the top menu select **VNS Configuration** and then press **Topologies** button.
2. If already defined, click the topology you want to define the IP address for. The **Topologies** window is displayed. Alternatively, press the New button to create a new topology. Depending on the preselected options, two or three tabs are displayed.

The screenshot shows the 'Virtual Network Configuration' interface for Enterasys. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar contains a tree view with categories like 'Global', 'Virtual Networks', 'WLAN Services', 'Policies', 'Classes of Service', and 'Topologies'. Under 'Topologies', several items are listed, including 'Admin', 'anRoute1', 'anV1Topology', 'anV2Topology', 'bac10-1', 'bac10-2', 'Bridged at AP untagged', 'phy2', 'phy3', 'physical 1', 'physical 2', and 'v2Topology'. The main content area is titled 'Topology:' and has three tabs: 'General', 'Multicast Filters', and 'Exception Filters'. The 'General' tab is selected and contains the following fields:

- Core:** Name: name; Mode: Routed (dropdown menu)
- Status:** Synchronize: (with a note: 'Replicated when Synchronize Configuration is enabled')
- Layer 3:** (checked); Gateway: [text box]; Mask: [text box]; DHCP: Local Server (dropdown) with a 'Configure' button; MTU: 1436; Management Traffic:
- Remote Settings:** Gateway: [text box]; Mask: [text box]; Address Range: from: [text box] to: [text box]

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

3. For IP interface configuration for **Routed** topologies, configure the following Layer 3 parameters.

- a. In the **Gateway** field, type the Enterasys Wireless Controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The Enterasys Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to MUs (in the VNS) as the default gateway for the VNS subnet. (MUs target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).
 - b. In the **Mask** field, type the appropriate subnet mask for the IP address. to separate the network portion from the host portion of the address (typically, 255.255.255.0).
 - c. If desired, enable Management traffic.
4. For IP interface configuration for **Bridge Traffic Locally at HWC topologies**, configure the following Layer 3 parameters.

- a. In the **Interface IP** field, type the IP address that corresponds to the Enterasys Wireless Controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.
- b. In the **Mask** field, type the appropriate subnet mask for the IP address. to separate the network portion from the host portion of the address (typically, 255.255.255.0).
- c. Configure Strict Subnet Adherence.
- d. If desired, configure AP Registration. If selected, Wireless APs can use this port for discovery and registration.
- e. If desired, enable Management traffic.

DHCP Configuration

You can configure DHCP settings for all modes except **Bridge Traffic Locally at AP** mode since all traffic for users in that VNS will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port). DHCP assignment is disabled by default for Bridged to VLAN mode. However, you can enable DHCP server/relay functionality to have the controller service the IP addresses for the VLAN (and wireless users).

To Configure DHCP Options:

1. Navigate to the Topology page.
2. On the Topology page, click the General tab and enable Layer 3.
3. From the **DHCP** drop-down list, select one of the following options and click the **Configure** button.
 - **Local Server** if the Enterasys Wireless Controller's local DHCP server is used for managing IP address allocation.
 - **Use Relay** if the Enterasys Wireless Controller forwards DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Enterasys Wireless Controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
4. If you selected **Local Server**, the following window displays. Configure the following parameters:

- a. In the **Domain Name** box, type the external enterprise domain name server to be used.
- b. In the **Lease default** box, type the default time limit. The default time limit dictates how long a wireless device can keep the DHCP server assigned IP address. The default value is 36000 seconds (10 hours).
- c. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
- d. In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
- e. Check the **Enable DLS DHCP Option** checkbox if you expect optiPoint WL2 wireless phone traffic on the VNS. Enterasys DLS (Enterasys Deployment Service) is an application that provides configuration management and software deployment and licensing for optiPoint WL2 phones.

- f. In the **Gateway** field, type the Enterasys Wireless Controller's own IP address in that topology. This IP address is the default gateway for the topology. The Controller advertises this address to the wireless devices when they sign on. For routed topologies, it corresponds to the IP address that is communicated to Wireless clients as the default gateway for the subnet. (wireless clients target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).

For a Bridge traffic locally at the HWC topology, the IP address corresponds to the Enterasys Wireless Controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.

- g. The **Address Range** boxes (from and to) populate automatically with the range of IP addresses to be assigned to wireless devices using this VNS, based on the IP address you provided.
- To modify the address in the **Address Range from** box, type the first available address.
 - To modify the address in the **Address Range to** box, type the last available address.
 - If there are specific IP addresses to be excluded from this range, click **Exclusion(s)**. The **DHCP Address Exclusion** dialog is displayed.



Address Exclusion

Configured DHCP Address Range: **10.1.0.2 - 10.1.0.254**

IP Address(es) to exclude from DHCP Address Range:

Range: From:

to:

Single Address:

Comment:

- In the **DHCP Address Exclusion** dialog, do one of the following:
 - To specify an IP range, type the first available address in the **From** box and type the last available address in the **to** box. Click **Add** for each IP range you provide.
 - To specify an IP address, select the **Single Address** option and type the IP address in the box. Click **Add** for each IP address you provide.
 - To save your changes, click **OK**. The DHCP Address Exclusion dialog closes.
 - h. The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the VNS.
 - i. Click **Close**.
5. If you selected **Use Relay**, a DHCP window displays.

- a. in the **DHCP Servers** box, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The Enterasys Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.



Note: The DHCP Server must be configured to match the topology settings. In particular for Routed topologies, the DHCP server must identify the Enterasys Wireless Controller's interface IP as the default Gateway (router) for the subnet. Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.

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

Defining a Next Hop Route and OSPF Advertisement

The next hop definition allows the administrator to define a specific host as the target for all non-VNS targeted traffic for users in a VNS. The next hop IP identifies the target device to which all VNS (user traffic) will be forwarded to. Next-hop definition supersedes any other possible definition in the routing table.

If the traffic destination from a wireless device on a VNS is outside of the VNS, it is forwarded to the next hop IP address, where this router applies policy and forwards the traffic. This feature applies to unicast traffic only. In addition, you can also modify the Open Shortest Path First (OSPF) route cost.

OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place.

To Define a Next Hop Route and OSPF Advertisement:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **Topologies** pane, then click the routed Topology you want to define a next-hop route for.

- In the Layer 3 area, click the **Configure** button. The DHCP configuration dialog window displays.

- In the **Next Hop Address** box, type the IP address of the next hop router on the network through which you wish all traffic on the VNS using this Topology to be directed.
- In the **OSPF Route Cost** box, type the OSPF cost of reaching the VNS subnet.

The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the Enterasys Wireless Controller as a better fit or lowest cost path to reach devices in a particular network. The higher the cost, the less likely of the possibility that the Enterasys Wireless Controller will be chosen as a route for traffic, unless that Enterasys Wireless Controller is the only possible route for that traffic.

- To disable **OSPF advertisement** on this VNS, select the **Disable OSPF Advertisement** checkbox.
- Click **Close**.
- To save your changes, click **Save**.

Exception Filtering

The exception filter provides a set of rules aimed at restricting the type of traffic that is delivered to the controller. By default, your system is shipped with a set of restrictive filtering rules that help control access through the interfaces to only those services that are absolutely necessary.

By configuring to allow management on an interface, an additional set of rules is added to the shipped filter rules that provide access to the system's management configuration framework (SSH, HTTPS, SNMP Agent). Most of this functionality is handled directly behind the scenes by the system, rolling and un-rolling canned filters as the system's topology and defined access privileges for an interface change.



Note: An interface for which **Allow Management** is enabled can be reached by any other interface. By default, **Allow Management** is disabled and shipped interface filters will only permit the interface to be visible directly from its own subnet.

The visible exception filter definitions, both in physical ports and topology definitions, allow administrators to define a set of rules to be prepended to the system's dynamically updated exception filter protection rules. Rule evaluation is performed top to bottom, until an exact match is determined. Therefore, these user-defined rules are evaluated before the system's own generated rules. As such, these user-defined rules may inadvertently create security lapses in the system's protection mechanism or create a scenario that filters out packets that are required by the system.



Note: Use exception filters only if absolutely necessary. Enterasys recommends that you avoid defining general allow all or deny all rule definitions since those definitions can easily be too liberal or too restrictive to all types of traffic.

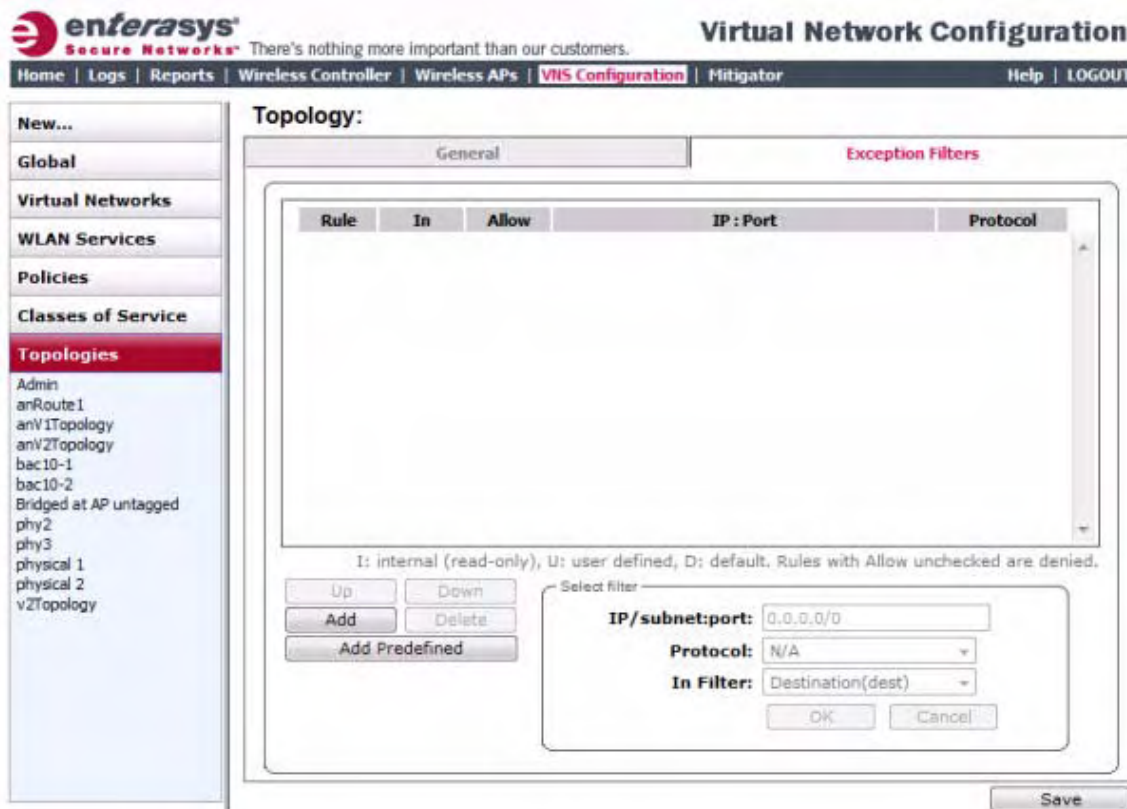
The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the filter rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number for the applicable service running on the controller's management plane.

The exception filter on an topology applies only to the packets directed to the controller and can be applied to the destination portion of the packet, or to the source portion of the packet when filtering is enabled. Traffic to a specified IP address and IP port is either allowed or denied. Adding exception filtering rules allows network administrators to either tighten or relax the built-in filtering that automatically drops packets not specifically allowed by filtering rule definitions. The exception filtering rules can deny access in the event of a DoS attack, or can allow certain types of management traffic that would otherwise be denied. Typically, **Allow Management** is enabled.

To Define Exception Filters:

1. On the **Topologies** page, click the **Exception Filters** tab.

The Exceptions Filter page displays.



2. Select an existing topology from the right hand pane to edit an existing topology, or click New. to create a new topology.

The **Topologies** configuration page displays. The Exception Filters tab is available only if Layer 3 (L3) configuration is enabled.

3. Click the Exception Filters tab to display the Exception Filters page.

Table 4-1 Exception Filters page - Fields and Buttons

Field/Button	Description
Rule	Identifies the type of filter rule. Options are: <ul style="list-style-type: none"> • D - Default rule • I - Internal (read-only) • T - Local interface rule • U - user-defined rule
In	Identifies the rule that applies to traffic from the network host or wireless device that is trying to get to a controller. You can change this setting using the drop-down menu. Options include: <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only
Allow	Select the Allow checkbox to allow this rule. Otherwise the rule is denied.

Table 4-1 Exception Filters page - Fields and Buttons (continued)

Field/Button	Description
IP:Port	Identifies the IP address and port to which this filter rule applies.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
Up, Down	Select a filter rule and click to either move the rule up or down in the list. The filtering rules are executed in the order in which you define them here
Add	Click to add a filter rule. The fields in the Add Filter area are enabled.
Delete	Click to remove this filter rule.
Add Predefined	Select a predefined filter rule. Click Add to add the rule to the rule table, otherwise click Cancel
Save	Click to save the configuration.
Advanced Mode	<p>Advanced filtering mode provides the ability to create bidirectional filters.</p> <p>If this controller participates in a mobility zone, before enabling advanced mode be sure that all controllers in the mobility zone are running V7.41 or greater.</p> <p>Note: After enabling advanced filtering mode you can no longer use NMS Wireless Manager V4.0 to manage the controller's policies and you cannot switch back to basic filter mode unless you return the controller to its default state.</p>
Add Filter section	
IP/subnet:port	Type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
In Filter	<p>In the drop-down menu, select an option that refers to traffic from the network host that is trying to get to a wireless device. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>By default, user-defined rules are enabled on ingress (In), and are assumed to be Allow rules. To disable the rule in either direction, or to make it a Deny rule, click the new filter, then de-select the relevant checkbox.</p>
OK	Click to add the filter rule to the filter group. The information displays in the filter rule table.
Cancel	Click Cancel to discard your changes.



Note: For external Captive Portal, you need to add an external server to a non-authentication filter.

Multicast Filtering

A mechanism that supports multicast traffic can be enabled as part of a topology definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.



Note: To use the mobility feature with this topology, you must select the **Enable Multicast Support** checkbox for the data port.

Define a list of multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.



Note: Before enabling multicast filters and depending on the topology, you may need to define which physical interface to use for multicast relay. Define the multicast port on the **IP Addresses** tab. For more information, see [“Setting Up the Data Ports”](#) on page 2-16.

To Enable Multicast for a Topology:

1. On the **Topologies** page, click the **Multicast Filters** tab.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. The left sidebar contains a tree view with 'Topologies' selected. The main content area is titled 'Topology:' and has three tabs: 'General', 'Multicast Filters' (active), and 'Exception Filters'. Under the 'Multicast Filters' tab, there is a checkbox for 'Multicast Support' which is checked. Below this is a table with columns 'IP', 'Group', and 'Wireless Replication'. At the bottom, there are two radio buttons: 'IP Group' (selected) and 'Defined groups'. The 'Defined groups' dropdown menu shows 'Spectralink Mcst (224.0.1.116)'. There are 'Up', 'Down', 'Add', and 'Delete' buttons. A 'Save' button is at the bottom right.

2. To enable the multicast function, select **Multicast Support**.
3. Define the multicast groups by selecting one of the radio buttons:
 - **IP Group** – Type the IP address range.
 - **Defined groups** – Click from the drop-down list.
4. Click **Add**. The group is added to the list above.

5. To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** checkbox.
6. To modify the priority of the multicast groups, click the group row, and then click the **Up** or **Down** buttons.

A Deny All rule is automatically added as the last rule, IP = *.*.* and the **Wireless Replication** checkbox is not selected. This rule ensures that all other traffic is dropped.

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



Note: The multicast packet size should not exceed 1450 bytes.

Configuring Policies

This chapter describes policy configuration, including:

For information about...	Refer to page...
Policy Overview	5-1
Configuring VLAN and Class of Service for a Policy	5-1
Filtering Rules	5-3

Policy Overview

Policy configuration defines the binding of a topology (VLAN), ingress and egress rate profiles applied to the traffic of a station, and filter rules.

Policies don't need to be fully specified; Unspecified attributes are retained by the user or inherited from Global Policy definitions (see "[Configuring the Global Default Policy](#)" on page 7-12 for more information).

Default Global Policy definitions provide a placeholder for completion of incomplete policies for initial default assignment. If a policy is defined as Default for a particular VNS, the policy inherits incomplete attributes from Default Global Policy definitions

Configuring VLAN and Class of Service for a Policy

From the VLAN & Class of Service tab you can assign a previously configured topology to a policy. You can also launch the Topology Configuration page to edit an existing topology or create a new one. For information about how to configure a topology, refer to [Chapter 4, Configuring Topologies](#).

In general, Class of Service (CoS) refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a station or port assigned to the policy is permitted. The CoS defines actions to be taken when rate limits are exceeded.

To configure VLAN and Class of Service for a policy:

1. From the top menu, click **VNS Configuration**.
The **Virtual Network Configuration** screen displays.
2. In the left pane expand the **Policies** pane and click the policy you want to edit, or click the **New** button to create a new policy.

The **Policy** configuration page displays. By default, the **VLAN & Class of Service** tab displays ([Figure 5-1](#)). [Table 5-1](#) describes the fields and buttons on the VLAN & Class of Service tab.

Figure 5-1 VLAN & Class of Service Tab

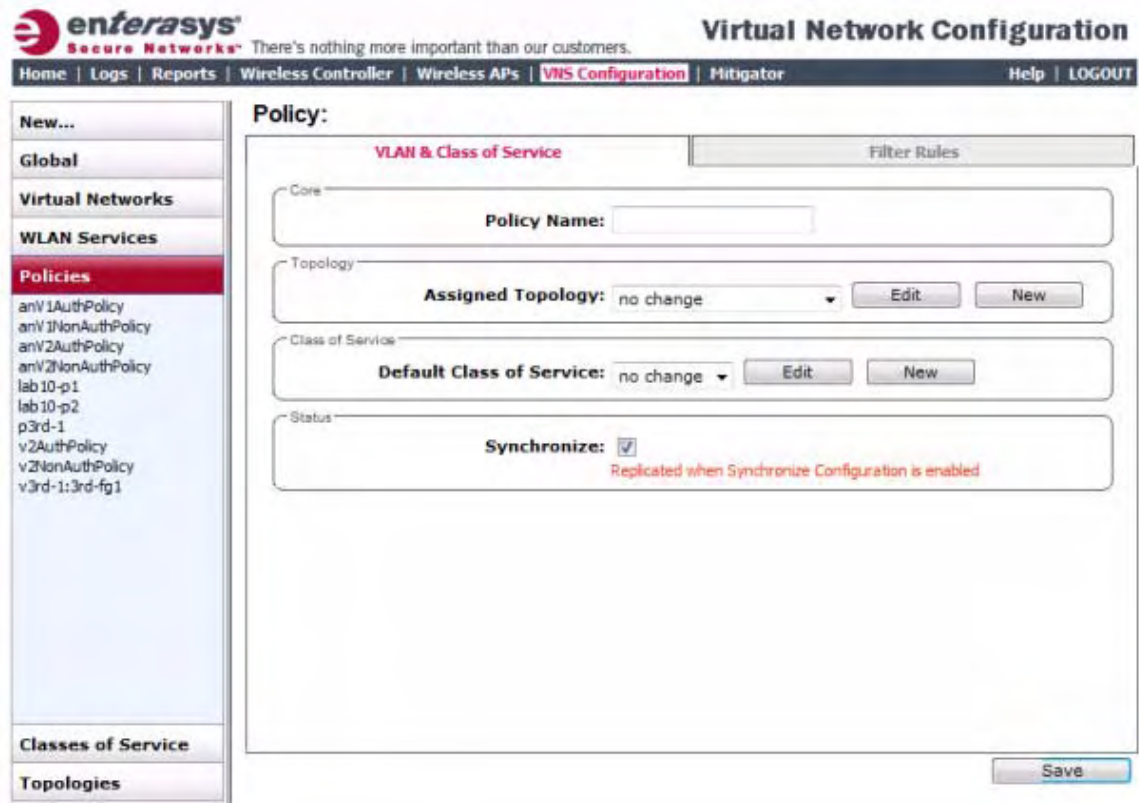


Table 5-1 VLAN & Class of Service Tab - Fields and Buttons

Field/Button	Description
Core	
Policy Name	Enter a name to assign to this policy.
Topology	
Assigned Topology	Select an existing topology from the Assigned Topology drop-down list, or click the New button to create a new topology. To edit an existing topology, select the topology and then click the Edit button. The Edit Topology page displays. For information about how to configure a topology, go to “Configuring Topologies” on page 4-1.
Class of Service	
Default Class of Service	Select an existing class of service from the Default Class of Service drop-down list, or click the New button to create a new topology. To edit an existing class of service, select the class of service and then click the Edit button. The Edit Class of Service page displays. For information about how to configure a Class of Service, go to Chapter 8, “Configuring Classes of Service.”
Status	
Synchronize	Click to enable synchronize configuration.

For more information about rate control profiles, go to [“Working with Bandwidth Control Profiles”](#) on page 7-11 for more information.

Filtering Rules

Optionally, you can define filter rules for the policy. The policy name should match filter ID values set up on the RADIUS servers.

If you do not define filter rules, then the system uses the default filter for authenticated users. However, if you require user-specific filter definitions, then the filter ID configuration identified the specific policy that should be applied to the user.

You can configure a filter definition to be static on the Enterasys Wireless Controller itself, or to be dynamically provisioned if RADIUS authentication is used. The standard RADIUS attribute can be used to identify a specific filter definition to apply to incoming/outgoing user traffic upon successful authentication of the user during authentication. You can configure up to three types of filters, depending on your network assignment type.

Table 5-2 Filter Types

Filter Type	AAA Network Assignment	SSID Assignment
Exception filter	Yes	Yes
Non-authenticated filter	-	Yes
Default filter	Yes	Yes

For information about configuring exception filters, refer to go to [“Exception Filtering”](#) on page 4-9

Filtering Rules for a Non-Authenticated Filter

Defining non-authenticated filters allows administrators to identify destinations to which a mobile user is allowed to access without incurring an authentication redirection. Typically, the recommended default rule is to deny all. Administrators should define a rule set that will permit users to access essential services:

- DNS (IP of DNS server)
- Default Gateway (VNS Interface IP)

Any HTTP streams requested by the client for denied targets will be redirected to the specified location.

The non-authenticated filter should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. This filter should also allow network access to the IP address of the DNS server and to the network address—the gateway of the Topology. The gateway is used as the IP for an internal Captive Portal page.

Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach Websites other than those specifically allowed in the non-authenticated filter will be redirected to the allowed destinations. Most HTTP traffic outside of that defined in the non-authenticated filter will be redirected.



Note: Although non-authenticated filters definitions are used to assist in the redirection of HTTP traffic for restricted or denied destinations, the non-authenticated filter is not restricted to HTTP operations. The filter definition is general. Any traffic other than HTTP that the filter does not explicitly allow will be discarded by the controller.

The non-authenticated filter is applied by the Enterasys Wireless Controller to sessions until they successfully complete authentication. The authentication procedure results in an adjustment to the user's applicable filters for access policy.

Typically, default filter ID access is less restrictive than a non-authenticated profile. It is the administrator's responsibility to define the correct set of access privileges.



Note: Administrators must ensure that the non-authenticated filter allows access to the corresponding authentication server:

- **Internal Captive Portal** — IP address of the VNS interface
- **External Captive Portal** — IP address of external Captive Portal server

Non-authenticated Filter Examples

A basic non-authenticated filter for internal Captive Portal should have three rules, in the following order:

Table 5-3 Non-authenticated Filter Example A

In	Out	Allow	IP / Port	Description
x	x	x	IP address of default gateway (VNS Interface IP)	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		*.*.*	Deny everything else.



Note: For external Captive Portal, an additional rule to Allow (in/out) access to the external Captive Portal authentication/Web server is required.

If you place URLs in the header and footer of the Captive Portal page, you must explicitly allow access to any URLs mentioned in the authentication server's page, such as:

- **Internal Captive Portal** — URLs referenced in a header or footer
- **External Captive Portal** — URLs mentioned in the page definition

Here is another example of a non-authenticated filter that adds two more filtering rules. The two additional rules do the following:

- Deny access to a specific IP address.
- Allow only HTTP traffic.

Table 5-4 Non-authenticated Filter Example B

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the default gateway	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as:0/24).
x	x	x	*.*.*:80	Allow all port 80 (HTTP) traffic.
x	x		*.*.*	Deny everything else.

Once a wireless device user has logged in on the Captive Portal page, and has been authenticated by the RADIUS server, then the following filters will apply:

- **Policy filters** — If a filter ID associated with this user is returned by the authentication server, then the Policy with the same name as the filter ID will be applied.
- **Default filter** — If no matching filter ID is returned from the authentication server.

Authenticated Filter Examples

Below are two examples of possible filtering rules for authenticated users. The first example disallows some specific access before allowing everything else.

Table 5-5 Filtering Rules Example A

In	Out	Allow	IP / Port	Description
x	x		*.*.*:22-23	SSH and telnet sessions
x	x		[specific IP address, range]	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.*	Allow everything else

The second example does the opposite of the first example. It allows some specific access and denies everything else.

Table 5-6 Filtering Rules Example B

In	Out	Allow	IP / Port	Description
x	x	x	[specific IP address, range]	Allow traffic to a specific IP address or address range.
x	x		*.*.*.*	Deny everything else.

ICMP Type Enforcement

ICMP filter rules can now be constrained to ICMP type/range. You can define the ICMP type/range in the Port field using the TCP/UDP port definition nomenclature. That is, define the rule as a normal IP/subnet:port signature (10.0.0.0/24:8), where the ICMP type is entered in the Port field.

This feature allows for tighter granularity over enforcement of ICMP restrictions. You can allow redirects and DF/MTU indications, and deny ICMP Echo (pings) for users.

Filtering Rules for a Default Filter

After authentication of the wireless device user, the default filter will apply only after:

- No filter ID attribute value is returned by the authentication server for this user.
- No Policy match is found on the Enterasys Wireless Controller for the filter ID value.

The final rule in the default filter should be a catch-all rule for any traffic that did not match a filter. A final Allow All rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found. VNS Policy is also applicable for Captive Portal and MAC-based authorization.

Default Filter Examples

The following are examples of filtering rules for a default filter:

Table 5-7 Default Filter Example A

In	Out	Allow	IP / Port	Description
x	x		Intranet IP, range	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to Web browsing
x	x		Intranet IP	Deny all access to a specific IP
x	x	x	*.*.*.*	Allow everything else

Table 5-8 Default Filter Example B

In	Out	Allow	IP / Port	Description
	x		Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to Web browsing the host
x			Intranet IP 10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as telnet (port 23) or FTP (port 21)
	x	x	Intranet IP 10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network
x		x	Intranet IP 10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x		*.*.*.*	Deny everything else

Filtering Rules Between Two Wireless Devices

Traffic from two wireless devices that are on the same VNS and are connected to the same Wireless AP will pass through the Enterasys Wireless Controller and therefore be subject to filtering policy. You can set up filtering rules that allow each wireless device access to the default gateway, but also prevent each device from communicating with each other.

Add the following two rules to a filter ID filter, before allowing everything else:

Table 5-9 Rules Between Two Wireless Devices

In	Out	Allow	IP / Port	Description
x	x	x	[Intranet IP]	Allow access to the Gateway IP address of the VNS only
x	x		[Intranet IP, range]	Deny all access to the VNS subnet range (such as 0/24)
x	x	x	*.*.*.*	Allow everything else



Note: You can also prevent the two wireless devices from communicating with each other by setting **Block Mu to MU traffic**. See [“Configuring a Basic WLAN Service”](#) on page 6-2.

Defining Filter Rules for Wireless APs

You can also apply filter rules on the Wireless AP. Applying filter rules at the Wireless AP helps restrict unwanted traffic at the edge of your network. The Wireless APs can support up to a

maximum of 32 filters rules per group. Filtering at the Wireless AP can be configured with the following Topology types:

- **Bridge Traffic Locally at the AP** — If filtering at the Wireless AP is enabled on a Bridge Traffic Locally at the AP topology, the filtering is applied to traffic in both the uplink and downlink direction — the uplink direction is from the wireless device to the network, and the downlink direction is from the network to the wireless device.
- **Routed and Bridge Traffic Locally at the HWC** — If filtering at the Wireless AP is enabled on a Routed or Bridge Traffic Locally at the HWC topology, the filtering is applied only to traffic in the UL direction. The filters applied in the UL direction at the Wireless AP can be the same as or different from filters applied at the Enterasys Wireless Controller.

Wireless AP Filtering

When filtering at the Wireless AP is enabled, Wireless APs obtain client filter information from the Enterasys Wireless Controller. In addition, direct inter-Wireless AP communication allows Wireless APs to exchange client filter information as clients roam from one Wireless AP to another. This allows the system to achieve a very fast roaming time. To take advantage of inter-Wireless AP communication, you should configure the network such that Wireless APs in the mobility domain can communicate with each other through the Wireless AP's Ethernet interface. Also, multicast traffic with an IP address of 224.0.1.178 should be allowed between Wireless APs.

Configuring Filter Rules

To configure filter rules for the controller:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **Policies** pane and click the Policy you want to edit, or click the **New** button to create a new policy.
The **Policy** configuration page is displayed.
3. Click the **Filter Rules** tab.
The **HWC Filters** tab displays. See [Figure 5-2](#) on page 5-8.
4. Configure filter rules for the controller. See [Table 5-10](#) on page 5-9.

To configure filter rules for the wireless AP:

1. Select the **AP Filtering** checkbox to enable the filter rules defined on the HWC Filters tab to be applied by Wireless APs. The **Custom AP Filters** checkbox becomes available.
2. Select the **Custom AP Filters** checkbox to configure additional filters for the APs. An **AP Filters** tab is added to the window.
3. Click the **AP Filters** tab. The AP Filters tab displays. [Figure 5-3](#) on page 5-8.
4. Configure filter rules for the APs. See [Table 5-10](#) on page 5-9.

Figure 5-2 Filter Rules Page - HWC Filters Tab

Virtual Network Configuration

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

Policy: anV1NonAuthPolicy

Inherit filter rules from currently applied policy

HWC Filters AP Filtering

Rule	In	Out	IP : Port	Protocol	Priority	ToS/DSCP	Access	CoS
D	dest	none	0.0.0.0/0	N/A	N/A	N/A	Allow	N/A
D	none	src	0.0.0.0/0	N/A	N/A	N/A	Allow	N/A

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

Add Edit Delete Up Down

New Delete Save

Figure 5-3 Filter Rules Page - AP Filters Tab

Virtual Network Configuration

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

Policy: anV1NonAuthPolicy

Inherit filter rules from currently applied policy

HWC Filters **AP Filters** AP Filtering Custom AP Filters

Rule	In	Out	IP : Port	Protocol	Priority	ToS/DSCP	Access	CoS
D	dest	none	0.0.0.0/0	N/A	N/A	N/A	Allow	N/A
D	none	src	0.0.0.0/0	N/A	N/A	N/A	Allow	N/A

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

Add Edit Delete Up Down

New Delete Save

Table 5-10 HWC and AP Filters tabs - Fields and Buttons

Field/Button	Description
Inherit filter rules from currently applied policy	<p>Select if you do not want to apply new filter settings.</p> <p>If you do not apply new filter settings, the wireless client uses filter settings from a previously applied policy. If filters were never defined, then the system enforces the filters from the Global Default Policy.</p> <p>If you choose to apply new filter settings by not selecting this option, the new filter settings will overwrite any pre-existing filter settings.</p>
AP Filtering	Select to apply the configured filters to the Wireless AP.
Custom AP Filters	Select to create a new filter definition to apply to the Wireless AP.
Rule	<p>Identifies the type of filter rule. Options are:</p> <ul style="list-style-type: none"> • D - Default rule • I - Internal (read-only) • T - Local interface rule • U - User-defined rule
In	<p>Identifies the rule that applies to traffic from the wireless device that is trying to get on the network. You can change this setting using the drop-down menu. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) - available in Advanced Filtering Mode only • Source (src) • None • Both - available in Advanced Filtering Mode only <p>The policy for inbound traffic may be impacted by the selection (mode) for Egress Filtering. For more information, see Egress Filtering Mode.</p>
Out	<p>Identifies the rule that applies to traffic from the network host that is trying to get to a wireless device. You can change this setting using the drop-down menu. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>The policy for outbound traffic may be impacted by the selection (mode) for Egress Filtering. For more information, see Egress Filtering Mode.</p>
Allow	Select the Allow checkbox to allow this rule. Otherwise the rule is denied.
IP:Port	Identifies the IP address and port to which this filter rule applies.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
Up, Down	Select a filter rule and click to either move the rule up or down in the list. The filtering rules are executed in the order in which you define them.
Add	Click to add a filter rule. The fields in the Add Filter area are enabled.

Table 5-10 HWC and AP Filters tabs - Fields and Buttons (continued)

Field/Button	Description
Delete	Click to remove this filter rule.
Save	Click to save the configuration.
Add Filter section	
IP/subnet	<p>Select one of the following:</p> <ul style="list-style-type: none"> • User Defined, then type the destination IP address and mask. Use this option to explicitly define the IP/subnet aspect of the filter rule. • IP - select to map the rule to the associated Topology IP address. • Subnet - select to map the rule to the associated Topology segment definition (IP address/mask).
Port	<p>From the Port drop-down list, select one of the following:</p> <p>User Defined, then type the port number.</p> <p>Use this option to explicitly specify the port number.</p> <p>A specific port type. The appropriate port number or numbers are added to the Port text field.</p>
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A. " ICMP Type Enforcement " on page 5-5 provides more information about selecting the ICMP protocol.
In Filter	<p>In the drop-down menu, select an option that refers to traffic from the network host that is trying to get to a wireless device. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>The policy for inbound traffic filters may be impacted by the selection (mode) for Egress Filtering. For more information, see Egress Filtering Mode.</p>
Out Filter	<p>In the drop-down menu, select an option that refers to traffic from the wireless device that is trying to get on the network. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>The policy for outbound traffic filters may be impacted by the selection (mode) for Egress Filtering. For more information, see Egress Filtering Mode.</p>
OK	Click to add the filter rule to the filter group. The information is displayed in the filter rule table.
Cancel	Click Cancel to discard your changes.



Note: For Captive Portal assignment, define a rule to allow access to the default gateway for this controller. You should also configure a rule denying HTTP on the controller.

Configuring WLAN Services

This chapter describes WLAN service configuration, including:

For information about...	Refer to page...
WLAN Services Overview	6-1
Third-party AP WLAN Service Type	6-2
Configuring a Basic WLAN Service	6-2
Configuring Privacy	6-8
Configuring Accounting and Authentication	6-14
Configuring the QoS Policy	6-34

WLAN Services Overview

A WLAN Service represents all the RF, authentication and QoS attributes of a wireless access service. The WLAN Service can be one of the following types:

- **Standard** — A conventional service. Only APs running Enterasys Wireless software can be part of this WLAN Service. This type of service may be used as a Bridged @ Controller, Bridged @ AP, or Routed VNS. This type of service provides access for mobile stations. Therefore, policies can be assigned to this type of WLAN service to create a VNS.
- **Third Party AP** — A wireless service offered by third party APs. This type of service provides access for mobile stations. Therefore, policies can be assigned to this type of WLAN service to create a VNS.
- **Dynamic Mesh and WDS (Static Mesh)**— A group of APs organized into a hierarchy for the purposes of providing a Wireless Distribution Service. This type of service is in essence a wireless trunking service rather than a service that provides access for stations. As such, this service cannot have policies attached to it.
- **Remote** — A service that resides on the edge (foreign) Enterasys Wireless Controller. Pairing a remote service with a remoteable service on the designated home Enterasys Wireless Controller allows you to provision centralized WLAN Services in the mobility domain. This is known as centralized mobility.

The remote service should have the same SSID name and privacy as the home remoteable service. Any WLAN Service/VNS can be a remoteable service, though deployment preference is given to tunneled topologies (Bridged@Controller and Routed).

To reduce the amount of information distributed across the mobility domain, you will explicitly select which WLAN Services are available from one controller to any other controller in the mobility domain.

The WLAN Service remoteable property is synchronized with the availability peer, making the WLAN service published by both the home and foreign controllers.

The following types of authentication are supported for remote WLAN services:

- None
- Internal/External Captive Portal
- Guest Portal
- Guest Splash
- AAA/802.1x

Third-party AP WLAN Service Type

For more information, see [Chapter 13, Working with Third-party APs](#).

A third-party AP WLAN Service allows for the specification of a segregated subnet by which non-Enterasys Wireless APs are used to provide RF services to users while still utilizing the Enterasys Wireless Controller for user authentication and user policy enforcement.



Note: Third-party AP devices are not fully integrated with the system and therefore must be managed individually to provide the correct user access characteristics.

The definition of third-party AP identification parameters allows the system to be able to differentiate the third-party AP device (and corresponding traffic) from user devices on that segment. Devices identified as third-party APs are considered pre-authenticated, and are not required to complete the corresponding authentication verification stages defined for users in that segment (typically Captive Portal enforcement).

In addition, third-party APs have a specific set of filters (third-party) applied to them by default, which allows the administrator to provide different traffic access restrictions to the third-party AP devices for the users that use those resources. The third-party filters could be used to allow access to third-party APs management operations (for example, HTTP, SNMP).

Configuring a Basic WLAN Service

To Configure a WLAN Service:

1. From the top menu, click **VNS Configuration**. Then, in the left pane, select **WLAN Services**.

The WLAN Services window displays.

2. To create a new service, click the **New** button. The New WLAN Services configuration window displays.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes links for Home, Logs, Reports, Wireless Controller, Wireless APs, **WNS Configuration**, Mitigator, Help, and LOGOUT. The left sidebar contains a tree view with categories: New..., Global, Virtual Networks, WLAN Services (selected), Policies, Classes of Service, and Topologies. The main content area is titled "WLAN:" and contains a "WLAN Services" configuration box. This box has a "Core" section with a "Name:" text field, a "Service Type:" section with radio buttons for Standard (selected), WDS, Mesh, Third Party AP, and Remote, and an "SSID:" text field. Below this is a "Status" section with "Synchronize:" and "Enable:" checkboxes, both of which are checked. A red note below the Synchronize checkbox reads "Replicated when Synchronize Configuration is enabled". A "Save" button is located at the bottom right of the configuration box.

- a. Enter a name for the WLAN service.
- b. Select the service type.
- c. Change the SSID (optional).
- d. Click Save.

The WLAN Services Configuration page displays.

- To edit an existing service, select the desired service from the left pane. The WLAN Services Configuration page displays. Table 6-1 describes the WLAN services configuration page fields and buttons.

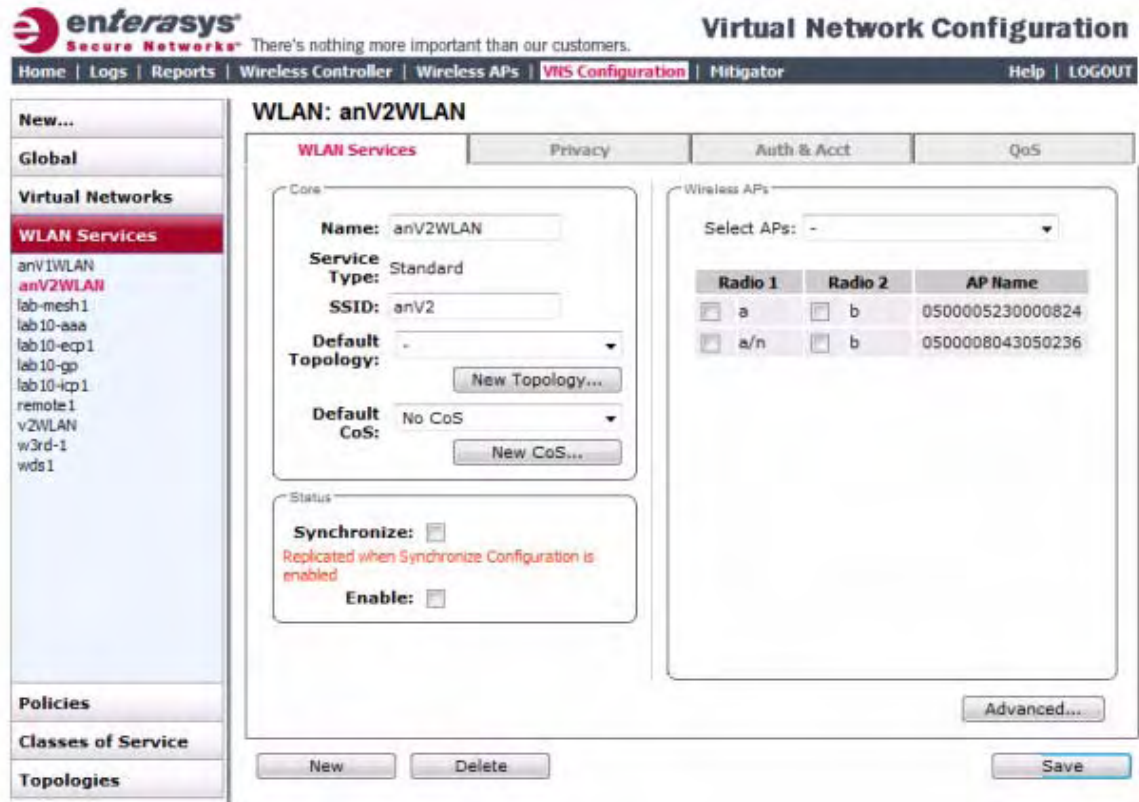


Table 6-1 WLAN Services Configuration Page

Field/Button	Description
Core	
Name	Enter a name for this WLAN service
Service Type	<p>Select the type of service to apply to this WLAN service. Options include:</p> <ul style="list-style-type: none"> Standard WDS Mesh Third Party AP Remote <p>If you selected Remote as the Service Type, select the Privacy type.</p> <p>If you set Service Type as either Standard or Remote, select Synchronize, in the Status area, if desired. Enabling this feature allows availability pairs to be synchronized automatically</p>
SSID	The software automatically populates this field with the WLAN service name that you supply. Optionally, you can change this. If you are creating a remote WLAN service, select the SSID of the remoteable service that this remote service will be paired with.

Table 6-1 WLAN Services Configuration Page (continued)

Field/Button	Description
Default Topology	<p>From the drop-down list, select a preconfigured topology or click New Topology to create a new one. Refer to “Configuring a Basic Topology” on page 4-2 for information about how to create a new topology.</p> <p>A WLAN service uses the topology of the policy assigned to the VNS, if such a topology is defined. If the policy doesn't define a topology, you can assign an existing topology as the default topology to the WLAN service. If you choose not to assign a default topology to the WLAN service, the WLAN service will use the topology of the global default policy (by default, Bridged at AP Untagged).</p> <p>Note: You cannot assign a default topology to a WDS, 3rd party, or remote WLAN service.</p>
Default CoS	<p>From the drop-down list, select a preconfigured CoS or click New CoS to create a new one. Refer to “Configuring Classes of Service” on page 8-1 for information on how to create a new CoS.</p> <p>A WLAN service uses the CoS of the policy assigned to the VNS, if such a CoS is defined. If the policy doesn't define a CoS, you can assign an existing CoS as the default CoS to the WLAN service. If you choose not to assign a default CoS to the WLAN service, the WLAN service will use the CoS of the global default policy (by default, Bridged at AP Untagged).</p> <p>Note: You cannot assign a default CoS to a WDS, 3rd party, or remote WLAN service.</p>
Status	
Enable	<p>Select the checkbox to enable this WLAN service. Otherwise, deselect this checkbox. The WLAN service is enabled by default, unless the number of supported enabled WLAN Services has been reached.</p>

Table 6-1 WLAN Services Configuration Page (continued)

Field/Button	Description
Wireless APs	
Select APs	<p>Select APs and their radios by grouping. Options include:</p> <ul style="list-style-type: none"> • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2. • clear all selections — Click to clear all of the AP radio assignments. • original selections — Click to return to the AP radio selections prior to the most recent save. <p>Note: If two Enterasys Wireless Controllers have been paired for availability (for more information, see “Availability” on page 11-1), each Enterasys Wireless Controller's registered Wireless APs are displayed as foreign in the list of available Wireless APs on the other Enterasys Wireless Controller</p>
Radio 1	Assign the Wireless APs' Radios to the service by selecting the individual radios' checkboxes. Alternatively, you can use the Select APs list.
Radio 2	Assign the Wireless APs' Radios to the service by selecting the individual radios' checkboxes. Alternatively, you can use the Select APs list.
Advanced	Click to access the WLAN service advanced configuration options. The Advanced configuration page options are described in Table 6-2 on page 6-7.
New	Click to create a new WLAN service.
Delete	Click to delete this WLAN service.
Save	Click to save the changes to this WLAN service. If you are creating a new service, the WLAN Services configuration window is displayed, allowing you to assign Wireless APs to the service.

Table 6-2 Advanced WLAN Service Configuration Page

Field/Button	Description
Timeout	
Idle (pre)	Specify the amount of time in minutes that a Mobile user can have a session on the controller in pre-authenticated state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time. The default value is 5 minutes.
Idle (post)	Specify the amount of time in minutes that a Mobile user can have a session on the controller in authenticated state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time. The default value is 30 minutes.
Session	Specify the maximum number of minutes of service to be provided to the user before the termination of the session.
RF - select one or more of the following options:	
Suppress SSID	Select to prevent this SSID from appearing in the beacon message sent by the Wireless AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
Enable 11h support	Select to enable 11h support. By default this option is disabled. Enterasys recommends that you enable this option.
Apply power reduction to 11h clients	Select to enable the Wireless AP to use reduced power (as does the 11h client). By default this option is disabled. Enterasys recommends that you enable this option. This option is available only if you enable 11h support.
Process client IE requests	Select to enable the Wireless AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IE's in the corresponding Probe Response frames. By default this option is disabled. Enterasys recommends that you enable this option.
Energy Save Mode	Select to reduce the number of beacons the AP transmits on a BSSID when no client is associated with the BSSID. This reduces both the power consumption of the AP and the interference created by the AP when no client is associated.
Egress Filtering Mode	
Enforce explicitly defined "Out" rules	Traffic is filtered as configured. For more information, see "Configuring Egress Filtering Mode" on page 7-14.
Apply "In" rules to "out" direction traffic	The role of the source and destination addresses are reversed. For more information, see "Configuring Egress Filtering Mode" on page 7-14.
Client Behavior	
Block MU to MU traffic	Select the Block Mu to MU traffic checkbox if you want to prevent two devices associated with this SSID and registered as users of the controller, to be able to talk to each other. The blocking is enforced at the L2 (device) classification level.

Table 6-2 Advanced WLAN Service Configuration Page (continued)

Field/Button	Description
802.1D	
8021D Base Port: xxx	The 802.1D Base Port number in the 802.1D area is the port number by which NetSight recognizes the SSID. It is read-only.
Remote Service	
Remoteable	Select the checkbox if you want to pair this service with a remote service.
Inter-WLAN Service Roaming	
Permit Inter-WLAN Service Roaming	Select to enable a client on a controller to maintain the session, including the IP address and policy assignment, while roaming between VNSs having the same SSID and privacy settings. If not selected, when the client roams among VNSs, the existing session terminates and a new session starts with the client having to associate and authenticate again. The list of VNSs that share the same SSID and privacy settings displays below.
Close	Click to close this page.



Note: If two Enterasys Wireless Controllers have been paired for availability (for more information, see “[Availability](#)” on page 11-1), each Enterasys Wireless Controller's registered Wireless APs are displayed as foreign in the list of available Wireless APs on the other Enterasys Wireless Controller.

After you have assigned a Wireless AP Radio to eight WLAN Services, it will not appear in the list for another WLAN Service setup. Each Radio can support up to eight SSIDs (16 per AP). Each AP can be assigned to any of the VNSs defined within the system. The Enterasys Wireless Controller can support the following active VNSs:

- C5110 – Up to 128 VNSs
- C4110 – Up to 64 VNSs
- C20 – Up to 8 VNSs
- C25 – Up to 16 VNs
- V2110 – Up to 48 VNSs



Note: You can assign the Radios of all three Wireless AP variants — Enterasys Wireless AP, Enterasys Wireless Outdoor AP, and Wireless 802.11n AP — to any VNS.

Configuring Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. The Enterasys Wireless Controller provides several privacy mechanism to protect data over the WLAN.

There are five privacy options:

- **None**
- **Static Wired Equivalent Privacy (WEP)** — Keys for a selected VNS, so that it matches the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 VNSs.

For each VNS, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.

- **Dynamic Keys** — The dynamic key WEP mechanism changes the key for each user and each session.
- **Wi-fi Protected Access (WPA)**
 - version 1 with encryption by temporal key integrity protocol (TKIP)
 - version 2 with encryption by advanced encryption standard with counter-mode/CBC-MAC protocol (AES-CCMP)
- **Wi-Fi Protected Access (WPA) Pre-Shared key (PSK)** — Privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.



Note: Regardless of the Wireless AP model or WLAN Service type, a maximum of 112 simultaneous clients, per radio, are supported by all of the data protection encryption techniques.

About Wi-Fi Protected Access (WPA V1 and WPA V2)



Note: To achieve the strongest encryption protection for your VNS, Enterasys recommends that you use WPA v.1 or WPA v.2.

WPA v1 and WPA v2 add authentication to WEP encryption and key management. Key features of WPA privacy include:

- Specifies 802.1x with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet (unicast key) or after the specified re-key time interval (broadcast key) expires
- An enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise
- A Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, which ensures that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

- A 128-bit key length, for the WPA2/802.11i implementation of AES
- Four stages that make up one round. Each round is iterated 10 times.
- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval expires.

- The Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include:
 - Counter mode (CTR) that achieves data encryption
 - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

The following is an overview of the WPA authentication and encryption process:

1. The wireless device client associates with Wireless AP.
2. Wireless AP blocks the client's network access while the authentication process is carried out (the Enterasys Wireless Controller sends the authentication request to the RADIUS authentication server).
3. The wireless client provides credentials that are forwarded by the Enterasys Wireless Controller to the authentication server.
4. If the wireless device client is not authenticated, the wireless client stays blocked from network access.
5. If the wireless device client is authenticated, the Enterasys Wireless Controller distributes encryption keys to the Wireless AP and the wireless client.
6. The wireless device client gains network access via the Wireless AP, sending and receiving encrypted data. The traffic is controlled with permissions and policy applied by the Enterasys Wireless Controller.

Wireless 802.11n APs and WPA Authentication



Note: If you configure a WLAN Service to use either WEP or TKIP authentication, any Wireless 802.11n AP associated to a VNS using that service will be limited to legacy AP performance rates.

If a VNS is configured to use WPA authentication, any Wireless 802.11n AP within that VNS will do the following:

- WPA v.1 — If WPA v.1 is enabled, the Wireless 802.11n AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 — If WPA v.2 is enabled, the Wireless 802.11n AP will do the following:
 - If WPA v.1 is enabled, the Wireless 802.11n AP will advertise TKIP as an available encryption protocol.



Note: If WPA v.2 is enabled, the Wireless 802.11n AP does not support the **Auto** option.

- If WPA v.1 is disabled, the Wireless 802.11n AP will advertise the encryption cipher AES (Advanced Encryption Standard).



Note: The security encryption for some network cards must not to be set to WEP or TKIP to achieve a data rate beyond 54 Mbps.

WPA Key Management Options

Wi-Fi Protected Access (WPA v1 and WPA v2) privacy offers you the following key management options:

- **None** — The wireless client device performs a complete 802.1x authentication each time it associates or tries to connect to a Wireless AP.
- **Opportunistic Keying** — Opportunistic Keying or opportunistic key caching (OKC) enables the client devices to roam fast and securely from one Wireless AP to another in 802.1x authentication setup.

The client devices that run applications such as video streaming and VoIP require rapid reassociation during roaming. OKC helps such client devices by enabling them to rapidly reassociate with the Wireless APs. This avoids delays and gaps in transmission and thus helps in secure fast roaming (SFR).



Note: The client devices should support OKC to use the OKC feature in the Enterasys WLAN.

- **Pre-authentication** — Pre-authentication enables a client device to authenticate simultaneously with multiple Wireless APs in 802.1x authentication setup. When the client device roams from one Wireless AP to another, it does not have to perform the complete 802.1x authentication to reassociate with the new Wireless AP as it is already pre-authenticated with it. This reduces the reassociation time and thus helps in seamless roaming.



Note: The client devices should support pre-authentication to use the pre-authentication feature in Enterasys WLAN.

- **Opportunistic Keying & Pre-auth** — Opportunistic Keying and Pre-auth options is meant for environments where device clients supporting either authentication method (OKC or Pre-Auth) may be expected. The method that is used in each case is up to the individual client device.

Configuring WLAN Service Privacy

To Configure Privacy:

1. If the WLAN Service configuration page is not already displayed, from the top menu, click **VNS Configuration**. Then, in the left pane, select **WLAN Services**. The WLAN Services window displays.
2. Select the desired service to edit from the left pane. The WLAN Service configuration page is displayed.

- Click the **Privacy** tab, then select the desired privacy method. The WLAN Services Privacy tab displays. [Table 6-3](#) describes the WLAN services privacy tab fields and buttons.

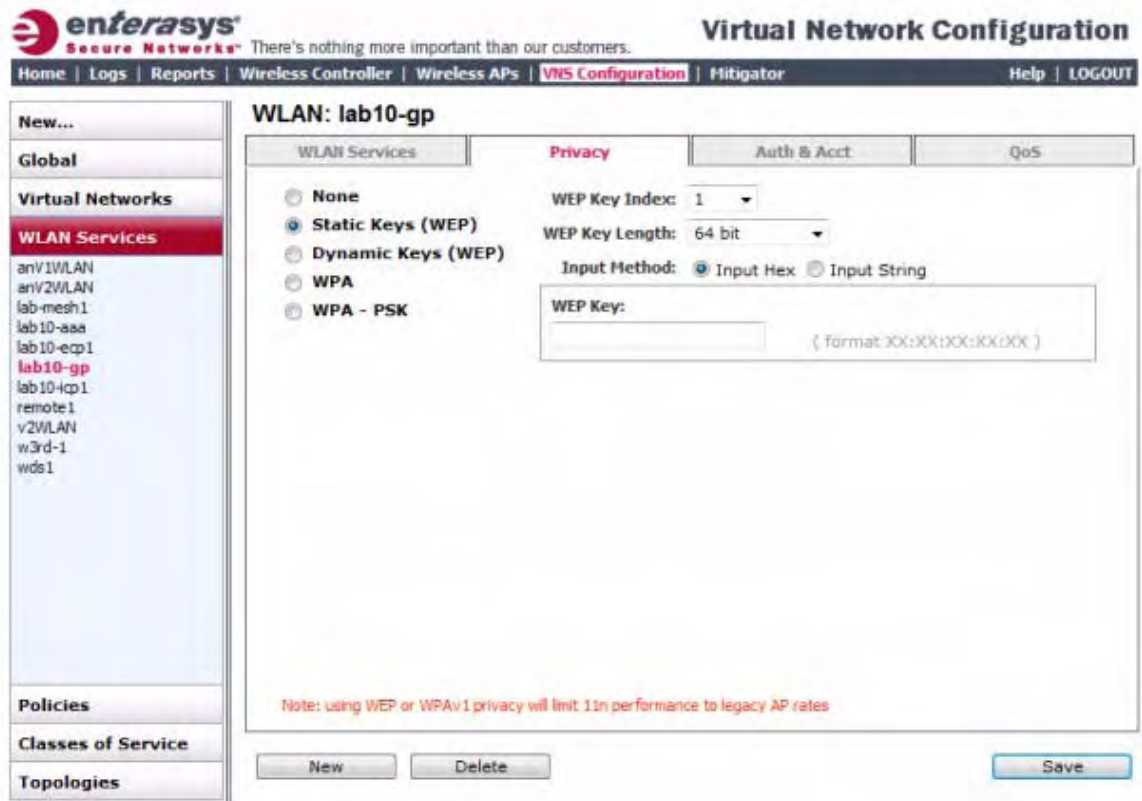


Table 6-3 WLAN Services Privacy Tab - Fields and Buttons

Field/Button	Description
None	Select to configure a WLAN service with no privacy settings.
Static Keys (WEP)	Select to configure static key (WEP) privacy settings.
WEP Key Index	From the WEP Key Index drop-down list, select the WEP encryption key index. Options are 1 to 4. Specifying the WEP key index is supported only for AP36XX Wireless APs. This field is available only when configuring static keys.
WEP Key Length	From the WEP Key Length drop-down list, click the WEP encryption key length . Options are: 64-bit, 128-bit, and 152-bit. This field is available only when configuring static keys.
Input Method	Select one of the following input methods: <ul style="list-style-type: none"> Input Hex — If you select Input Hex, type the WEP key input in the WEP Key box. The key is generated automatically, based on the input. Input String — If you select Input String, type the secret WEP key string used for encrypting and decrypting in the Strings box. The WEP Key box is automatically filled by the corresponding Hex code. This field is available only when configuring static keys.
WEP Key	Type the WEP key using the input method chosen above.

Table 6-3 WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Dynamic Keys (WEP)	Select to configure dynamic keys (WEP) privacy settings.
WPA	Select to configure WPA privacy settings.
WPA - PSK	Select to configure dynamic keys (WEP) privacy settings.
WPA v.1	<p>Select the checkbox to enable WPA v.1 encryption, and then select an encryption method:</p> <p>Auto — If you click Auto, the Wireless AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.</p> <p>AES only — If you click AES, the Wireless AP advertises CCMP as an available encryption protocol. It will not advertise TKIP</p> <p>This field is available only when configuring WPA and WPA - PSK privacy settings.</p>
WPA v.2	<p>Select the checkbox to enable WPA v.2 encryption, and then select an encryption method:</p> <ul style="list-style-type: none"> • Auto — If you click Auto, the Wireless AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default. • AES only — If you click AES, the Wireless AP advertises CCMP as an available encryption protocol. It will not advertise TKIP <p>This field is available only when configuring WPA and WPA - PSK privacy settings.</p>
Key Management Options	<p>Click one of the following key management options:</p> <ul style="list-style-type: none"> • None — The mobile units (client devices) perform a complete 802.1x authentication each time they associate or connect to a Wireless AP. • Opportunistic Keying — Enables secure fast roaming (SFR) of mobile units. For more information, see Configuring WLAN Service Privacy on 6-11. • Pre-authentication — Enables seamless roaming. For more information, see Configuring WLAN Service Privacy on 6-11. • Opportunistic Keying & Pre-auth — For more information, see Configuring WLAN Service Privacy on 6-11.
Broadcast re-key interval	<p>To enable re-keying after a time interval, select the Broadcast re-key interval box, then type the time interval after which the broadcast encryption key is changed automatically. The default is 3600 seconds.</p> <p>If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions which will reduce the level of security for wireless communications.</p>
Group Key Power Save Retry	<p>To enable the group key power save retry</p> <p>The group key power save retry is only supported for AP36XX Wireless APs.</p>

Table 6-3 WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Input Method	Select one of the following input methods: <ul style="list-style-type: none"> • Input Hex — If you select Input Hex, type the pre-shared key as hex characters. • Input String — If you select Input String, type the pre-shared key as a string of characters.
Pre-shared key String	In the Pre-Shared Key box, type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key. To proofread your entry before saving the configuration, click Unmask to display the Pre-Shared Key. To mask the key, click Mask
Save	Click to save the configuration.

Configuring Accounting and Authentication

The next step in configuring a WLAN Service is to set up the authentication mechanism. There are various authentication modes available:

- none
- Internal Captive Portal
 - GuestPortal
 - GuestSplash
- External Captive Portal
- 802.1x authentication, the wireless device user must be authenticated before gaining network access



Note: You cannot configure accounting and authentication for a remote WLAN service. The authentication that you configure for the corresponding remoteable WLAN service applies to the remote WLAN service as well.

The first step for any type of authentication is to select RADIUS servers for the following:

- Authentication
- Accounting
- MAC-based authentication

Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Enterasys Wireless Convergence Software authentication mechanism provides six VSAs for RADIUS and other authentication mechanisms ([Table 6-4](#)).

Table 6-4 Vendor Specific Attributes

Attribute Name	ID	Type	Messages	Description
Siemens-AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign policy based on AP name or location.
Siemens-AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.
Siemens-VNS-Name	4	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning policy and billing options, based on service selection.
Siemens-SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning policy and billing options, based on service selection.
Siemens-BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning policy and billing options, based on service selection and location.
Siemens-Policy-Name	7	string	Sent to RADIUS server	The name of the policy applied to the station's session.
Siemens-Topology-Name	8	string	Sent to RADIUS server	The name of the topology applied to the station's session.
Siemens-Ingress-RC-Name	9	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's outbound traffic.
Siemens-Egress-RC-Name	10	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's inbound traffic.

The RADIUS message also includes RADIUS attributes Called-Station-Id and Calling-Station-Id to include the MAC address of the wireless device.



Note: Siemens-URL-Redirection is supported by MAC-based authentication.

Defining Accounting Methods for a WLAN Service

Accounting tracks the activity of wireless device users. There are two types of accounting available:

- **Controller accounting** — Enables the Enterasys Wireless Controller to generate Call Data Records (CDRs), containing usage information about each wireless session. CDR generation is enabled on a per VNS basis. For more information on CDRs, refer to section “[Call Detail Records \(CDRs\)](#)” on page 15-17.
- **RADIUS accounting** — Enables the Enterasys Wireless Controller to generate an accounting request packet with an accounting start record after successful login by the wireless device user, and an accounting stop record based on session termination. The Enterasys Wireless Controller sends the accounting requests to a remote RADIUS server.

Enterasys Wireless Controller accounting creates Call Data Records (CDRs). If RADIUS accounting is enabled, a RADIUS accounting server needs to be specified.

To Define Accounting Methods:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to define accounting methods for. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab.

The screenshot shows the 'WLAN: raffi4' configuration page in the 'Auth & Acct' tab. The 'Authentication' section is set to 'Internal' mode. Under 'MAC-based Authorization', 'Enable' is checked. The 'RADIUS Servers' section features a table with the following data:

Server	Auth	MAC	Acct
r3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The 'Common RADIUS Settings' section includes options for 'Include VSA Attributes' (AP, VNS, SSID), 'Policy', 'Topology', 'Ingress Rate Control', and 'Egress Rate Control'. A checkbox at the bottom right is checked for 'Collect Accounting Information of Wireless Controller'.

4. To enable Controller accounting, select **Collect Accounting Information of Wireless Controller**.
5. To enable RADIUS accounting, from the **RADIUS Servers** drop-down list, click the RADIUS server you want to use for RADIUS accounting, and then click **Use**.

The server name is added to the **Server** table of assigned RADIUS servers. The selected server is no longer available in the **RADIUS servers** drop-down list.

The RADIUS servers are defined on the **Global Settings** screen. For more information, see [“Defining RADIUS Servers and MAC Address Format”](#) on page 7-4.

6. In the **Server** table, select the checkbox in the **Acct** column to enable accounting for each applicable RADIUS server.
7. In the **Server** table click the RADIUS server, and then click **Configure**. The **RADIUS Parameters** dialog is displayed.

The configured values for the selected server are displayed in the table at the top.

Port	Timeout	NAS IP	NAS Identifier	Auth Type
Accl: 1813	5	VNS IP	VNS NAME	-

NAS IP Address: Use VNS IP address or use:

NAS Identifier: Use VNS name or use:

OK Cancel

8. For **NAS IP Address**, accept the default of “Use VNS IP address” or de-select the checkbox and type the IP address of a Network Access Server (NAS).
9. For **NAS Identifier**, accept the default of “Use VNS name” or type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned.
10. Click **OK**.
11. To save your changes, click **Save**.

Configuring Authentication for a WLAN Service

- **802.1x Authentication** — If 802.1x authentication mode is configured, the wireless device must successfully complete the user authentication verification prior to being granted network access. This enforcement is performed by both the user's client and the AP. The wireless device's client utility must support 802.1x. The user's EAP packets request for network access along with login identification or a user profile is forwarded by the Enterasys Wireless Controller to a RADIUS server.
- **Captive Portal Authentication** — For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the non-authenticated filter. For more information, see “[Filtering Rules](#)” on page 5-3. One of these destinations should be a server, either internal or external, which presents a Web login page — the Captive Portal. The wireless device user must input an ID and a password. This request for authentication is sent by the Enterasys Wireless Controller to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the Enterasys Wireless Controller implements policy and allows the appropriate network access.

Captive Portal authentication relies on a RADIUS server on the enterprise network. There are three mechanisms by which Captive Portal authentication can be carried out:

- **Internal Captive Portal** — The Enterasys Wireless Controller displays the Captive Portal Web page, carries out the authentication, and implements policy.
- **External Captive Portal** — After an external server displays the Captive Portal Web page and carries out the authentication, the Enterasys Wireless Controller implements policy.
- **External Captive Portal with internal authentication** — After an external server displays the Captive Portal Web page, the Enterasys Wireless Controller carries out the authentication and implements policy.

- RADIUS servers — RADIUS servers can perform the following for a WLAN Service:
 - **Authentication** — RADIUS servers are configured to provide authentication.
 - **MAC authentication** — RADIUS servers are configured to provide MAC-based authentication.
 - **Accounting** — RADIUS servers are configured to provide accounting services.

MAC-Based Authentication for a WLAN Service

- MAC-based authentication — MAC-based authentication enables network access to be restricted to specific devices by MAC address. The Enterasys Wireless Controller queries a RADIUS server for a MAC address when a wireless client attempts to connect to the network.
- MAC-based authentication can be set up on any type of WLAN Service. To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC (or a password defined by the administrator) for each user. Specifying a MAC address format and policy depends on which RADIUS server is being used.
- If MAC-based authentication is to be used in conjunction with the 802.1x or Captive Portal authentication, an additional account with a real UserID and Password must also be set up on the RADIUS server.

MAC-based authentication responses may indicate to the Enterasys Wireless Controller what VNS a user should be assigned to. Authentication (if enabled) can apply on every roam.

Assigning RADIUS Servers for Authentication

To Assign RADIUS Servers for Authentication:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.

- Click the **Auth & Acct** tab.

The screenshot shows the 'Virtual Network Configuration' interface for 'WLAN: raffi4'. The 'Auth & Acct' tab is active. In the 'Authentication' section, 'Node' is set to 'Internal'. Under 'MAC-based Authorization', the 'Enable' checkbox is checked, while 'MAC-based authorization on roam', 'Automatically Authenticate Authorized Users', and 'Allow Un-Authorized Users' are unchecked. The 'RADIUS Servers' section features a table with one entry, 'r3', and checkboxes for 'Auth', 'MAC', and 'Acct', all of which are checked. To the right, 'Common RADIUS Settings' includes 'Include VSA Attributes' checked, with sub-options for 'AP', 'VNS', and 'SSID'. At the bottom, the 'Collect Accounting Information of Wireless Controller' checkbox is also checked.

- If applicable, in the **MAC Based Authorization** section, select the **Enable** checkbox to enable the RADIUS server to perform MAC-based authentication for the VNS with Captive Portal.
 - If MAC-based authentication is enabled, select the **MAC-based authorization on roam** checkbox.
 - To automatically authenticate users, select the **Automatically Authenticate Authorized Users** checkbox.
 - To allow un-authorized users, select the **Allow Un-Authorized Users** checkbox.
 - Select a **Radius Server Timeout Policy** from the drop-down list.



Note: Only select this checkbox if you want your clients to be authorized every time they roam to another Wireless AP. If this option is not enabled, and MAC-based authentication is in use, the client is authenticated only at the start of a session.

- In the **RADIUS Servers** drop-down list, click the server you want to assign to the WLAN Service, and then click **Use**.

The server name is added to the **Server** table of assigned RADIUS servers. The selected server is no longer available in the **RADIUS servers** drop-down list.

The RADIUS servers are defined on the **Global Settings** screen. For more information, see [“Defining RADIUS Servers and MAC Address Format”](#) on page 7-4.

- In the **Server** table, select the checkboxes in the **Auth**, **MAC**, or **Acct** columns, to enable the authentication or accounting, if applicable.
- To save your changes, click **Save**.

Defining the RADIUS Server Priority for RADIUS Redundancy

If more than one server has been defined for any type of authentication, you can define the priority of the servers in the case of failover.

In the event of a failover of the main RADIUS server—if there is no response after the set number of retries—then the other servers in the list will be polled on a round-robin basis until a server responds.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

To Define the RADIUS Server Priority for RADIUS Redundancy:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab.
4. In the **Server** table, click the RADIUS server and then click **Move Up** or **Move Down** to arrange the order. The first server in the list is the active one.
5. To save your changes, click **Save**.

Configuring Assigned RADIUS Servers

Configuring assigned RADIUS servers for a VNS can include the following:

- [Defining Common RADIUS Settings](#)
- [Defining RADIUS Settings for Individual RADIUS Servers](#)
- [Testing RADIUS Server Connections](#)
- [Viewing the RADIUS Server Configuration Summary](#)
- [Removing an Assigned RADIUS Server from a WLAN Service](#)

Defining Common RADIUS Settings

To Define Common RADIUS Settings:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab.
4. In the **Common RADIUS Settings** section, select the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:
 - **AP's**
 - **VNS's**
 - **SSID**
 - **Policy**
 - **Topology**
 - **Ingress Rate Control**

- **Egress Rate Control**

The Vendor Specific Attributes must be defined on the RADIUS server.

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

Defining RADIUS Settings for Individual RADIUS Servers

To Define RADIUS Settings for Individual RADIUS Servers:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab.
4. In the **Server** table, click the RADIUS server you want to define, and then click **Configure**. The **RADIUS Parameters** dialog is displayed.

Port	Timeout	NAS IP	NAS Identifier	Auth Type
Auth 1812	5	VNS IP	VNS NAME	EAP
Acct 1813	5	VNS IP	VNS NAME	-

NAS IP Address: Use VNS IP address or use:

NAS Identifier: Use VNS name or use:

NAS port type: Wireless IEEE 802.11

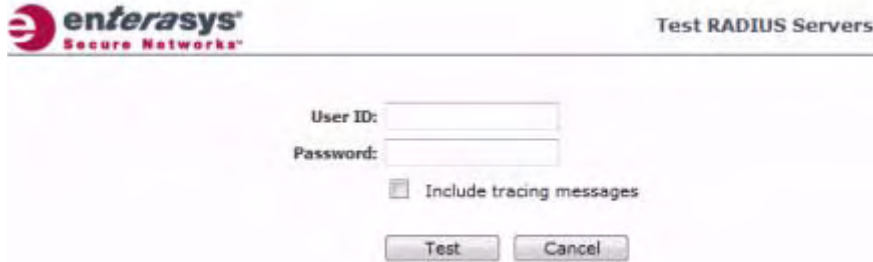
5. For **NAS IP Address**, accept the default of “Use VNS IP address” or de-select the checkbox and type the IP address of a Network Access Server (NAS).
6. For **NAS Identifier**, accept the default of “Use VNS name” or type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned.
7. Click **OK**.
8. To save your changes, click **Save**.

Testing RADIUS Server Connections

To Test RADIUS Server Connections:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab.

4. In the **Server** table, click the RADIUS server whose connection you want to test, and then click **Test**. The **Test RADIUS Servers** screen is displayed.



The RADIUS test is a test of connectivity to the RADIUS server, not of full RADIUS functionality. The Enterasys Wireless Controller's RADIUS connectivity test initiates an access-request, to which the RADIUS server will respond. If a response is received (either access-reject or access-accept), then the test is deemed to have succeeded. If a response is not received, then the test is deemed to have failed. In either case, the test ends at this point.

If the WLAN Service Authentication mode is Internal or External Captive Portal, or if MAC-Based Authorization is selected, then this test can also test a user account configured on the RADIUS server. In these cases, if proper credentials are filled in for **User ID** and **Password**, an access-accept could be returned.

If the WLAN Service Authentication mode is 802.1x, however, an Access-Reject is expected if the RADIUS server is accessible, and the text is considered a success.

5. In the **User ID** box, type the user ID that you know can be authenticated.
6. In the **Password** box, type the corresponding password. A password is not required for a AAA VNS.
7. Click **Test**. The **Test Result** screen is displayed.
8. Click **Close** after reviewing the test results.
9. To save your changes, click **Save**.

Viewing the RADIUS Server Configuration Summary

To View the RADIUS Server Configuration Summary:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab.

- In the **Server** table, click a RADIUS server whose configuration summary you want to view, and then click **Summary**. The **RADIUS Summary** screen is displayed.

Server	Use For	Priority	Port	# of Retries	Timeout	NAS Identifier	Auth. Type
r2	Acct	1	1813	3	5	VNS NAME	n/a
	Auth	1	1812	3	5	VNS NAME	EAP

- Click **Close**.
- To save your changes, click **Save**.

Removing an Assigned RADIUS Server from a WLAN Service

To Remove an Assigned RADIUS Server from a WLAN Service:

- From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
- In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to define accounting methods for. The **WLAN Services** configuration page is displayed.
- Click the **Auth & Acct** tab.
- In the **Server** table, click the assigned RADIUS server that you want to remove from the VNS, and then click **Remove**. The RADIUS server is removed from the VNS.
- To save your changes, click **Save**.

Defining a WLAN Service with No Authentication

You can set up a WLAN Service that will bypass all authentication mechanisms and run the Enterasys Wireless Convergence Software with no authentication of a wireless device user.

A WLAN Service with no authentication can still control network access using filtering rules. For more information on how to set up filtering rules that allow access only to specified IP addresses and ports, see "[Filtering Rules](#)" on page 5-3.

To Define a WLAN Service with No Authentication:

- From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
- In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to configure or click **New**. The **WLAN Services** configuration page is displayed.
- Configure the service as described in "[WLAN Services Overview](#)" on page 6-1.
- Click the **Auth & Acct** tab.
- From the **Authentication Mode** drop-down list, select **Disabled**.
- To save your changes, click **Save**.

Configuring Captive Portal for Internal or External Authentication

Captive Portal allows you to require network users to complete a defined process, such as logging in or accepting a network usage policy, before accessing the internet.

The Captive Portal options are:

- **802.1x** - Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the **Enterasys Wireless Controller** request to a RADIUS server.
- **Internal Captive Portal** — Define the parameters of the internal Captive Portal page displayed by the Enterasys Wireless Controller, and the authentication request from the Enterasys Wireless Controller to the RADIUS server.
- **External Captive Portal** — Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the Enterasys Wireless Controller request to a RADIUS server.
- **GuestPortal** — Define the parameters for a GuestPortal Captive Portal page. A GuestPortal provides wireless device users with temporary guest network services.
- **Guest Splash** — Define the parameters of the Guest Splash page displayed by the Enterasys Wireless Controller. These parameters are similar to those for an internal Captive Portal page, except that the options to configure the labels for user id and password fields are not present since login information is not required when the user is re-directed to the authorization Web page. This type of Captive Portal could be used where the user is expected to read and accept some terms and conditions before being granted network access.

Configuring Basic Captive Portal Settings

When configuring captive portal, different settings become available depending on the captive portal option you choose.

To Configure the Captive Portal Settings:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.

- Click the **Auth & Acct** tab. The Auth & ACCT page displays.

The screenshot shows the Enterasys Virtual Network Configuration interface. The left sidebar contains a tree view with categories: New..., Global, Virtual Networks, WLAN Services (selected), Policies, Classes of Service, and Topologies. Under WLAN Services, several WLANs are listed, with 'raffi4' highlighted in red. The main content area is titled 'WLAN: raffi4' and has four tabs: WLAN Services, Privacy, Auth & Acct (active), and QoS. The 'Auth & Acct' tab is active, showing the following configuration options:

- Authentication:** Mode: Internal (dropdown), with a 'Configure' button.
- MAC-based Authorization:**
 - Enable MAC-based authorization on roam
 - Automatically Authenticate Authorized Users
 - Allow Un-Authorized Users
 - RADIUS Server Timeout Policy: Treat like Access-Reject (dropdown)
- RADIUS Servers:**
 - vvm (dropdown), with a 'Use' button.
 - Table with columns: Server, Auth, MAC, Acct. One server 'r3' is listed with all three columns checked.
 - Buttons: New, Move Up, Move Down, Configure, Test, Summary, Remove.
- Common RADIUS Settings:**
 - Include VSA Attributes:
 - AP VNS SSID
 - Policy Topology
 - Ingress Rate Control
 - Egress Rate Control

At the bottom of the configuration area, there is a checkbox for 'Collect Accounting Information of Wireless Controller' which is checked, and a 'Save' button.

- In the **Authentication Mode** drop-down list, select a Captive Portal option:
 - Disabled
 - 802.1x
 - Internal
 - External
 - Guest Portal
 - Guest Splash
- Click **Configure**. The Captive Portal configuration page displays. The page display differs depending on the mode selected. See [Figure 6-1](#) for Internal and Splash modes, [Figure 6-2](#) for External and 802.1x modes, and [Figure 6-3](#) for GuestPortal mode. Use the fields and buttons available on each page to configure Captive Ports.

[Table 6-5](#) describes the internal captive portal configuration fields and buttons. [Table 6-6](#) describes the external captive portal configuration fields and buttons. Use these field and button descriptions to configure captive portal.

Figure 6-1 Captive Portal Page Configuration Page for Internal and Guest Splash Modes

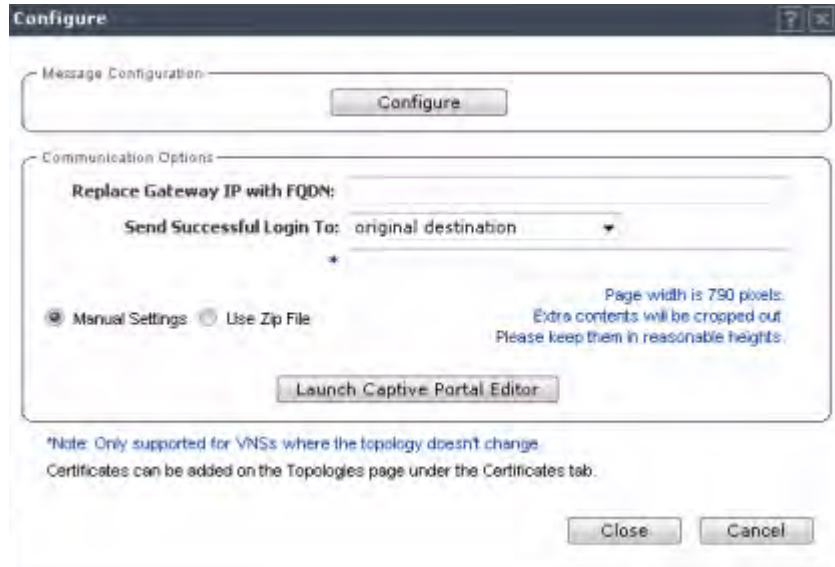


Figure 6-2 Captive Portal Page for External and 802.1x Modes

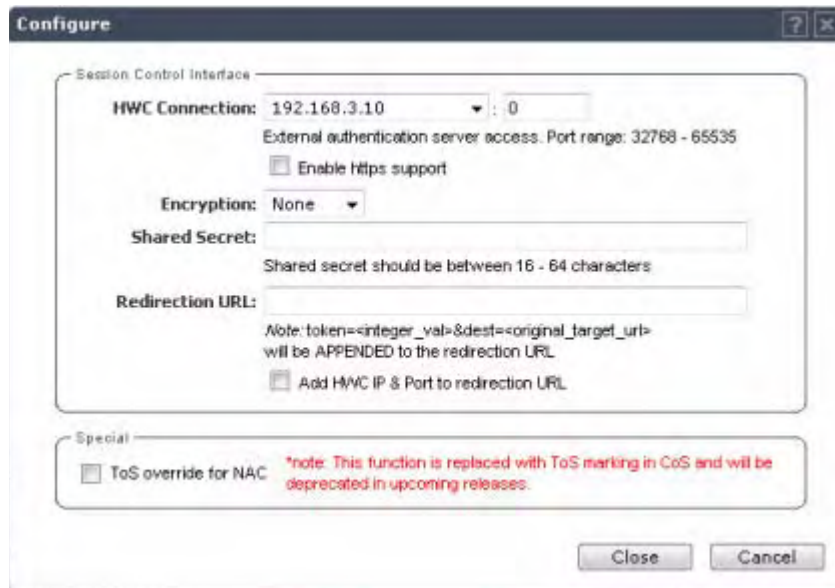


Figure 6-3 Captive Portal Page for Guest Portal Mode

Table 6-5 Configure Internal Captive Portal Page - Fields and Buttons

Field/Button	Description
Guest Portal - this section becomes available only when configuring a Guest Portal.	
Manage Guest Users	Click to add and configure guest user accounts. The Manage Guest Users page displays. For information about adding and managing guest users, see “Working with GuestPortal Administration” on page 18-1
Configure Ticket Page	Click to configure the guest portal ticket. The Configure ticket page displays. For information about how guest portal ticket pages and how to activate them, see “Working with GuestPortal Administration” on page 18-1.
Account Lifetime	Type the account lifetime, in days, for the guest account. A value of 0 specifies no limit to the account lifetime.
Guest Admin Can Set Account Lifetime	Select to enable the guest administrator to set the amount of time for which this account will be active.
Maximum Session Lifetime	Type the maximum session lifetime, in hours, for the 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.
User ID Prefix	Type a prefix that will be added to all guest account user IDs. The default is Guest .

Table 6-5 Configure Internal Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Minimum Password Length	Type a minimum password length that will be applied to all guest accounts.
Message Configuration	
Configure	Click to configure error messages that may display on the internal captive portal page. The Message Configuration page displays (Table 6-7).
Communication Options	
Replace Gateway IP with FDQN	Type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.
Send Successful Login To:	
Manual Settings	Select this option if you want to manually define the elements on the Captive Portal page. When you select this option, you enable the Launch Captive Portal Editor button.
Use Zip File	Select this option to upload a zip file that contains custom Captive Portal content. The zip file you upload must have a flat structure — it cannot contain any sub-directories. The contents of the zip must adhere to the following file formats: <ul style="list-style-type: none"> Content to be used in the captive portal login page must be in a file named login.htm Content to be used in the captive portal index page must be in a file named index.htm. The number of graphics and the size of the graphics is unlimited, and can be either .gif, .jpg, or .png.
Upload Zip File	Click the Browse button and navigate to the zip file to use for setting up the captive portal.
View Sample Login Page	Click to view the sample login page for this captive portal.
View Sample Index Page	Click to view the sample index page for this captive portal.
Download	Click to download the specified zip file. The File Download page displays.
Launch Captive Portal Editor	Click to launch the Captive Portal Editor. Using the Captive Portal Editor (Figure), you can configure the elements on the captive portal page. This button becomes available when you select the Manual Setting radio button.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Table 6-6 External Captive Portal Page - Fields and Buttons

Field/Button	Description
--------------	-------------

Session Control Interface

Table 6-6 External Captive Portal Page - Fields and Buttons

Field/Button	Description
HWC Connection	In the drop-down list, click the IP address of the external Web server. and then enter the port of the Enterasys Wireless Controller. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the Enterasys Wireless Controller to allow the Enterasys Wireless Controller to continue with the RADIUS authentication and filtering.
Enable HTTPS support	Select Enable https support if you want to enable HTTPS support (TLS/SSL) for this external captive portal.
Encryption	Select the data encryption to use. Options are: <ul style="list-style-type: none"> • None • Legacy • AES
Shared Secret	Type the password common to both the Enterasys Wireless Controller and the external Web server if you want to encrypt the information passed between the Enterasys Wireless Controller and the external Web server.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Add HWC IP & Port to redirection URL	Select the checkbox to enable redirection.
Special	
ToS override for NAC	Allows for ToS marking results in redirection to a captive portal via a NAC server.
Close	Click to save your changes and close this page.
Cancel	Click to discard the configuration



Note: You must add a filtering rule to the non-authenticated filter that allows access to the external Captive Portal site. For more information, see [“Filtering Rules”](#) on page 5-3.

Error Message Configuration

You can configure informational and error messages that a user may encounter when trying to access a captive portal.

To configure the error and informational messages:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab. The Auth & Accounting page displays.
4. In the **Authentication Mode** drop-down list, select a Captive Portal option.
5. Click Configure. The Captive Portal Configuration page displays.

6. In the Message Configuration section, click the Configure button. The Message Configuration page displays. [Table 6-7](#) describes the message configuration fields and buttons.

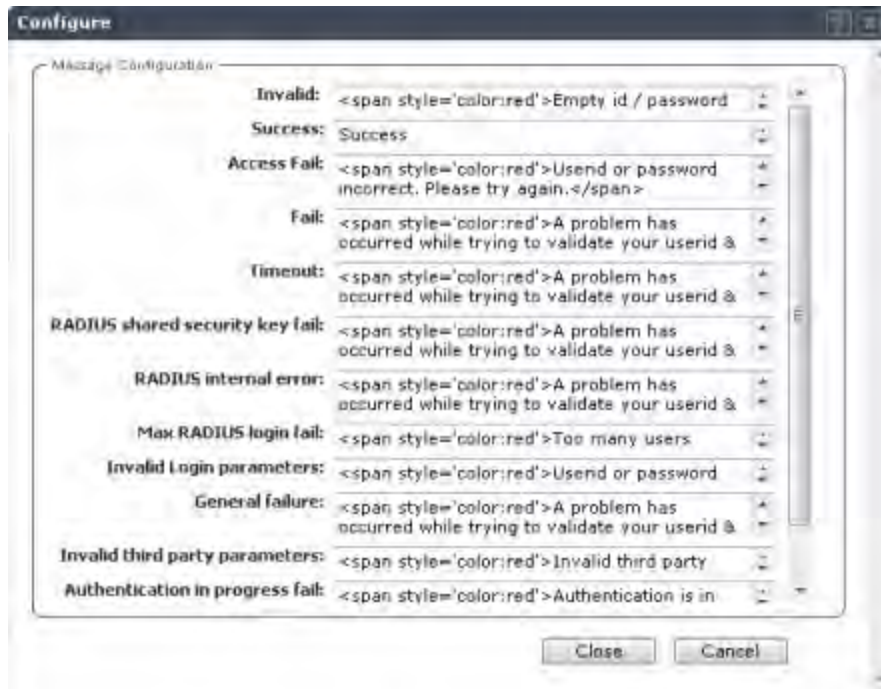


Table 6-7 Message Configuration page - Fields and Buttons

Field/Button	Description
Invalid	Enter a message indicating that the user entered an invalid username or password combination.
Success	Enter a message to indicate when a user successfully logs in.
Access Fail	Enter an error message that indicates the a user login was unsuccessful.
Fail	Enter a message indicating an internal error.
Timeout	Enter an error message indicating that the user authentication timed out.
RADIUS shared secret security key fail	Enter an error message indicating that RADIUS shared secret failed.
RADIUS internal error	Enter an error message indicating an internal RADIUS client error
Max RADIUS login fail	Enter a message that indicates that the maximum number of simultaneous captive portal logins have been reached.
Invalid Login parameters	Enter a message indicating that the user entered an invalid username or password combination.
General failure	Enter a message indicating that a general failure has occurred.
Invalid third party parameters	Enter an error message indicating that one or more parameters passed from the external captive portal server to the controller is either invalid or missing.
Authentication in progress fail	Enter a message indicating that the user credentials were not authenticated.
Topology Change	Enter an error message indicating that the topology failed.

Table 6-7 Message Configuration page - Fields and Buttons (continued)

Field/Button	Description
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Using the Captive Portal Editor

The Captive Portal Editor enables you to configure the look and feel of a captive portal page.

To launch the captive Portal Editor:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **Auth & Acct** tab. The Auth & Accounting page displays.
4. In the **Authentication Mode** drop-down list, select a Captive Portal option.
5. Click Configure. The Captive Portal Configuration page displays.
6. In the Communications Options section, select Manual Settings and then click the Launch Captive Portal Editor button. The Captive Portal Editor page displays. [Table 6-8](#) describes the captive portal editor fields and buttons.



Note: The Captive Portal Editor page supports only one administrator editing a captive portal page at one time.

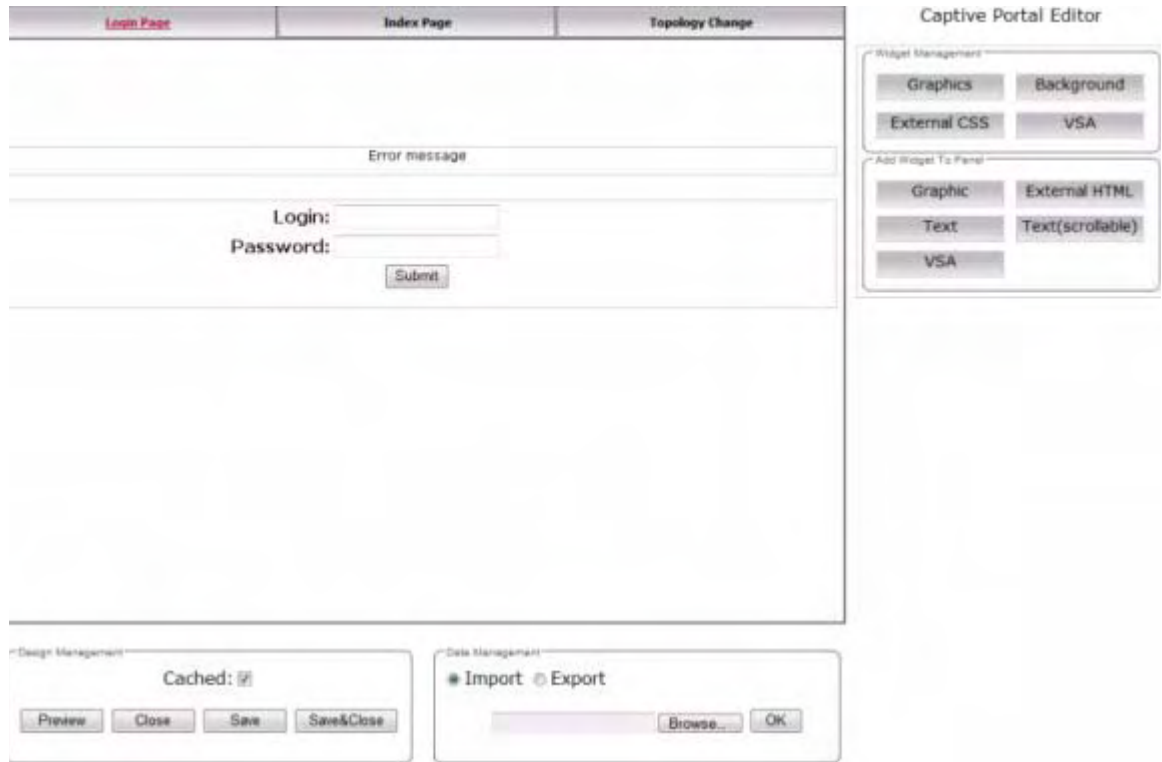


Table 6-8 Captive Portal Editor Fields and Buttons

Field/Button	Description
Login Page tab	<p>Click to view and configure the elements that will display on the Captive Portal login page. By default, widgets for a Login username and Password, as well as an Accept button are configured by default. You can accept or change these widgets using the Captive Portal Editor widget management tools in the right-hand panel.</p> <p>Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can:</p> <ul style="list-style-type: none"> • configure the background colors and forms • add graphics • add an external cascading style sheet (.CSS) • VSA attributes
Index Page Tab	<p>Click to view and configure the elements that will display on the Captive Portal Index page. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can:</p> <ul style="list-style-type: none"> • configure the background colors and forms • add graphics • add a Logoff button. The Logoff button launches a pop-up logoff page, allowing users to control their logoff. • add a Status Check button The Status check button launches a pop-up window, which allows users to monitor session statistics such as system usage and time left in a session. • add an external cascading style sheet (.CSS)

Table 6-8 Captive Portal Editor Fields and Buttons (continued)

Field/Button	Description
Topology Change Tab	<p>Click to view and configure the elements that will display on the Captive Portal Topology change page. By default, a login confirmation and informational message, as well as a Close button, are preconfigured. You can accept or change these elements using the Captive Portal Editor widget management tools in the right-hand panel.</p> <p>Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can:</p> <ul style="list-style-type: none"> • configure the background colors and forms • add graphics • add an external cascading style sheet (.CSS)
Design Management	
Cached	Select to cache most of the widgets from the design to rescue the amount of time it takes a captive portal page to load.
Preview	Select to view the way the configured widgets will display to a user.
Close	Select to close this page without saving the configuration.
Save	Select to save the configuration changes.
Save&Close	Select to save the configuration changes and close this window.
Data Management	
Import	Select and click Browse to navigate to the directory and filename of the a configuration that you want to import. Click OK to import the configuration.
Export	Select to save this configuration and enter the name of the file you want to save it in. Click the Browse button to navigate to a directory where you want to store the configuration file. Click OK. to save the configuration.
Widget Management	
Graphics	Click to locate and upload a graphic. The graphic becomes available in the Show Images section of the Property Editor.
Background	Click to configure the background color of the page
External CSS	Click to identify a cascading style sheet (.CSS) that will determine the page format.
VSA	<p>Click to configure the following VSA attributes:</p> <ul style="list-style-type: none"> • AP Serial • AP Name • VNS Name • SSID • MAC Address <p>The selections influence what URL is returned in either section. For example, wireless users can be identified by which Wireless AP or which VNS they are associated with, and can be presented with a Captive Portal Web page that is customized for those identifiers.</p>

Table 6-8 Captive Portal Editor Fields and Buttons (continued)

Field/Button	Description
Add Widget to Panel	Use the fields in this section to add the configured widgets to the page.
Graphic	Select to add a graphic to the page. Use the Property Editor select a preconfigured graphic, and to determine the size and location of the graphic.
Text	Select to add text to the page. Use the Property Editor to type and format the text, and to determine the location of the text and the conditions under which it displays.
VSA	Select to add a VSA attribute to the page. Use the Property Editor to determine the size and position of the VSA attribute, and the conditions under which it displays, and identify the link and select the type of VSA attribute to include.
External HTML	Select to add an external HTML link to the page. Use the Property Editor select a preconfigured graphic, and to determine the size and location of the graphic
Text (Scrollable)	Select to add scrollable text to the page. Use the Property Editor to type and format the text, and to determine the location of the text and the conditions under which it displays.



Caution: In order for Captive Portal authentication to be successful, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the non-authenticated filter. For more information, see [“Filtering Rules”](#) on page 5-3.



Caution: If you use logos or graphics, ensure that the graphics or logos are appropriately sized. Large graphics or logos may force the login section out of view.

Configuring the QoS Policy

The following is an overview of the steps involved in configuring the QoS for WLAN Services.

Step 1 — Define the QoS Mode for the Service:

- **Legacy** — Enables DL (downlink) classification for all clients
- **WMM:**
 - Enables WMM support
 - Enables DL classification for WMM clients
 - Enables UL (uplink) classification in WMM clients
- **802.11e:**
 - Enables 802.11e support
 - Enables DL classification for 802.11e clients
 - Enables UL classification in 802.11e clients

WMM and 802.11e are similar, but they use different signaling (same as WPA and WPA2).

Step 2 — Enable Turbo Voice:

- Ensures traffic is optimized for voice performance and capacity

- Can be enabled or disabled on individual WLAN Services
 - If Turbo Voice is enabled, together with QoS modes **Legacy**, **WMM**, or **802.11e**, DL voice traffic is sent via Turbo Voice queue instead of voice queue. A separate turbo voice queue allows for some VNSs to use the Turbo Voice parameters for voice traffic, while other VNSs use the voice parameters for voice traffic.
 - If WMM mode is also enabled, WMM clients use Turbo Voice-like contention parameters for UL voice traffic.
 - If 802.11e mode is also enabled, 802.11e clients use Turbo Voice-like contention parameters for UL voice traffic.



Note: The Wireless 802.11n AP does not support the Turbo Voice option.

Step 3 — Define the DSCP and Service Class Classifications:

All 64 DSCP code-points are supported. The IETF defined codes are listed by name and code. Undefined codes are listed by code. The following is the default DSCP service class classification (where SC is Service Class and UP is User Priority):

Table 6-9 DSCP Code-Points

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS0/DE	2/0	AF11	2/0	AF33	4/4
CS1	0/1	AF12	2/0	AF41	5/5
CS2	1/2	AF13	2/0	AF42	5/5
CS3	3/3	AF21	3/3	AF43	5/5
CS4	4/4	AF22	3/3	EF	6/6
CS5	5/5	AF23	3/3	Others	0/1
CS6	6/6	AF31	4/4		
CS7	7/7	AF32	4/4		

Step 4 — If Preferred Instead of DSCP Classification, Enable Priority Override:

- Click the applicable service class and implicitly desired UP
 - Updates UP in user packet
 - Updates UP for WASSP frame (if field exists) sent by AP
- Select the desired DSCP
 - Updates DSCP for WASSP frames sent by AP
 - Does not change DSCP in user packet

Step 5 — Configure the Advanced Wireless QoS:

- Enable the **Unscheduled Automatic Power Save Delivery (U-APSD)** feature
- Works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled

Step 6 — Configure Global Admission Control:

- Enable admission control. Admission control protects admitted traffic against new bandwidth demands. Admission control is available for Voice and Video.
- If admission control is enabled, you can configure the UL and DL policies action.
- The UL and DL policies act as enforcement of a traffic management system. Depending on the TSPEC negotiation per traffic class, Voice and Video, you can configure what actions the Wireless AP takes when admitted traffic has violated its TSPEC.
 - You can configure the UL and DL policers per VNS
 - TSPEC statistics can be viewed in the **Admission Control Statistics by Wireless AP** display. For more information, see [Chapter 15, Working with Reports and Displays](#).

Defining Priority Level and Service Class

Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks are enabling the integration of internet telephony technology on wireless networks. Various issues including Quality-of-Service (QoS), call control, network capacity, and network architecture are factors in VoIP over 802.11 WLANs.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called isochronous data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn to avoid data collisions. Regular traffic on a wireless network is an asynchronous process in which data streams are broken up by random intervals.

To reconcile the needs of isochronous data, mechanisms are added to the network that give voice data traffic or another traffic type priority over all other traffic, and allow for continuous transmission of data.

To provide better network traffic flow, the Enterasys Wireless Convergence Software provides advanced Quality of Service (QoS) management. These management techniques include:

- **WMM (Wi-Fi Multimedia)** — Enabled on individual WLAN Services, is a standard that provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service) or DSCP (Diffserv Codepoint)** — The ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. The IP ToS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header—this is referred to as Adaptive QoS.

Defining the Service Class

Service class is determined by the combination of the following operations:

- The class of treatment given to a packet. For example, queuing or per hop behavior (PHB).
- The packet marking of the output packets (user traffic and/or transport).

Table 6-10 Service classes

Service class name (number)	Priority level
Network Control (7)	7 (highest priority)
Premium (Voice) (6)	6
Platinum (video) (5)	5

Table 6-10 Service classes

Service class name (number)	Priority level
Gold (4)	4
Silver (3)	3
Bronze (2)	2
Best Effort (1)	1
Background (0)	0 (lowest priority)

The service class is equivalent to the 802.1D UP (user priority).

Table 6-11 Relationship between service class and 802.1D UP

SC name	SC Value	802.1d UP	AC	Queue
Network Control	7	7	VO	VO or TVO
Premium (voice)	6	6	VO	VO or TVO
Platinum (video)	5	5	VI	VI
Gold	4	4	VI	VI
Silver	3	3	BE	BE
Bronze	2	0	BE	BE
Best Effort	1	2	BK	BK
Background	0	1	BK	BK

Configuring the Priority Override

Priority override allows you to define and force the traffic to a desired priority level. Priority override can be used with any combination, as displayed in [Table 6-11](#). You can configure the service class and the DSCP values.

When **Priority Override** is enabled, the configured service class overrides the queue selection in the downlink and uplink direction, the 802.1P UP for the VLAN tagged Ethernet packets, and the UP for the wireless QoS packets (WMM or 802.11e) according to the mapping in [Table 6-10](#). If **Priority Override** is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

QoS Modes

You can enable the following QoS modes for a WLAN Service:

- **Legacy** — If enabled, the AP will classify and prioritize the downlink traffic for all clients according to the same rules.
- **WMM** — If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.

- **802.11e** — If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic.
- **Turbo Voice** — If any of the above QoS modes are enabled, the Turbo Voice mode is available. If enabled, all the downlink traffic that is classified to the Voice (VO) AC and belongs to that VNS is transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. The TVO queue is tailored in terms of contention parameters and number of retries to maximize voice quality and voice capacity.

All combinations of the three modes are valid. The following table summarizes all possible combinations:

Table 6-12 QoS mode combinations

Configuration	Legacy mode	x		x		x		x
	WMM mode		x	x			x	x
	802.11e mode				x	x	x	x
Traffic that is classified and prioritized	To legacy client	x		x		x		x
	From legacy client							
	To WMM client	x	x	x		x	x	x
	From WMM client		x	x			x	x
	To 802.11e client	x		x	x	x	x	x
	From 802.11e client				x	x	x	x

The APs are capable of supporting 5 queues. The queues are implemented per radio. For example, 5 queues per radio. The queues are:

Table 6-13 Queues

Queue Name	Purpose
AC_VO	Voice
AC_VI	Video
AC_BK	Background
AC_BE	Best Effort
AC_TVO	Turbo Voice

The Enterasys Wireless Controller supports the definition of 8 levels of user priority (UP). These priority levels are mapped at the AP to the best appropriate access class. Of the 8 levels of user priority, 6 are considered low priority levels and 2 are considered high priority levels.

WMM clients have the same 4 AC queues. WMM clients will classify the traffic and use these queues when they are associated with a WMM-enabled AP. WMM clients will behave like non-WMM clients—map all traffic to the Best Effort (BE) queue—when not associated with WMM-enabled AP.

The prioritization of the traffic on the downstream (for example, from wired to wireless) and on the upstream (for example, from wireless to wired) is dictated by the configuration of the WLAN Service and the QoS tagging within the packets, as set by the wireless devices and the host devices on the wired network.

Both Layer 3 tagging (DSCP) and Layer 2 (802.1d) tagging are supported, and the mapping conforms with the WMM specification. If both L2 and L3 priority tags are available, then both are

taken into account and the chosen AC is the highest resulting from L2. If only one of the priority tags is present, it is used to select the queue. If none is present, the default queue AC_BE is chosen.



Note: If the wireless packets to be transmitted must include the L2 priority (send to a WMM client from a WMM-enabled AP), the outbound L2 priority is copied from the inbound L2 priority if available, or it is inferred from the L3 priority using the above table if the L2 inbound priority is missing.

Table 6-14 Traffic Prioritization

VNS type	Packet Source	Packet type	L2	L3
Tunneled	Wired	Untagged	No	Yes
Branch	Wired	VLAN tagged	Yes	Yes
Branch	Wired	Untagged	No	Yes
Branch or Tunneled	Wireless	WMM	Yes	Yes
Branch or Tunneled	Wireless	non-WMM	No	Yes

To Configure QoS Policy:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
3. Click the **QoS** tab.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes 'Home | Logs | Reports | Wireless Controller | Wireless APs | VNS Configuration | Mibgator | Help | LOGOUT'. The main content area is titled 'WLAN: lab10-gp' and has four tabs: 'WLAN Services', 'Privacy', 'Auth & Acct', and 'QoS'. The 'QoS' tab is active, showing the 'Wireless QoS' section with the following options:

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

 Below this is the 'Admission Control' section:

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

 A note states: '* Global admission controls are configured through Global Settings'. On the right side of the QoS configuration, there is a checkbox for 'Flexible Client Access' which is checked. At the bottom of the configuration area, there are 'New', 'Delete', and 'Save' buttons. The left sidebar shows a tree view with 'WLAN Services' expanded and 'lab10-gp' selected.

4. From the **Wireless QoS** list, do the following:
 - **Legacy** — Select if your service will support legacy devices.

- **WMM** — Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all WMM clients. Note that WMM clients will also classify and prioritize the uplink traffic. WMM is part of the 802.11e standard for QoS. If selected, the **Turbo Voice** and **Enable U-APSD** options are displayed.
 - **802.11e** — Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic. If selected, the **Turbo Voice** and the **Enable U-APSD** options are displayed:
 - **Turbo Voice** — Select to enable all downlink traffic that is classified to the Voice (VO) AC and belongs to that VNS to be transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. When **Turbo Voice** is enabled together with **WMM** or **802.11e**, the WMM and/or 802.11e clients in that VNS are instructed by the AP to transmit all traffic classified to VO AC with special contention parameters tailored to maximize voice performance and capacity.
 - **Enable U-APSD** — Select to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature. This feature can be used by mobile devices to efficiently sustain one or more real-time streams while being in power-save mode. This feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.
5. From the **Admission Control** list, do the following:
- **Use Global Admission Control for Voice (VO)** - Select to enable admission control for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands. For more information, see [VNS Global Settings](#).
 - **Use Global Admission Control for Video (VI)** - This feature is only available if admission control is enabled for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands. Select to provide distinct thresholds for VI (video). For more information, see [VNS Global Settings](#).
6. To configure advanced QoS policy settings, click **Advanced**. The Advanced dialog is displayed.



7. To force a service class and DSCP marking, select the **Priority Override** checkbox. For the Service Class selection, you can click one of the eight service classes.
 - **Service class** – From the drop-down list, click the appropriate priority level:
 - Network control (7) – The highest priority level.
 - Premium (Voice) (6)
 - Platinum (5)
 - Gold (4)
 - Silver (3)
 - Bronze (2)
 - Best Effort (1)
 - Background (0) – The lowest priority level
 - **DSCP marking** – From the drop-down list, click the DSCP value used to tag the IP header of the encapsulated packets.

When **Priority Override** is enabled, the configured service class forces queue selection in the downlink direction, the 802.1P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority. If **Priority Override** is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

8. If you want to assign a service class to each DSCP marking, clear the **Priority Override** checkbox and define the DSCP service class priorities in the DSCP classification table.
9. The **Advanced Wireless QoS** options are only displayed if the WMM or 802.11e checkboxes are selected:
 - **UL Policer Action** – If **Use Global Admission Control for Voice (VO)** or **Use Global Admission Control for Video (VI)** is enabled, click the action you want the Wireless AP to take when TSPEC violations occurring on the uplink direction are discovered:
 - **Do nothing** – Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.
 - **Send DELTS to Client** – Click to end TSPEC violations when it they are discovered. This action deletes the TSPEC.
 - **DL Policer Action** – If **Use Global Admission Control for Voice (VO)** or **Use Global Admission Control for Video (VI)** is enabled, click the action you want the Wireless AP to take when TSPEC violations occurring on the downlink direction are discovered:
 - **Do nothing** – Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.
 - **Downgrade** – Click to force the transmission's data packets to be downgraded to the next priority when a TSPEC violation is discovered.
 - **Drop** – Click to force the transmission's data packets to be dropped when a TSPEC violation is discovered.
10. Close the Advanced window.
11. Check the **Use Flexible Client Access** checkbox to enable flexible client access. Flexible client access levels are set as part of the VNS global settings.



Note: TSPEC must be disabled when using Flexible Client Access.

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

Configuring a VNS

This chapter describes VNS (Virtual Network Services) configuration, including:

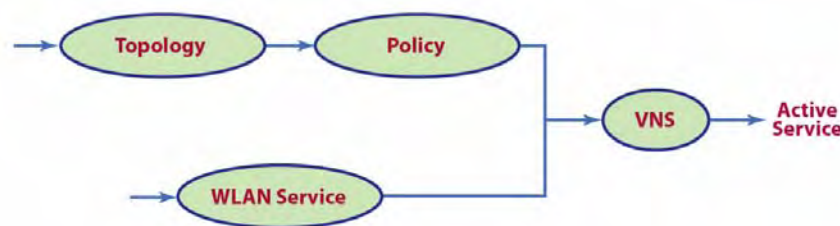
For information about...	Refer to page...
High Level VNS Configuration Flow	7-1
VNS Global Settings	7-3
Methods for Configuring a VNS	7-17
Manually Creating a VNS	7-18
Creating a VNS Using the Wizard	7-19
Enabling and Disabling a VNS	7-47
Renaming a VNS	7-48
Deleting a VNS	7-48

High Level VNS Configuration Flow

Setting up a VNS defines a binding between a default policy specified for wireless users and an associated WLAN Service set, as shown in [Figure 7-1](#) below.

There are conceptually hierarchical dependencies on the configuration elements of a VNS. However, the provisioning framework is flexible enough that you may select an existing dependent element or create one on the fly. Therefore, each element can be provisioned independently (WLAN services, Topologies, and Policies). For service activation, all the pieces will need to be in place, or defined during VNS configuration.

Figure 7-1 VNS Configuration Flow



You can use the **VNS Creation Wizard** to guide you through the necessary steps to create a virtual network service (and the necessary subcomponents during the process). The end result is a fully resolved set of elements and an active service.

The recommended order of configuration events is:

1. Before you begin, draft out the type of services the system is expected to provide — wireless services, encryption types, infrastructure mapping (VLANs), and connectivity points (switch ports). Switch port VLAN configuration/trunks must match the controller's.
2. Set up basic controller services such as NTP, Routing, DNS, and RADIUS Servers, using one of the following methods:
 - Run the **Basic Configuration Wizard**, or
 - Manually define the necessary infrastructure components such as RADIUS Servers. RADIUS Servers are defined via the VNS Configuration > Global > Authentication tab.
3. Define Topologies. Topologies represent the controller's points of network attachment. Therefore, VLANs and port assignments need to be coordinated with the corresponding switch ports.
4. Define Policies. Policies are typically bound to Topologies. Policy application assigns user traffic to the corresponding network point of attachment.
 - Policies define mobile user access rights by filtering.
 - Policies reference the mobile user's traffic rate control profiles.
5. Define the WLAN Service.
 - Define SSID and privacy settings for the wireless link.
 - Select the set of APs and Radios on which the service is present.
 - Configure the method of credential authentication for wireless users (None, Internal CP, External CP, GuestPortal, 802.1x[EAP]).
6. Create a **VNS** that binds the **WLAN Service** to the **Policy** that will be used for default assignment upon user network attachment.

The VNS configuration page in turn allows for in-place creation of any dependencies it may require. For example:

- Create a new WLAN Service.
- Create a new Policy.
 - Create a new Topology.
 - Create a new Class of Service.

Controller Defaults

The default shipping Enterasys Wireless Controller configuration does not include any pre-configured WLAN Services, VNSs, or Policies.

The Enterasys Wireless Controller system does ship with Topology entities representing each of its physical interfaces, plus an admin interface.

There are, however, global default settings corresponding to:

- A Default Topology named "Bridged @ AP Untagged"
- An "Unlimited" Rate Control Profile
- A Filter Definition of "Deny all"

These entities are simply placeholders for Policy completion, in case policies are incompletely defined. For example, a Policy may be defined as "no-change" for Topology assignment.

If an incomplete Policy is assigned as the default for a VNS / WLAN Service (wireless port), the incomplete Policy needs to be fully qualified, at which point the missing values are picked from the Default Global Policy definitions, and the resulting policy is applied as default.



Note: You can edit the attributes of the Default Global Policy (in the VNS > Globals tab) to any other parameters of your choosing (for example, any other topology, more permissive filter sets, more restrictive Rate Control profile).

It is possible to define a Default Global Policy to refer to a specific Topology (for example, Topology_VLAN), and then configure every other Policy's topology simply as "No-change." This will cause the default assignment to Topology_VLAN, so that all user traffic, regardless of which policy they're currently using (with different access rights, different rate controls) will be carried through the same VLAN.

VNS Global Settings

Before defining a specific VNS, define the global settings that will apply to all VNS definitions. These global settings include:

- Authentication
 - Configuring RADIUS servers on the enterprise network. The defined servers are displayed as available choices when you set up the authentication mechanism for each WLAN Service.
 - Configuring the MAC format.
- DAS (Dynamic Authorization Service)
 - Configuring Dynamic Authorization Service (DAS) support. DAS helps secure your network by providing the ability to disconnect a mobile device from your network.
- Wireless QoS, comprising Admission Control Thresholds and Flexible Client Access Fairness Policy.
 - Admission control thresholds protect admitted traffic against overloads, provide distinct thresholds for VO (voice) and VI (video), and distinct thresholds for roaming and new streams.
 - Flexible Client Access provides the ability to adjust media access fairness in five levels between Packet Fairness and Airtime Fairness.
- Bandwidth Control
 - The Bandwidth Control Profiles you define are displayed as available choices in the **Rate Profiles** menu when you set up CoS policy.
- Default Policy

The Global Default Policy specifies:

- A topology to use when a VNS is created using a policy that does not specify a topology
- A set of filters

The Enterasys Wireless Controller ships from the factory with a default "Global Default Policy" that has the following settings:

- Topology is set to an Bridged at AP untagged topology. This topology will itself be defined in Enterasys Wireless Controllers by default.
- Filters - A single "Allow All" filter.

The Global Default Policy is user-configurable. Changes to the Global Default Policy immediately effect all shadow policies created from it, just as if the administrator had made a comparable change directly to the incomplete policy.

- Egress Filtering Mode

The global egress filtering mode setting overrides the individual WLAN service egress filter mode setting.

- Sync Summary

The “Sync Summary” screen provides an overview of the synchronization status of paired controllers. The screen is divided into 4 sections: Virtual Networks, WLAN services, Policies and Topologies. Each section lists the name of the corresponding configuration object, its synchronization mode, and the status of last synchronization attempt. For more information, see “[Using the Sync Summary](#)” on page 7-16.

Defining RADIUS Servers and MAC Address Format

The Authentication global settings include configuring RADIUS servers, the MAC format to be used, the SERVICE-TYPE attribute in the client ACCESS-REQUEST messages, and how long a notice Web page displays if a topology change occurs during authentication. The notice Web page indicates that authentication was successful and that the user must restart the browser to gain access to the network.

Defining RADIUS Servers for VNS Global Settings

To Define RADIUS Servers for VNS Global Settings:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then **Authentication**.

- To enable changing RADIUS server settings per WLAN Service, select **Strict Mode**.

The screenshot shows the Enterasys Virtual Network Configuration interface. The left sidebar contains a navigation menu with options: New..., Global, Authentication, DAS, Wireless QoS, Bandwidth Control, and Default Policy. Below this are sections for Virtual Networks, WLAN Services, Policies, Classes of Service, and Topologies. The main content area is titled "RADIUS Servers" and includes a checkbox for "Strict Mode". Below this is a table of RADIUS servers:

	Server		Default		Retries		Timeouts		Ports		Priority	
	Alias	Hostname/IP	Protocol	Auth	Acct	Auth	Acct	Auth	Acct	Auth	Acct	
<input type="checkbox"/>	test1	2.2.2.2	PAP	3	3	5	5	1812	1813	12	12	
<input type="checkbox"/>	test2	2.2.2.3	PAP	3	3	5	5	1812	1813	2	2	
<input type="checkbox"/>	test3	3.3.3.3	PAP	3	3	5	5	1812	1813	3	3	
<input type="checkbox"/>	test5	5.5.5.5	PAP	3	3	5	5	1812	1813	4	4	

Below the table, there is a note: "RADIUS servers which are currently associated with WLAN Service(s) cannot be removed". There are "New" and "Delete Selected" buttons. The "MAC Address" section has a "MAC Address Format" dropdown set to "XXXXXXXXXXXX" and an "Advanced..." button. A "Save" button is at the bottom right.

- To define a new RADIUS server available on the network, click the **New** button. The **RADIUS Settings** pop up window displays.

The screenshot shows the "RADIUS Settings" dialog box. It is titled "RADIUS Server" and contains the following fields:

- Server Alias: [text input]
- Hostname IP: [text input]
- Shared Secret: [text input] with an "Unmask" button
- Default Protocol: PAP (dropdown)

There are two sections for configuration:

- Authentication:**
 - Priority: 7
 - Total Number of Tries: 3
 - RADIUS Request Timeout: 5 (seconds)
 - Port: 1812
- Accounting:**
 - Priority: 7
 - Total Number of Tries: 3
 - RADIUS Request Timeout: 5 (seconds)
 - Interim Accounting Interval: 30 (minutes)
 - Port: 1813

At the bottom, there are "Save" and "Cancel" buttons.

5. In the **Server Alias** box, type a name that you want to assign to the RADIUS server.



Note: You can also type the RADIUS server's IP address in the **Server Alias** box in place of a nickname. The RADIUS server will identify itself by the value typed in the **Server Alias** box in the **RADIUS Servers** drop down list on the **RADIUS Authentication** tab of the **Login Management** screen (**top menu > Wireless Controller > Login Management**). For more information, see "[Configuring the Login Authentication Mode](#)" on page 2-35.

6. In the **Hostname/IP** box, type either the RADIUS server's FQDN (fully qualified domain name) or IP address.



Note: If you type the host name in the **Hostname/IP address** box, the Enterasys Wireless Controller will send a host name query to the DNS server for host name resolution. The DNS servers must be appropriately configured for resolving the RADIUS servers' host names. For more information, see "[Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers](#)" on page 2-52.

7. In the **Shared Secret** box, type the password that will be used to validate the connection between the Enterasys Wireless Controller and the RADIUS server.

To proofread your shared secret key, click **Unmask**. The password is displayed.



Note: You should always proofread your **Shared Secret** key to avoid any problems later when the Enterasys Wireless Controller attempts to communicate with the RADIUS server.

8. If desired, change the **Default Protocol** using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
9. If desired, change the pre-defined default values for **Authentication** and **Accounting** operations:
 - a. Priority — default is 4
 - b. Total number of tries — default is 3
 - c. RADIUS Request timeout — default is 5 seconds
 - d. Port — default Authentication port is 1812. Default Accounting port is 1813.
 - e. For Accounting operations, the Interim Accounting Interval — default is 30 minutes.

10. To save your changes, click **Save**. The new server is displayed in the **RADIUS Servers** list.

enterasys
Secure Networks™ There's nothing more important than our customers.

Virtual Network Configuration

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

New...

Global

Authentication

DAS
Wireless QoS
Bandwidth Control
Default Policy

Virtual Networks

WLAN Services

Policies

Classes of Service

Topologies

RADIUS Servers

Strict Mode

	Server		Default		Retries		Timeouts		Ports		Priority	
	Alias	Hostname/IP	Protocol	Auth	Acct	Auth	Acct	Auth	Acct	Auth	Acct	
<input type="checkbox"/>	test1	2.2.2.2	PAP	3	3	5	5	1812	1813	12	12	
<input type="checkbox"/>	test2	2.2.2.3	PAP	3	3	5	5	1812	1813	2	2	
<input type="checkbox"/>	test3	3.3.3.3	PAP	3	3	5	5	1812	1813	3	3	
<input type="checkbox"/>	test5	5.5.5.5	PAP	3	3	5	5	1812	1813	4	4	

* RADIUS servers which are currently associated with WLAN Service(s) cannot be removed

MAC Address

MAC Address Format: XXXXXXXXXXXX



Note: The RADIUS server is identified by its **Server Alias**.

11. To edit an existing server, click the row containing the server. The RADIUS Settings window displays, containing the server's configuration values.
12. To remove a server from the list, select the checkbox next to the server, and then click **Delete Selected**. You cannot remove a server that is used by any VNS.

Configuring the Global MAC Address Format for Use with the RADIUS Servers

To Configure the Global MAC Address Format for Use with the RADIUS Servers:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then **Authentication**.
3. In the **MAC Address** area, select the **MAC Address Format** from the drop down list.
4. Click **Save** to save your changes.

Including the **SERVICE-TYPE** Attribute in the Client **ACCESS-REQUEST** Messages

To Include the **SERVICE-TYPE** Attribute in the Client **ACCESS-REQUEST** Messages:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then **Authentication**.
3. In the **MAC Address** area, click **Advanced**.
4. Select **Include Service-Type attribute in Client Access Request messages**.
5. Click **Close**.
6. Click **Save** to save your changes.

Changing the Display Time of the Notice Web Page

To Change How Long the Notice Web Page Displays If a Topology Change Occurs During Authentication:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then **Authentication**.
3. In the **MAC Address** area, click **Advanced**.
4. In the **Delay for Client Message for Topology Change** field, specify how long, in seconds, the Web page is displayed to the client when the topology changes as a result of a policy change.

The Web page indicates that authentication was successful and that the user must close all browser windows and then restart the browser for access to the network.

Currently this is supported for Internal Captive Portal, Guest Portal, and Guest Splash.

5. Click **Close**.
6. Click **Save** to save your changes.

Configuring Dynamic Authorization Server Support

DAS helps secure your network by forcing the disconnection of any mobile device from your network. Typically, you would want to disconnect any unwelcome or unauthorized mobile device from your network. The “disconnect message” that is defined in RFC 3576 is enforced by the DAS support. If an unauthorized mobile device is detected on the network, the DAS client sends a disconnect packet, forcing the mobile device off the network. Your DAS client can be an integration with NAC or another third-party application, including RADIUS applications. For more information, see [“NAC integration with Enterasys Wireless WLAN”](#) on page 1-12.

DAS support is available to all physical interfaces of the Enterasys Wireless Controller, and by default DAS listens to the standard-specified UDP port 3799.

To Configure Dynamic Authorization Server Support:

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

- In the left pane, click **Global**, then click **DAS**.

The screenshot shows the 'enterasys' logo at the top left with the tagline 'Secure Networks. There's nothing more important than our customers.' The page title is 'Virtual Network Configuration'. The navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration' (highlighted), and 'Mitigator'. The left sidebar has a 'New...' section with 'Global' selected, and sub-items: 'Authentication', 'DAS' (highlighted), 'Wireless QoS', 'Bandwidth Control', 'Default Policy', 'Egress Filtering Mode', and 'Sync Summary'. Below this are sections for 'Virtual Networks', 'WLAN Services', 'Policies', 'Classes of Service', and 'Topologies'. The main content area is titled 'Dynamic Authorization Server Configuration' and contains two input fields: 'Port: 3799' and 'Replay Interval: 300 seconds'. A 'Save' button is located at the bottom right of the main area.

- In the **Port** box, type the UDP port you want DAS to monitor. By default, DAS is configured for the standard-specified UDP port 3799. It is unlikely this port value needs to be revised.
- In the **Replay Interval** box, type how long you want DAS to ignore repeated identical messages. By default, DAS is configured for 300 seconds.
This time buffer helps defend against replay network attacks.
- To save your changes, click **Save**.

Defining Wireless QoS Admission Control Thresholds

Defining the wireless QoS global settings include the following:

- [Configuring QoS Admission Control Thresholds](#)
- [Configuring QoS Flexible Client Access](#)

Configuring QoS Admission Control Thresholds

To Define Admission Control Thresholds for VNS Global Settings:

- From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.

- In the left pane, click **Global**, then click **Wireless QoS**.

The screenshot shows the Enterasys Virtual Network Configuration web interface. The left navigation pane is expanded to show 'Global' and 'Wireless QoS'. The main content area is titled 'Admission Control Thresholds' and contains four dropdown menus for bandwidth settings:

- Max Voice (VO) BW for roaming streams: 80%
- Max Voice (VO) BW for new streams: 60%
- Max Video (VI) BW for roaming streams: 60%
- Max Video (VI) BW for new streams: 40%

A note below these settings states: "Settings only apply on APs serving QoS-enabled WLAN Service with Admission Control enabled". Below this is the 'Flexible Client Access' section, which includes a 'Fairness Policy' dropdown menu set to '100% Packet'. A 'Save' button is located at the bottom right of the configuration area.

- In the **Admission Control Thresholds** area, define the thresholds for the following:
 - Max Voice (VO) BW for roaming streams** — The maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.
 - Max Voice (VO) BW for new streams** — The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.
 - Max Video (VI) BW for roaming streams** — The maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.
 - Max Video (VI) BW for new streams** — The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.

These global QoS settings apply to all APs that serve QoS enabled VNSs with admission control.

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

Configuring QoS Flexible Client Access

This feature allows you to adjust client access policy in multiple steps between “packet fairness” and “airtime fairness.”

- Packet fairness is the default 802.11 access policy. Each WLAN participant gets the same (equal) opportunity to send packets. All WLAN clients will show the same throughput, regardless of their PHY rate.
- Airtime fairness gives each WLAN participant the same (equal) time access. WLAN clients’ throughput will be proportional to their PHY rate.

To Define Flexible Client Access for VNS Global Settings:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then click **Wireless QoS**.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. The left sidebar shows a tree view with 'Global' selected, and sub-items: Authentication, DAS, Wireless QoS (highlighted), Bandwidth Control, Default Policy, Egress Filtering Mode, and Sync Summary. Below this are sections for Virtual Networks, WLAN Services, Policies, Classes of Service, and Topologies. The main content area is titled 'Admission Control Thresholds' and contains four dropdown menus: Max Voice (VO) BW for roaming streams (80%), Max Voice (VO) BW for new streams (60%), Max Video (VI) BW for roaming streams (60%), and Max Video (VI) BW for new streams (40%). A note below states: 'Settings only apply on APs serving QoS-enabled WLAN Service with Admission Control enabled'. Below this is the 'Flexible Client Access' section with a 'Fairness Policy' dropdown menu set to '100% Packet'. A 'Save' button is located at the bottom right of the main content area.

3. In the **Flexible Client Access** area, select a policy from the **Fairness Policy** drop-down list. Choices range from 100% packet fairness to 100% airtime fairness.



Note: TSPEC must be disabled when using Flexible Client Access.

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

Working with Bandwidth Control Profiles

Bandwidth control limits the amount of bidirectional traffic from a mobile device. A bandwidth control profile provides a generic definition for the limit applied to certain wireless clients' traffic. A bandwidth control profile is assigned on a per policy basis. A bandwidth control profile is not applied to multicast traffic.

A bandwidth control profile consists of the following parameters:

- **Profile Name** — Name assigned to a profile
- **Committed Information Rate (CIR)** — Rate at which the network supports data transfer under normal operations. It is measured in kilo bytes per second (Kbps).

The bandwidth control profiles you define on the **VNS Global Settings** screen are displayed as available choices in the **Bandwidth Control Profiles** list on the **Classes of Service** screen.

To create a bandwidth control profile:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then click **Bandwidth Control**.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes the Enterasys logo, the tagline "Secure Networks. There's nothing more important than our customers.", and the title "Virtual Network Configuration". Below the navigation bar are links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. A Help and LOGOUT link is also present.

The left sidebar contains a "New..." section with a red header, listing various configuration options: Global (highlighted), Authentication, DAS, Wireless QoS, Bandwidth Control (highlighted), Default Policy, Egress Filtering Mode, and Sync Summary. Below this are sections for Virtual Networks, WLAN Services, Policies, Classes of Service, and Topologies.

The main content area is titled "Bandwidth Control Profiles". It features a list of profiles on the left: "e3" (highlighted), "rate1", and "Unlimited". To the right of the list are input fields for "Profile Name" (containing "e3") and "Average Rate (CIR)" (containing "166" Kbps). A "Save Profile" button is located below these fields. At the bottom of the list area are buttons for "Remove selected profile" and "Add new profile". A "Save" button is located at the bottom right of the main content area.

3. Create a bandwidth control profile by doing the following:
 - **Profile Name** — Type a name for the bandwidth control profile.
 - In the **Average Rate (CIR)** — Type the CIR value for the bandwidth control profile.
4. Click **Add Profile**. The profile is created and displayed in the **Bandwidth Control Profiles** list.
5. Create additional bandwidth control profiles, if applicable.
6. To save your changes, click **Save**.

Configuring the Global Default Policy

The Enterasys Wireless Controller ships with a Global Default Policy that can be configured. The Global Default Policy specifies:

- A topology to use when a VNS is created using a policy that does not specify a topology. The default assigned topology is named Bridged at AP untagged.
- A set of filters

Configuring the Topology and Rate Profiles

To Configure the Topology and Rate Profiles:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, click **Global**, then click **Default Policy**.
3. Select the **VLAN & Class of Service** tab.

4. In the **Topology** area, select a topology using one of the following methods:
 - Select an existing topology from the **Assigned Topology** drop-down list.
 - Select an existing topology from the **Assigned Topology** drop-down list, then click **Edit**. The **Edit Topology** window displays, showing the current values for the selected topology.
 - Click the **New** button. The **New Topology** window displays.

Edit or create the selected topology as described in “[Configuring a Basic Topology](#)” on page 4-2.

Configuring the Filters

To Configure the Filters:

1. Click the **Filter Rules** tab. The **HWC Filters** tab displays, allowing you to create filter rules that will be applied by the controller when default non-authentication policy does not specify filters.

The screenshot shows the Enterasys Virtual Network Configuration interface. The main content area is titled 'Policy: Global Default Policy' and is divided into two tabs: 'VLAN & Class of Service' and 'Filter Rules'. The 'Filter Rules' tab is active, showing a table of filter rules. The table has columns for Rule, In, Out, IP : Port, Protocol, Priority, ToS/DSCP, Access, and CoS. There are two rules listed, both with 'D' in the Rule column and 'Allow' in the Access column. Below the table are buttons for 'Add', 'Edit', 'Delete', 'Up', and 'Down'. A legend at the bottom of the table indicates: 'T: local interface, U: user defined, D:default, Rules with Allow unchecked are denied.'

Rule	In	Out	IP : Port	Protocol	Priority	ToS/DSCP	Access	CoS
D	dest	none	0.0.0.0/0	N/A	N/A	N/A	Allow	N/A
D	none	src	0.0.0.0/0	N/A	N/A	N/A	Allow	N/A

2. To add a rule, click **Add**. The fields in the Add Filter area are enabled.
 3. Configure the fields as desired. For more information, see [“Filtering Rules”](#) on page 5-3.
 4. To configure custom AP filters, select the **AP Filtering** checkbox, then select the **Custom AP Filters** checkbox and click the **AP Filters** tab. Then configure the rules as desired.
- For more information, see [“Defining Filter Rules for Wireless APs”](#) on page 5-6.

Configuring Egress Filtering Mode

The Enterasys Wireless Controller can be configured to support Policy Manager’s Egress Policy mode. Egress Policy refers to taking the ingress filters assigned to a port, exchanging the source and destination addresses with each other in each policy rule and applying the result to the traffic egressing the port.

Enterasys Wireless Convergence Software applies egress filtering mode to WLAN services. When egress filtering is enabled, any policy that is applied to a station on the WLAN service will have its outbound filters replaced with rules in which the source and destination addresses of the inbound filters are swapped.

The same policy can be assigned to stations on WLAN services that have egress filtering mode enabled and on WLAN services that have it disabled.

- For stations that are on WLAN services with egress filtering mode enabled, the policies outbound filters will be replaced by ones derived from the inbound filter rules.

- For stations that are on WLAN services with egress filtering disabled, the outbound filters of the policy will be applied as defined. In other words the same policy can be applied in two different ways at the same time, based on the egress filter mode settings of the WLAN services it is used with.

The global egress filtering mode setting overrides the individual WLAN service egress filter mode setting. By default the global egress filtering mode is set to Use WLAN setting. In this mode, egress filtering can be enabled for some WLAN services and not others, by using the Egress Filtering Mode setting available in each WLAN service's Advanced configuration dialog.

Changing the global egress filtering mode doesn't alter each individual WLAN service's own egress filtering mode setting, although it can override them. Changing the global egress filtering mode doesn't alter the outbound filter rules of each policy. Each policy's filter rules are stored on the controller as they were entered. Changing the global egress filtering mode flag will affect how a policy's filter rules are interpreted when they are applied.

Configuring the In/Out Rules for WLAN Services Settings

To Configure the Egress Filtering Mode:

- From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
- In the left pane, click **Global**, then **Egress Filtering Mode**. The **Egress Filtering Mode Configuration** screen displays.

The screenshot shows the Enterasys Virtual Network Configuration interface. The top navigation bar includes the Enterasys logo, the tagline "Secure Networks. There's nothing more important than our customers.", and the title "Virtual Network Configuration". The navigation menu includes Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), Mitigator, Help, and LOGOUT. The left sidebar shows a tree view with "Global" selected, containing sub-items: Authentication, DAS, Wireless QoS, Bandwidth Control, Default Policy, Egress Filtering Mode (highlighted), and Sync Summary. Below the sidebar are sections for Virtual Networks, WLAN Services, Policies, Classes of Service, and Topologies. The main content area is titled "Egress Filtering Mode Configuration" and contains three radio button options:

- All WLAN Services enforce explicitly defined "Out" rules
- All WLAN Services apply "In" filter rules to "Out" direction traffic *
- Use WLAN Service setting

 A red note at the bottom of the main area states: "* When 'In' filter rules are applied to 'Out' traffic, the role of the source and destination address are reversed". A "Save" button is located at the bottom right of the configuration area.

- In the Egress Filtering Mode Configuration area select an egress filtering mode:
 - When egress filtering mode is set to **All WLAN Services enforce explicitly defined "Out" rules**, all WLAN services will enforce outbound filters on egress traffic, exactly as they are defined in the policy.

- When egress filtering mode is set to **All WLAN Services apply “In” filter rules to “Out” direction traffic**, all WLAN services will enforce that any outbound filter rules explicitly defined in the policy are overridden by a set of rules created by copying each inbound filter rule and swapping the source and destination address roles in the rule.
- When egress filtering mode is set to **Use WLAN Service setting**, each policy’s filter rules will be interpreted in accordance with the **Egress Filtering Mode** setting of each WLAN Service on which the policy is applied. In this mode, it is possible that a policy’s filter rules can be interpreted in two different ways at the same time, if it is used simultaneously on a WLAN service that has **Enforce explicitly defined “Out” rules** enabled and on a WLAN service that has **Apply “In” rules to “Out” direction traffic** at the same time.



Note: It is recommended that this setting be left at **Use WLAN Service setting**. If you are using Policy Manager, configure each WLAN Service’s Egress filtering option directly from Policy Manager. Enabling Egress Filtering on a WLAN Service port in Policy Manager is equivalent to setting **Apply “In” rules to “Out” direction traffic** in the WLAN Service’s Advanced dialog.

Using the Sync Summary

The Sync Summary screen provides an overview of the synchronization status of paired controllers. The screen is divided into five sections: Virtual Networks, WLAN services, Policies, Classes of Service, and Topologies. Each section lists the name of the corresponding configuration object, its synchronization mode, and the status of last synchronization attempt.

If Synchronization of an object is not enabled, then there is a button in the Status field which says “Synchronize Now”, which performs a single synchronization of the object, pushing the object from local controller to the peer.

If Synchronization of an object is enabled, then the “Status” field can have the following values:

- Synchronized
- Not Synchronized
- Failed
- Conflict (with a button called “Resolve”)

The checkbox “Synchronize System Configuration” acts as a global synchronization flag. When it's disabled, synchronization is not performed in the background. When it is enabled, only the objects that have “Sync” enabled are synchronized.

An object may have a synchronization state of “Conflict” if it was updated on both controllers in the availability pair while the availability link was down. In such a case, the “Resolve” button lets you choose which version of the object should be taken, local or remote. Please note that controllers don't compare the actual configuration when they declare a conflict — only the fact that the object was updated on both controllers in the availability pair triggers the “Conflict” state.

Methods for Configuring a VNS

To configure a VNS, you can use one of the following methods:

- **Manual configuration** — Allows you to create a new VNS by first configuring the topology, policy, and WLAN services and then configuring any remaining individual VNS tabs that are necessary to complete the process.

When configuring a VNS, you can navigate between the various VNS tabs and define your configuration without having to save your changes on each individual tab. After your VNS configuration is complete, click **Save** on any VNS tab to save your completed VNS configuration.



Note: If you navigate away from the VNS configuration tabs without saving your VNS changes, your VNS configuration changes will be lost.

- **Wizard configuration** — The VNS wizard helps create and configure a new VNS by prompting you for a minimum amount of configuration information. The VNS is created using minimum parameters. The remaining parameters are automatically assigned in accordance with best practice standards.

DRAFT

After the VNS wizard completes the VNS creation process, you can then edit or revise any of the VNS configuration to suit your network needs.

Manually Creating a VNS

Advanced configuration allows administrators to create a new VNS once the topology, policy, and WLAN services required by the VNS parameters are available. The topology, policy and WLAN services could be created in advance or could be created at the time of VNS configuration.

When you create a new VNS, additional tabs are displayed depending on the selections made in the Core box of the main VNS configuration tab.

When configuring a VNS, you can navigate between the various VNS tabs and define your configuration without having to save your changes on each individual tab. After your VNS configuration is complete, click **Save** on any VNS tab to save your complete VNS configuration.



Note: If you navigate away from the VNS Configuration tabs without saving your VNS changes, your VNS configuration changes will be lost.

The following procedure lists the steps necessary to create a VNS in advanced mode. Each step references a section in this document that describes the full details. Follow the links provided to go directly to the appropriate sections.

To Create a VNS Manually:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **Virtual Networks** pane and select an existing VNS to edit, or click the **New** button.
3. Enter a name for the VNS.
4. Select an existing WLAN Service for the VNS, or create a new WLAN Service, or edit an existing one.

For more information, see [“Configuring a Basic WLAN Service”](#) on page 6-2.

5. Configure the Default Policies for the VNS. Select existing policies, or create new policies, or edit existing ones.

For more information, see:

- [“Configuring Policies”](#) on page 5-1.
- [“Configuring Topologies”](#) on page 4-1.

6. Configure the Status parameters for the VNS:
 - **Synchronize** — Enable automatic synchronization with its availability peer. Refer to [“Using the Sync Summary”](#) on page 7-16 for information about viewing synchronization status. If this VNS is part of an availability pair, Enterasys recommends that you enable this feature.
 - **Restrict Policy Set** — This feature provides backward compatibility for legacy VNSs that were upgraded from software releases prior to V7.0. When it is enabled, the controller respects the prior hierarchical view of parent/child VNSs and maps external references to properly named (that is, hierarchically named) Policies.
 - **Enabled** — Check to enable the VNS.
7. Click **Save** to save your changes.

Also, as with creating a new VNS, you can:

- Configure a topology for the VNS
- Configure a policy for the VNS
- Configure WLAN services for the VNS
- Configure additional policies for the VNS

Creating a VNS Using the Wizard

The VNS wizard helps create and configure a new VNS by prompting you for a minimum amount of configuration information during the sequential configuration process. After the VNS wizard completes the VNS creation process, you can then continue to configure or revise any of the VNS configuration to suit your network needs.

When using the VNS wizard to create a new VNS, you can create the following types of VNSs:

- **NAC SSID-based VNS** — NAC gateway-compatible VNS. The Enterasys Wireless Controller integrates with an Enterasys NAC Controller to provide authentication, assessment, remediation and access control for mobile users. For more information, see [“Creating a NAC VNS Using the VNS Wizard”](#) on page 7-19.
- **Voice** — Voice-specific VNS that can support various wireless telephones, including optiPoint, Spectralink, Vocera, and Mobile Connect - Nokia. For more information, see [“Creating a Voice VNS Using the VNS Wizard”](#) on page 7-22.
- **Data** — Data-specific VNS, that can be configured to use either SSID or AAA authentication. For more information, see [“Creating a Data VNS Using the VNS Wizard”](#) on page 7-25.
- **Captive Portal** — A VNS that employs a Captive Portal page, which requires mobile users to provide login credentials when prompted to access network services. In addition, use the VNS wizard to configure a GuestPortal VNS using the Captive Portal option. For more information, see [“Creating a Captive Portal VNS Using the VNS Wizard”](#) on page 7-30.
- **Other** — Use this VNS wizard option to create a VNS as you would if you were creating a new VNS using the advanced configuration method. For more information, see [“Enabling and Disabling a VNS”](#) on page 7-47.

The VNS type dictates the configuration information that is required during the VNS creation process.

Creating a NAC VNS Using the VNS Wizard

The Enterasys Wireless Controller integrates with an Enterasys NAC Controller to provide authentication, assessment, remediation and access control for mobile users. For more information, see [“NAC integration with Enterasys Wireless WLAN”](#) on page 1-12.

Use the VNS wizard to configure a NAC gateway-compatible VNS by defining the following essential parameters:

- **VNS Name** — The name that will be assigned to the VNS and SSID.
- **IP Address** — The IP address of the Enterasys Wireless Controller’s interface on the VLAN.
- **Mask** — The subnet mask for the IP address to separate the network portion from the host portion of the address.
- **VLAN ID** — ID number of the VLAN to which the Enterasys Wireless Controller is bridged for the VNS.
- **Port** — Physical L2 port to which the configured VLAN is attached.

- **RADIUS server** — IP address of the Enterasys NAC Controller.
- **Redirection URL** — The URL that points to the NAC Controller’s web server.

The VNS wizard creates a **Bridge Traffic Locally at HWC VNS**. This VNS has the crucial attributes — SSID Network Assignment Type, MAC-based external captive portal authentication and WPA-PSK encryption — that makes it compatible with the Enterasys NAC Controller. The remaining VNS parameters are defined automatically according to best practice standards.

To configure a NAC VNS using the VNS wizard:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen is displayed.



3. In the **Name** box, type a name for the NAC SSID-based VNS.

4. In the **Category** drop-down list, click **NAC VNS**, and then click **Next**. The **NAC-compatible SSID-based VNS** screen is displayed.

enterasys
Secure Networks™ There's nothing more important than our customers.

Virtual Network Configuration

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

NAC-compatible VNS

This wizard enables you to quickly configure a NAC-compatible VNS by entering the essential settings only. The other settings are filled in automatically according to best practice standards.

VNS Name: testguest

IP Address:

Mask:

Interface: esa0

VLAN ID:

NAS: -

NAC server: Use existing server Add new server
(for MAC-based auth) test1

NAC web server IP:

Back Finish Cancel

5. Do the following:
- In the **IP address** box, type the IP address of the Enterasys Wireless Controller's interface on the VLAN.
 - In the **Mask** box, type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
 - In the **VLAN ID** box, type the VLAN tag to which the Enterasys Wireless Controller will be bridged for the VNS.
 - In the **Interface** drop-down list, select the physical port that provides the access to the VLAN.
 - In the **NAS** drop-down list, click the interface/port through which the NAC gateway will communicate with the Enterasys Wireless Controller. The IP address in this field will be used as the NAS IP RADIUS attribute when communicating with the NAC gateway.
 - In the **NAC server** drop-down list, click the existing NAC server you want to use for the VNS, or select the **Add new server** option, and then do the following:
 - (1) In the **Server Alias** box, type the name or IP address of the NAC server.
 - (2) In the **Hostname/IP** box, type the NAC server's FQDN (fully qualified domain name) or IP address.
 - (3) In the **Shared Secret** box, type the password that will be used to validate the connection between the Enterasys Wireless Controller and the NAC server.
 - (4) To proofread your shared secret key, click **Unmask**. The password is displayed.
- After the new NAC server is added, it will be displayed in the **Use existing server** drop-down list the next time you use the VNS wizard.



Note: You should always proofread your **Shared Secret** key to avoid any problems later when the Enterasys Wireless Controller attempts to communicate with the NAC Controller.

- (5) In the **NAC web server IP** box, type the NAC web server IP address.
6. To save your changes, click **Finish**. The VNS wizard creates a SSID-based NAC Controller-compatible VNS, and displays the configuration summary.
7. To close the VNS wizard, click **Close**.
8. If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Voice VNS Using the VNS Wizard

Use the VNS wizard to create a voice-specific VNS that can support various wireless telephones, including optiPoint, Spectralink, Vocera, and Mobile Connect - Nokia.

When you use the VNS wizard to create a voice-specific VNS, you optimize the voice VNS to support one wireless telephone vendor. If the voice VNS needs to be optimized for more than one wireless phone vendor, use the advanced method to create the voice-specific VNS. For more information, see “[Enabling and Disabling a VNS](#)” on page 7-47.

When you create a new voice VNS using the VNS wizard, you configure the VNS in the following stages:

- Basic settings
- Authentication settings, if applicable
- DHCP settings
- Privacy settings
- Radio assignment settings
- Summary

To Configure a Voice VNS Using the VNS Wizard:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen is displayed.
3. Click **Start VNS Wizard**. The **VNS Creation Wizard** screen is displayed.
4. In the **Name** box, type a name for the voice VNS.
5. In the **Category** drop-down list, click **Voice**, and then click **Next**. The **Basic Settings** screen is displayed.
6. Configure the VNS basic settings. The VNS type and mode you configure on the **Basic Settings** screen will dictate the VNS information you will need to provide.
 - **Enabled** — By default, the **Enabled** checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
 - **Type** — Click the wireless phone you want to support for the new voice VNS you are creating.

- **Mode** – Click the VNS mode you want to assign:
 - **Routed** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller.
 - **Bridge Traffic Locally at HWC** is a VNS type that has associated with it a Topology with a mode of Bridge Traffic Locally at HWC. User traffic is tunneled to the Enterasys Wireless Controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at HWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding Enterasys Wireless Controller interface must match the correct VLAN.

If you configure a routed voice VNS, do the following:

- (1) **Gateway** – Type the Enterasys Wireless Controller's own IP address of the topology associated with that VNS. This IP address is also the default gateway for the VNS. The Enterasys Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).
- (2) **Mask** – Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
- (3) **Gateway/SVP** – If the voice VNS is to support Spectralink wireless phones, type the IP address of the SpectraLink Voice Protocol (SVP) gateway.
- (4) **Vocera Server** – If the voice VNS is to support Vocera wireless phones, type the IP address of the Vocera server.
- (5) **PBX** – If the voice VNS is to support either WL2 or Mobile Connect - Nokia wireless phones, type the PBX IP address.
- (6) **Enable Authentication** – If applicable, select this checkbox to enable authentication for the new voice VNS.
- (7) **Enable DHCP** – By default, this option is selected.

If you configure a bridge traffic locally at the HWC voice VNS, do the following:

- (1) **Interface** – Click the physical interface that provides the access to the VLAN.
- (2) **Interface IP address** – Type the IP address of the Enterasys Wireless Controller's interface on the VLAN.
- (3) **Mask** – Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
- (4) **VLAN ID** – Type the VLAN tag to which the Enterasys Wireless Controller will be bridged for the VNS.
- (5) **Gateway/SVP** – If the voice VNS is to support Spectralink wireless phones, type the IP address of the SpectraLink Voice Protocol (SVP) gateway.
- (6) **Vocera Server** – If the voice VNS is to support Vocera wireless phones, type the IP address of the Vocera server.
- (7) **PBX Server** – If the voice VNS is to support either WL2 or Mobile Connect - Nokia wireless phones, type the PBX IP address.
- (8) **Enable Authentication** – If applicable, select this checkbox to enable authentication for the new voice VNS.

- (9) **Enable DHCP** — If applicable, select this checkbox to enable DHCP authentication for the new voice VNS.
7. Click **Next**.
- If the **Enable Authentication** checkbox is selected, you now must configure the Authentication properties of the new voice VNS. Continue with [Step 8](#).
- If the **Enable Authentication** checkbox is clear, you must now configure the DHCP properties of the new voice VNS. Continue with [Step 10](#).
8. On the **Authentication** screen, do the following:
- **Radius Server** — Click the RADIUS server you want to assign to the new voice VNS, or click **Add New Server** and then do the following:
 - **Server Alias** — Type a name you want to assign to the new RADIUS server.
 - **Hostname/IP** — Type either the RADIUS server’s FQDN (fully qualified domain name) or IP address.
 - **Shared Secret** — Type the password that will be used to validate the connection between the Enterasys Wireless Controller and the RADIUS server.
 - **Mask/Unmask** — Click to display or hide your shared secret key.
 - **Roles** — Select the authentication role options for the RADIUS server.
 - MAC-based Authentication** — Select to enable the RADIUS server to perform MAC-based authentication on the voice VNS.
 - If applicable, and the **MAC-based authentication** option is enabled, select to enable **MAC-based authorization on roam**.
9. Click **Next**. The **DHCP** screen is displayed.
10. On the **DHCP** screen, in the **DHCP Option** drop-down list, click one of the following:
- **Use DHCP Relay** — Using DHCP relay forces the Enterasys Wireless Controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Enterasys Wireless Controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
 - **DHCP Servers** — Type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The Enterasys Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the Enterasys Wireless Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)
 - **Local DHCP Server** — If applicable, edit the local DHCP server settings.
11. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
12. In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
13. Click **Next**. The **Privacy** screen is displayed. Most options on this screen are view-only.
14. On the **Privacy** screen, do the following:
- **Pre-shared key** — Type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key.

- **Mask/Unmask** – Click to display or hide your shared secret key.
15. Click **Next**. The **Radio Assignment** screen is displayed.
 16. On the **Radio Assignment** screen, do the following:
 - In the **AP Default Settings** section, select the radios of the AP default settings profile that you want to broadcast the voice VNS.
 - In the **AP Selection** section, select the group of APs that will broadcast the voice VNS:
 - **all radios** – Click to assign all of the APs’ radios.
 - **radio 1** – Click to assign only the APs’ Radio 1.
 - **radio 2** – Click to assign only the APs’ Radio 2.
 - **local APs - all radios** – Click to assign only the local APs.
 - **local APs - radio 1** – Click to assign only the local APs’ Radio 1.
 - **local APs - radio 2** – Click to assign only the local APs’ Radio 2.
 - **foreign APs - all radios** – Click to assign only the foreign APs.
 - **foreign APs - radio 1** – Click to assign only the foreign APs’ Radio 1.
 - **foreign APs - radio 2** – Click to assign only the foreign APs’ Radio 2.
 - If applicable, select the **WMM** checkbox. WMM (Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.
 17. Click **Next**. The **Summary** screen is displayed.
 18. Confirm your voice VNS configuration. To revise your configuration, click **Back**.
 19. To create your VNS, click **Finish**, and then click **Close**.
 20. If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Data VNS Using the VNS Wizard

Use the VNS wizard to create a data-specific VNS that can be configured to use either SSID or AAA authentication.

When you create a new data VNS using the VNS wizard, you configure the VNS in the following stages:

- Basic settings
- Authentication settings
- DHCP settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary

To configure a data VNS using the VNS wizard:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen is displayed.
3. Click **Start VNS Wizard**. The **VNS Creation Wizard** screen is displayed.
4. In the **Name** box, type a name for the data VNS.
5. In the **Category** drop-down list, click **Data**, and then click **Next**. The **Basic Settings** screen is displayed.
6. Configure the data VNS basic settings. The VNS type and mode you configure on the **Basic Settings** screen will dictate the VNS information you will need to provide.
 - **Enabled** — By default, the **Enabled** checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
 - **Type** — Click the type of network assignment for the VNS. There are two options for network assignment, **Disabled** or **802.1x**.
 - **Mode** — Click the VNS mode you want to assign:
 - **Routed** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller.
 - **Bridge Traffic Locally at HWC** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at HWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding Enterasys Wireless Controller interface must match the correct VLAN.
 - **Bridge Traffic Locally at AP** is a VNS type where user traffic is directly bridged to a VLAN at the AP network point of access (switch port).

If you are configuring a routed data VNS, do the following:

- (1) **Gateway** — Type the Enterasys Wireless Controller's own IP address of the topology associated with that VNS. This IP address is the default gateway for the VNS. The Enterasys Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).
- (2) **Mask** — Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
- (3) **Enable Authentication** — This option is enabled by default if the **Type** is 802.1x.
- (4) **Enable DHCP** — By default, this option is enabled for a routed data VNS.

If you configuring a bridge traffic locally at AP data VNS, do the following:

- (1) **Tagged** — Select if you want to assign this VNS to a specific VLAN.
- (2) **VLAN ID** — Type the VLAN tag to which the Enterasys Wireless Controller will be bridged for the data VNS.
- (3) **Untagged** — Select if you want this VNS to be untagged. This option is selected by default.

- (4) **Enable Authentication** — If applicable, select this checkbox to enable authentication for the new data VNS. This option is enabled by default if the **Type** is 802.1x.

If you are configuring a bridge traffic locally at HWC data VNS, do the following:

- (1) **Interface** — Click the physical port that provides the access to the VLAN.
 - (2) **Interface IP address** — Type the IP address of the Enterasys Wireless Controller's interface on the VLAN.
 - (3) **Mask** — Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
 - (4) **VLAN ID** — Type the VLAN tag to which the Enterasys Wireless Controller will be bridged for the VNS.
 - (5) **Enable Authentication** — If applicable, select this checkbox to enable authentication for the new data VNS. This option is enabled by default if the **Type** is 802.1x.
 - (6) **Enable DHCP** — If applicable, select this checkbox to enable DHCP authentication for the new data VNS.
7. Click **Next**. The **Authentication** screen is displayed.
 8. On the **Authentication** screen, do the following:
 - **Radius Server** — Click the RADIUS server you want to assign to the new data VNS, or click **Add New Server** and then do the following:
 - **Server Alias** — Type a name you want to assign to the new RADIUS server.
 - **Hostname/IP** — Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
 - **Shared Secret** — Type the password that will be used to validate the connection between the Enterasys Wireless Controller and the RADIUS server.
 - **Mask/Unmask** — Click to display or hide your shared secret key.
 - **Roles** — Select the authentication role options for the RADIUS server:
 - **MAC-based Authentication** — Select to enable the RADIUS server to perform MAC-based authentication on the data VNS.
If applicable, and the **MAC-based authentication** option is enabled, select to enable **MAC-based authorization on roam**.
 9. Click **Next**. The **DHCP** screen is displayed, if DHCP was enabled previously.
 10. In the **DHCP Option** drop-down list, click one of the following:
 - **Use DHCP Relay** — Using DHCP relay forces the Enterasys Wireless Controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Enterasys Wireless Controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
 - **DHCP Servers** — If **Use DHCP Relay** was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The Enterasys Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the Enterasys Wireless Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)

- **Local DHCP Server** — If applicable, edit the local DHCP server settings.
- 11. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
- 12. In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
- 13. Click **Next**. The **Filtering** screen is displayed.
- 14. On the **Filtering** screen, do the following:
 - In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the Enterasys Wireless Controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the Enterasys Wireless Controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
- 15. In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
- 16. Click **Next**. The **Privacy** screen is displayed.
- 17. On the **Privacy** screen, select one of the following:
 - **Static Keys** — Select to configure static keys. Then enter:
 - **WEP Key Index** — Click the WEP encryption key index: **1, 2, 3, or 4**.



Note: Specifying the WEP key index is supported only for AP36XX Wireless APs.

- **WEP Key Length** — Click the WEP encryption key length: **64 bit, 128 bit, or 152 bit**.
- Select an **Input Method**:
 - Input Hex** — type the WEP key input in the WEP Key box. The key is generated automatically based on the input.
 - Input String** — type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The **WEP Key** box is automatically filled by the corresponding Hex code.
- **WPA-PSK** — Select to configure Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management.
 - To enable WPA v1 encryption, select **WPA v.1**. In the **Encryption** drop-down list, select one of the following encryption types:
 - Auto** — The Wireless AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard).
 - TKIP only** — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.
 - To enable WPA v2 encryption, select **WPA v.2**. In the **Encryption** drop-down list, click one of the following encryption types:
 - Auto** — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard).

AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.

- To enable re-keying after a time interval, select **Broadcast re-key interval**, then type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.

If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.

- To enable the group key power save retry, select **Group Key Power Save Retry**.



Note: The group key power save retry is only supported for AP36XX Wireless APs.

- In the **Pre-shared key** box, type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key.
 - **Mask/Unmask** — Click to display or hide your shared secret key.

18. Click **Next**. The **Radio Assignment** screen is displayed.

19. On the **Radio Assignment** screen, do the following:

- In the **AP Default Settings** section, select the radios of the AP default settings profile that you want to broadcast the data VNS.
- In the **AP Selection** section, select the group of APs that will broadcast the data VNS:
 - **all radios** — Click to assign all of the APs' radios.
 - **radio 1** — Click to assign only the APs' Radio 1.
 - **radio 2** — Click to assign only the APs' Radio 2.
 - **local APs - all radios** — Click to assign only the local APs.
 - **local APs - radio 1** — Click to assign only the local APs' Radio 1.
 - **local APs - radio 2** — Click to assign only the local APs' Radio 2.
 - **foreign APs - all radios** — Click to assign only the foreign APs.
 - **foreign APs - radio 1** — Click to assign only the foreign APs' Radio 1.
 - **foreign APs - radio 2** — Click to assign only the foreign APs' Radio 2.
- If applicable, select the **WMM** checkbox. WMM (Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.

20. Click **Next**. The **Summary** screen is displayed.

21. Confirm your data VNS configuration. To revise your configuration, click **Back**.

22. To create your VNS, click **Finish**, and then click **Close**.

The data VNS is created and saved.

23. If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

If the Enterasys Wireless Controller is configured to be part of an availability pair, you can choose to synchronize the VNS on the secondary Enterasys Wireless Controller. See [Chapter 11, Availability and Session Availability](#) for more information.

Creating a Captive Portal VNS Using the VNS Wizard

Use the VNS wizard to create a Captive Portal VNS. A Captive Portal VNS employs an authentication method that uses a Web redirection which directs a mobile user's Web session to an authentication server. Typically, the mobile user must provide their credentials (user ID, password) to be authenticated. There are three types of Captive Portal VNSs you can create:

- **Internal Captive Portal** — The Enterasys Wireless Controller's own Captive Portal authentication page — configured as an editable form — is used to request user credentials. The redirection triggers the locally stored authentication page where the mobile user must provide the appropriate credentials, which then is checked against what is listed in the configured RADIUS server.
- **External Captive Portal** — An entity outside of the Enterasys Wireless Controller is responsible for handling the mobile user authentication process, presenting the credentials request forms and performing user authentication procedures. The external Web server location must be explicitly listed as an allowed destination in the non-authenticated filter.
- **GuestPortal** — A GuestPortal VNS provides wireless device users with temporary guest network services.

When you create a new captive portal VNS using the VNS wizard, you configure the VNS in the following stages:

- Basic settings
- Authentication settings
- DHCP settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary review

Creating an Internal Captive Portal VNS

To Configure an Internal Captive Portal VNS Using the VNS Wizard:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen is displayed.
3. In the **Name** box, type a name for the Captive Portal VNS.
4. In the **Category** drop-down list, click **Captive Portal**, and then click **Next**. The **Basic Settings** screen is displayed.
5. Configure the Captive Portal VNS basic settings. The VNS type and mode you configure on the **Basic Settings** screen will dictate the VNS information you will need to provide.
 - **Enabled** — By default, the **Enabled** checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
 - **Authentication Mode** — Click **Internal Captive Portal**.

- **Mode** – Click the VNS mode you want to assign:
 - **Routed** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller.
 - **Bridge Traffic Locally at HWC** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at HWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding Enterasys Wireless Controller interface must match the correct VLAN.

If configuring a routed internal Captive Portal VNS, do the following:

- (1) **Gateway** – Type the Enterasys Wireless Controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The Enterasys Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).
- (2) **Mask** – Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
- (3) **Message** – Type a brief message.
- (4) **Enable Authentication** – By default, this option is selected if the **VNS Type** is **Internal Captive Portal**, which enables authentication for the new Captive Portal VNS.
- (5) **Enable DHCP** – By default, this option is selected if the **VNS Type** is **Internal Captive Portal**, which enables DHCP authentication for the new Captive Portal VNS.

If configuring a bridge traffic locally at HWC internal Captive Portal VNS, do the following:

- (1) **Interface** – Click the physical port that provides the access to the VLAN.
- (2) **Interface IP address** – Type the IP address of the Enterasys Wireless Controller's interface on the VLAN.
- (3) **Mask** – Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
- (4) **VLAN ID** – Type the VLAN tag to which the Enterasys Wireless Controller will be bridged for the VNS.
- (5) **Message** – Type a brief message that will be displayed above the **Login** button that greets the mobile device user.
- (6) **Enable Authentication** – By default, this option is selected if the **VNS Type** is **Internal Captive Portal**, which enables authentication for the new Captive Portal VNS.
- (7) **Enable DHCP** – If applicable, select this checkbox to enable DHCP authentication for the new Captive Portal VNS.

6. Click **Next**. The **Authentication** screen is displayed.

7. On the **Authentication** screen, do the following:

- **Radius Server** – Click the RADIUS server you want to assign to the new Captive Portal VNS, or click **Add New Server** and then do the following:
 - **Server Alias** – Type a name you want to assign to the new RADIUS server.

- **Hostname/IP** — Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
 - **Shared Secret** — Type the password that will be used to validate the connection between the Enterasys Wireless Controller and the RADIUS server.
 - **Mask/Unmask** — Click to display or hide your shared secret key.
 - **Roles** — Select the authentication role options for the RADIUS server:
 - **Authentication** — By default, this option is selected if the **VNS Type** is **Internal Captive Portal**, which enables the RADIUS server to perform authentication on the Captive Portal VNS.
 - **MAC-based Authentication** — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS.
If the **MAC-based authentication** option is enabled, select to enable **MAC-based authorization on roam**, if applicable.
 - **Accounting** — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.
8. Click **Next**. The **DHCP** screen is displayed.
9. On the **DHCP** screen, do the following:
- In the **DHCP Option** drop-down list, click one of the following:
 - **Use DHCP Relay** — Using DHCP relay forces the Enterasys Wireless Controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Enterasys Wireless Controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
 - **DHCP Servers** — Type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The Enterasys Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the Enterasys Wireless Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)
 - **Local DHCP Server** — If applicable, edit the local DHCP server settings.
10. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
11. In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
12. Click **Next**. The **Filtering** screen is displayed.
13. On the **Filtering** screen, do the following:
- In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the Enterasys Wireless Controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the Enterasys Wireless Controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.

- **Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal Web page for login.
14. In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
 15. Click **Next**. The **Privacy** screen is displayed.
 16. On the **Privacy** screen, do the following:
 - **None** — Select if you do not want to assign any privacy mechanism.
 - **Static Keys** — Select to configure static keys.
 - **WEP Key Index** — Click the WEP encryption key index: **1, 2, 3, or 4**.



Note: Specifying the WEP key index is supported only for AP36XX Wireless APs.

- **WEP Key Length** — Click the WEP encryption key length: **64 bit, 128 bit, or 152 bit**.
- Select one of the following input methods:
 - Input Hex** — If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically based on the input.
 - Input String** — If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The **WEP Key** box is automatically filled by the corresponding Hex code.
- **WPA-PSK** — Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.
- To enable WPA v1 encryption, select **WPA v.1**. If WPA v.1 is enabled, click one of the following encryption types from the **Encryption** drop-down list:
 - **Auto** — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
 - **TKIP only** — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.
- To enable WPA v2-type encryption, select **WPA v.2**. The other options for this drop-down list are:
 - **Auto** — If you click **Auto**, the Wireless AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard).
 - **AES only** — If you click **AES**, the Wireless AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.
- To enable re-keying after a time interval, select **Broadcast re-key interval**. If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.
 - In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically.

- To enable the group key power save retry, select **Group Key Power Save Retry**.



Note: The group key power save retry is only supported for AP36XX Wireless APs.

- In the **Pre-shared key** box, type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key.
 - **Mask/Unmask** — Click to display or hide your shared secret key.

17. Click **Next**. The **Radio Assignment** screen is displayed.

18. On the **Radio Assignment** screen, do the following:

- In the **AP Default Settings** section, select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
- In the **AP Selection** section, select the group of APs that will broadcast the Captive Portal VNS:
 - **all radios** — Click to assign all of the APs' radios.
 - **radio 1** — Click to assign only the APs' Radio 1.
 - **radio 2** — Click to assign only the APs' Radio 2.
 - **local APs - all radios** — Click to assign only the local APs.
 - **local APs - radio 1** — Click to assign only the local APs' Radio 1.
 - **local APs - radio 2** — Click to assign only the local APs' Radio 2.
 - **foreign APs - all radios** — Click to assign only the foreign APs.
 - **foreign APs - radio 1** — Click to assign only the foreign APs' Radio 1.
 - **foreign APs - radio 2** — Click to assign only the foreign APs' Radio 2.
- If applicable, select the **WMM** checkbox. WMM (Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.

19. Click **Next**. The **Summary** screen is displayed.

20. Confirm your data VNS configuration. To revise your configuration, click **Back**.

21. To create your VNS, click **Finish**, and then click **Close**.

22. If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating an External Captive Portal VNS

To configure an external Captive Portal VNS using the VNS wizard:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen is displayed.
3. In the **Name** box, type a name for the Captive Portal VNS.

4. In the **Category** drop-down list, click **Captive Portal**, and then click **Next**. The **Basic Settings** screen is displayed.
5. Configure the Captive Portal VNS basic settings. The VNS type and mode you configure on the **Basic Settings** screen will dictate the VNS information you will need to provide.
 - **Enabled** – By default, the **Enabled** checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
 - **Authentication Mode** – Click **External Captive Portal**.
 - **Mode** – Click the VNS mode you want to assign:
 - **Routed** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller.
 - **Bridge Traffic Locally at HWC** is a VNS type where user traffic is tunneled to the Enterasys Wireless Controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at HWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding Enterasys Wireless Controller interface must match the correct VLAN.

If configuring a routed external Captive Portal VNS, do the following:

- (1) **Gateway** – Type the Enterasys Wireless Controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The Enterasys Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).
- (2) **Mask** – Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
- (3) **HWC Connection** – Click the Enterasys Wireless Controller IP address. Also type the port of the Enterasys Wireless Controller in the accompanying box.

If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the Enterasys Wireless Controller to allow the Enterasys Wireless Controller to continue with the RADIUS authentication and filtering.

- (1) **Redirection URL** – Type the URL to which the wireless device user will be directed to after authentication.
- (2) **Shared Secret** – Type the password that is common to both the Enterasys Wireless Controller and the external Web server if you want to encrypt the information passed between the Enterasys Wireless Controller and the external Web server.
- (3) **Enable Authentication** – Select this checkbox to enable authentication for the new Captive Portal VNS.
- (4) **Enable DHCP** – Select this checkbox to enable DHCP services for this new Captive Portal VNS.

If configuring a bridge traffic locally at HWC external Captive Portal VNS, do the following:

- (1) **Interface** – Click the physical port that provides the access to the VLAN.
- (2) **Interface IP address** – Type the IP address of the Enterasys Wireless Controller's interface on the VLAN.

- (3) **Mask** — Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
 - (4) **VLAN ID** — Type the VLAN tag to which the Enterasys Wireless Controller will be bridged for the VNS.
 - (5) **HWC Connection** — Click the Enterasys Wireless Controller IP address. Also type the port of the Enterasys Wireless Controller in the accompanying box.

If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the Enterasys Wireless Controller to allow the Enterasys Wireless Controller to continue with the RADIUS authentication and filtering.
 - (6) **Redirection URL** — Type the URL to which the wireless device user will be directed to after authentication.
 - (7) **Shared Secret** — Type the password that is common to both the Enterasys Wireless Controller and the external Web server if you want to encrypt the information passed between the Enterasys Wireless Controller and the external Web server.
 - (8) **Enable Authentication** — Select this checkbox to enable authentication for the new Captive Portal VNS.
 - (9) **Enable DHCP** — Select this checkbox to enable DHCP authentication for the new Captive Portal VNS.
6. Click **Next**. The VNS wizard displays the appropriate configuration screens, depending on your selection of the **Enable Authentication** and **Enable DHCP** checkboxes.
 7. If applicable, on the **Authentication** screen, do the following:
 - **Radius Server** — Click the RADIUS server you want to assign to the new Captive Portal VNS, or click **Add New Server** and then do the following:
 - **Server Alias** — Type a name you want to assign to the new RADIUS server.
 - **Hostname/IP** — Type either the RADIUS server’s FQDN (fully qualified domain name) or IP address.
 - **Shared Secret** — Type the password that will be used to validate the connection between the Enterasys Wireless Controller and the RADIUS server.
 - **Mask/Unmask** — Click to display or hide your shared secret key.
 - **Roles** — Select the authentication role options for the RADIUS server:
 - **Authentication** — Select to enable the RADIUS server to perform authentication on the Captive Portal VNS.
 - **MAC-based Authentication** — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS.
 If the **MAC-based authentication** option is enabled, select to enable **MAC-based authorization on roam**, if applicable.
 - **Accounting** — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.
 8. Click **Next**.
 9. If applicable, on the **DHCP** screen, do the following:
 - In the **DHCP Option** drop-down list, click one of the following:
 - **Use DHCP Relay** — Using DHCP relay forces the Enterasys Wireless Controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Enterasys Wireless Controller

and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.

- **DHCP Servers** — Type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The Enterasys Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the Enterasys Wireless Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)

- **Local DHCP Server** — If applicable, edit the local DHCP server settings.
10. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
 11. In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
 12. Click **Next**. The **Filtering** screen is displayed.
 13. On the **Filtering** screen, do the following:
 - In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the Enterasys Wireless Controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the Enterasys Wireless Controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
 - **Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal Web page for login.
 14. In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
 15. Click **Next**. The **Privacy** screen is displayed.
 16. On the **Privacy** screen, do the following:
 - **None** — Select if you do not want to assign any privacy mechanism.
 - **Static Keys** — Select to configure static keys.
 - **WEP Key Index** — Click the WEP encryption key index: **1, 2, 3, or 4**.



Note: Specifying the WEP key index is supported only for AP36XX Wireless APs.

- **WEP Key Length** — Click the WEP encryption key length: **64 bit, 128 bit, or 152 bit**.
- Select one of the following input methods:
 - Input Hex** — If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically based on the input.
 - Input String** — If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The **WEP Key** box is automatically filled by the corresponding Hex code.

- **WPA-PSK** — Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.
 - To enable WPA v1 encryption, select **WPA v.1**. If WPA v.1 is enabled, click one of the following encryption types from the **Encryption** drop-down list:
 - Auto** — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
 - TKIP only** — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.
 - To enable WPA v2-type encryption, select **WPA v.2**. The other options for this drop-down list are:
 - Auto** — If you click **Auto**, the Wireless AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard).
 - AES only** — If you click **AES**, the Wireless AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.
- To enable re-keying after a time interval, select **Broadcast re-key interval**. If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.
 - In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically.
- To enable the group key power save retry, select **Group Key Power Save Retry**.



Note: The group key power save retry is only supported for AP36XX Wireless APs.

- In the **Pre-shared key** box, type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key.
 - **Mask/Unmask** — Click to display or hide your shared secret key.

17. Click **Next**. The **Radio Assignment** screen is displayed.

18. On the **Radio Assignment** screen, do the following:

- In the **AP Default Settings** section, select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
- In the **AP Selection** section, select the group of APs that will broadcast the Captive Portal VNS:
 - **all radios** — Click to assign all of the APs' radios.
 - **radio 1** — Click to assign only the APs' Radio 1.
 - **radio 2** — Click to assign only the APs' Radio 2.
 - **local APs - all radios** — Click to assign only the local APs.
 - **local APs - radio 1** — Click to assign only the local APs' Radio 1.

- **local APs - radio 2** — Click to assign only the local APs' Radio 2.
 - **foreign APs - all radios** — Click to assign only the foreign APs.
 - **foreign APs - radio 1** — Click to assign only the foreign APs' Radio 1.
 - **foreign APs - radio 2** — Click to assign only the foreign APs' Radio 2.
- If applicable, select the **WMM** checkbox. WMM (Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.
19. Click **Next**. The **Summary** screen is displayed.
 20. Confirm your data VNS configuration. To revise your configuration, click **Back**.
 21. To create your VNS, click **Finish**, and then click **Close**.
 22. If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a GuestPortal VNS

A GuestPortal provides wireless device users with temporary guest network services. A GuestPortal is serviced by a GuestPortal-dedicated VNS. An Enterasys Wireless Controller is allowed only one GuestPortal-dedicated VNS at a time. GuestPortal user accounts are administered by a GuestPortal manager. A GuestPortal manager is a login group — GuestPortal managers must have their accounts created for them on the Enterasys Wireless Controller. For more information, see "[Working with GuestPortal Administration](#)" on page 18-1

The GuestPortal VNS is a Captive Portal authentication-based VNS that uses a database on the Enterasys Wireless Controller for managing user accounts. The database is administered through a simple, user-friendly graphic user interface that can be used by non-technical staff.

The GuestPortal VNS can be a Routed or a Bridge Traffic Locally at the HWC VNS, with SSID-based network assignment. The GuestPortal VNS is a simplified VNS. It does not support the following:

- RADIUS authentication or accounting
- MAC-based authorization
- Child VNS support

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS. When you create a new VNS using the VNS wizard, you configure the VNS in the following stages:

- Basic settings
- DHCP settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary

Use the following high-level description to set up a GuestPortal on your system:

1. Create a GuestPortal VNS.

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS.

2. Configure the GuestPortal ticket.

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. For more information, see [“Working with the GuestPortal Ticket Page”](#) on page 18-11.

3. Configure availability, if applicable.

Availability maintains service availability in the event of a Enterasys Wireless Controller outage. For more information, see [Chapter 11, Availability and Session Availability](#).

4. Create GuestPortal manager and user accounts.

For more information, see [“Working with GuestPortal Administration”](#) on page 18-1

5. Manage your guest accounts and GuestPortal logs.

For more information, see the Enterasys Wireless Convergence Software *Maintenance Guide*.

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS. A Enterasys Wireless Controller is allowed only **one** GuestPortal-dedicated VNS at a time.

To Create a GuestPortal VNS from an Already Existing VNS:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, select and expand the **Virtual Networks** pane.
3. Click on the VNS you want to configure as a GuestPortal VNS. The VNS configuration window **Core** tab is displayed.
4. Select a preconfigured WLAN Service and click **Edit**, or press **New** to create a new WLAN Service.
5. In the Edit WLAN Service window, click the **Auth & Acct** tab.
6. In the **Authentication Mode** drop-down list, click **GuestPortal**.
7. To save your changes, click **Save**.

To Create a New GuestPortal VNS Using the VNS Wizard:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen is displayed.
3. In the **Name** box, type a name for the GuestPortal VNS.

- In the **Category** drop-down list, click **Captive Portal**, and then click **Next**. The **Basic Settings** screen is displayed.

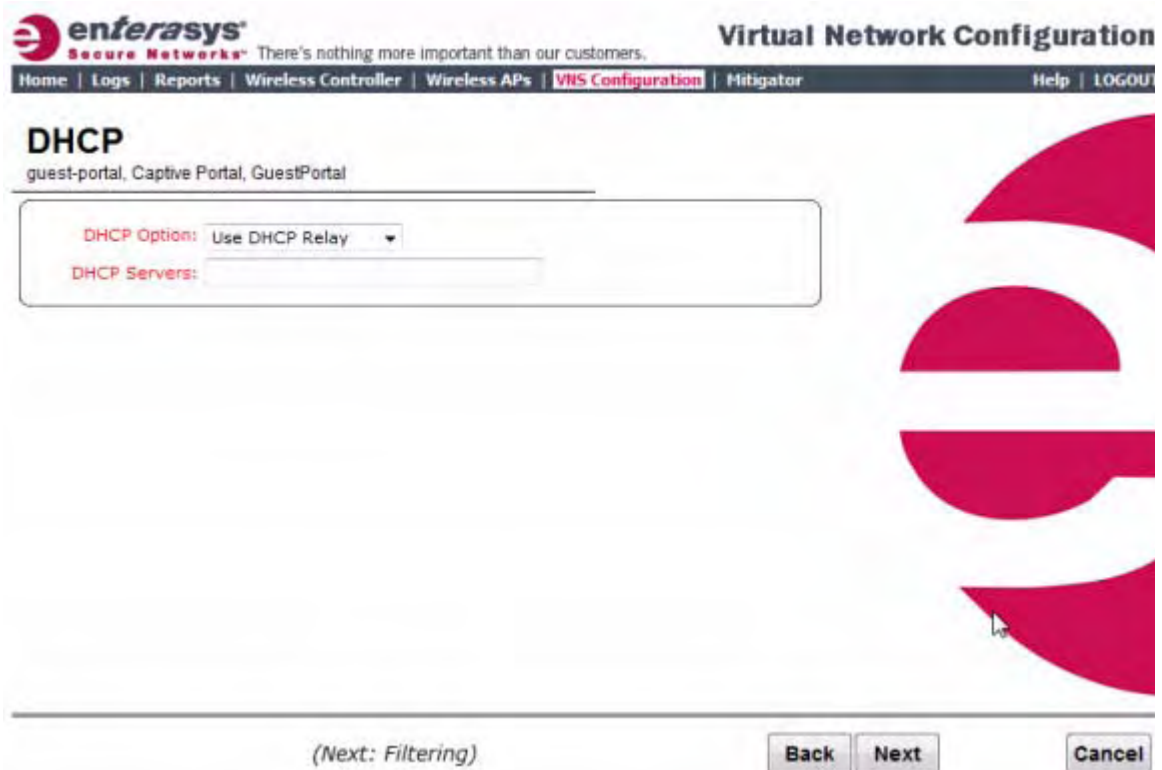
The screenshot shows the Enterasys Virtual Network Configuration wizard. The page title is "Virtual Network Configuration" and the breadcrumb trail includes "Home | Logs | Reports | Wireless Controller | Wireless APs | VNS Configuration | Hitigator". The main heading is "Basic Settings" for a "guest-portal, Captive Portal" VNS. The settings are as follows:

- Enabled:**
- Synchronize:**
- Name:** guest-portal
- Category:** Captive Portal
- SSID:** guest-portal
- Authentication Mode:** -
- Mode:** -

At the bottom of the form, there are three buttons: "Back", "Next", and "Cancel". A link "(Next: Privacy)" is also visible.

- Configure the VNS basic settings:
 - Enabled** — By default, the **Enabled** checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
 - Authentication Mode**— In the drop-down list, click **GuestPortal**.
 - Mode** — In the drop-down list, click the VNS mode. either **Routed** or **Bridge Traffic Locally at HWC**:
 - Routed** — User traffic is tunneled to the Enterasys Wireless Controller.
 - In the **Gateway** box, type the Enterasys Wireless Controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The Enterasys Wireless Controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the Enterasys Wireless Controller's interface in their effort to route packets to an external host).
 - In the **Mask** box, type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
 - Bridge Traffic Locally at HWC** — User traffic is tunneled to the Enterasys Wireless Controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at HWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding Enterasys Wireless Controller interface must match the correct VLAN.

- In the **Interface** drop-down list, click the physical interface that provides the access to the VLAN.
 - In the **Interface IP address** box, type the IP address of the Enterasys Wireless Controller's interface on the VLAN.
 - In the **Mask** box, type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
 - In the **VLAN ID** box, type the VLAN to which the Enterasys Wireless Controller will be bridged for the VNS. Then, select either **Untagged** or **Tagged**.
 - If applicable, select the **Enable DHCP** checkbox.
6. Click **Next**. The **DHCP** screen is displayed.
- If DHCP is disabled, continue with [step 11](#) on page 7-43. The **Filtering** screen is displayed.



7. Configure the DHCP settings. In the **DHCP Option** drop-down list, click one of the following:
- **Use DHCP Relay** — Using DHCP relay forces the Enterasys Wireless Controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Enterasys Wireless Controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
 - **DHCP Servers** — Type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The Enterasys Wireless Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the Enterasys Wireless Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach

devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)

- **Local DHCP Server** – If applicable, edit the local DHCP server settings.
8. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
 9. In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
 10. Click **Next**. The **Filtering** screen is displayed.

Filtering
guest-portal, Captive Portal, GuestPortal

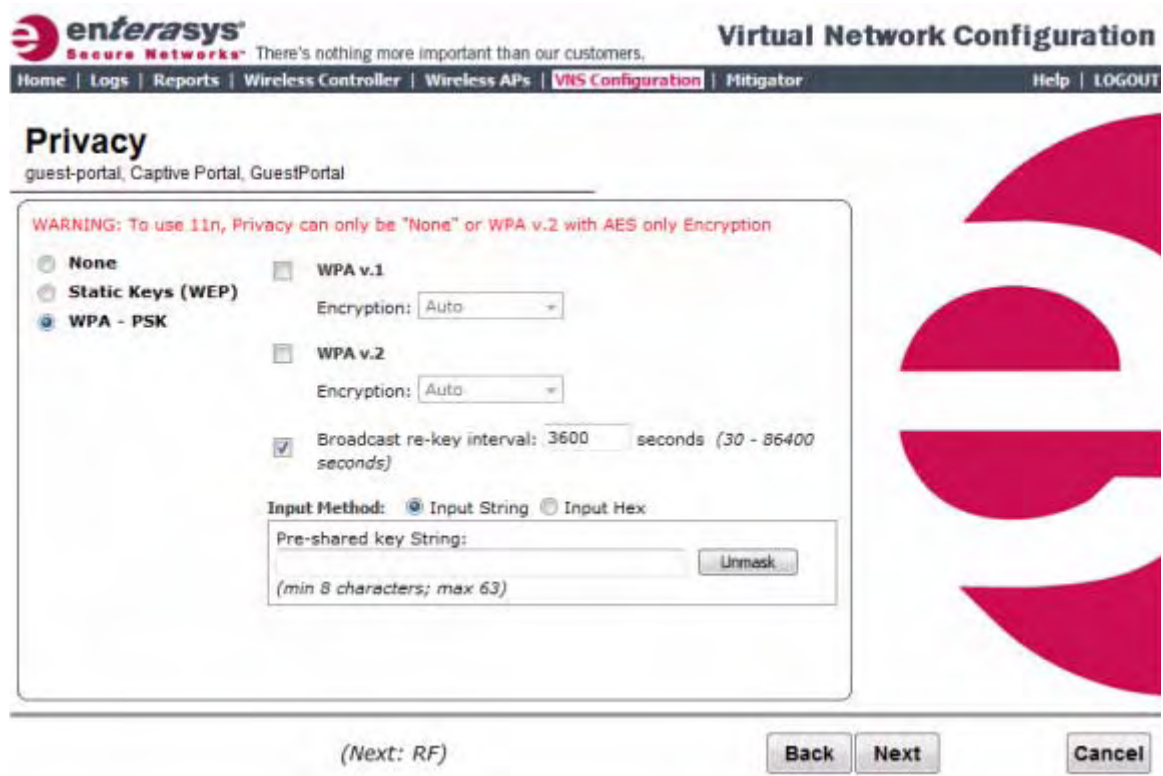
Filter ID: Authenticated

Enable	Allow	Deny	Filter Description
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	IMAP (0.0.0.0/0:143, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	FTP (0.0.0.0/0:20-21, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	POP (0.0.0.0/0:110, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SMTP (0.0.0.0/0:25, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	HTTP (0.0.0.0/0:80 AND 0.0.0.0/0:8080, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	HTTPS (0.0.0.0/0:443, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TELNET (0.0.0.0/0:23, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SIP (0.0.0.0/0:5060-5061, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SSH (0.0.0.0/0:22, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TACACS (0.0.0.0/0:49, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	DNS (0.0.0.0/0:53, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	BootP (0.0.0.0/0:67, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TFTP (0.0.0.0/0:69, UDP)

(Next: Privacy) Back Next Cancel

11. Configure the VNS filtering settings:
12. In the **Filter ID** drop-down list, click one of the following:
 - **Authenticated** – Controls network access after the user has been authenticated.
 - **Non-authenticated** – Controls network access and to direct users to a Captive Portal Web page for login.
13. In the **Filter** table, select the **Enable** checkbox for the desired filters, then select the **Allow** or **Deny** option buttons for each filter as needed.
14. At the bottom of the Filter list, select **Allow** or **Deny** for **All Other Traffic**.

15. Click **Next**. The **Privacy** screen is displayed.



16. Configure the VNS Privacy settings:

- **None** — Select if you do not want to assign any privacy mechanism.
- **Static Keys (WEP)** — Select to use keys on the VNS that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 VNSs. For each VNS, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.
 - From the **WEP Key Index** drop-down list, click the WEP encryption key index: **1, 2, 3, or 4**.



Note: Specifying the WEP key index is supported only for AP36XX Wireless APs.

- From the **WEP Key Length** drop-down list, click the WEP encryption key length: **64 bit, 128 bit, or 152 bit**.
- **Input Method** — Select one of the following:
 - Input Hex** — If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.
 - Input String** — If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **Strings** box. The **WEP Key** box is automatically filled by the corresponding Hex code.
- **WPA-PSK** — Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.

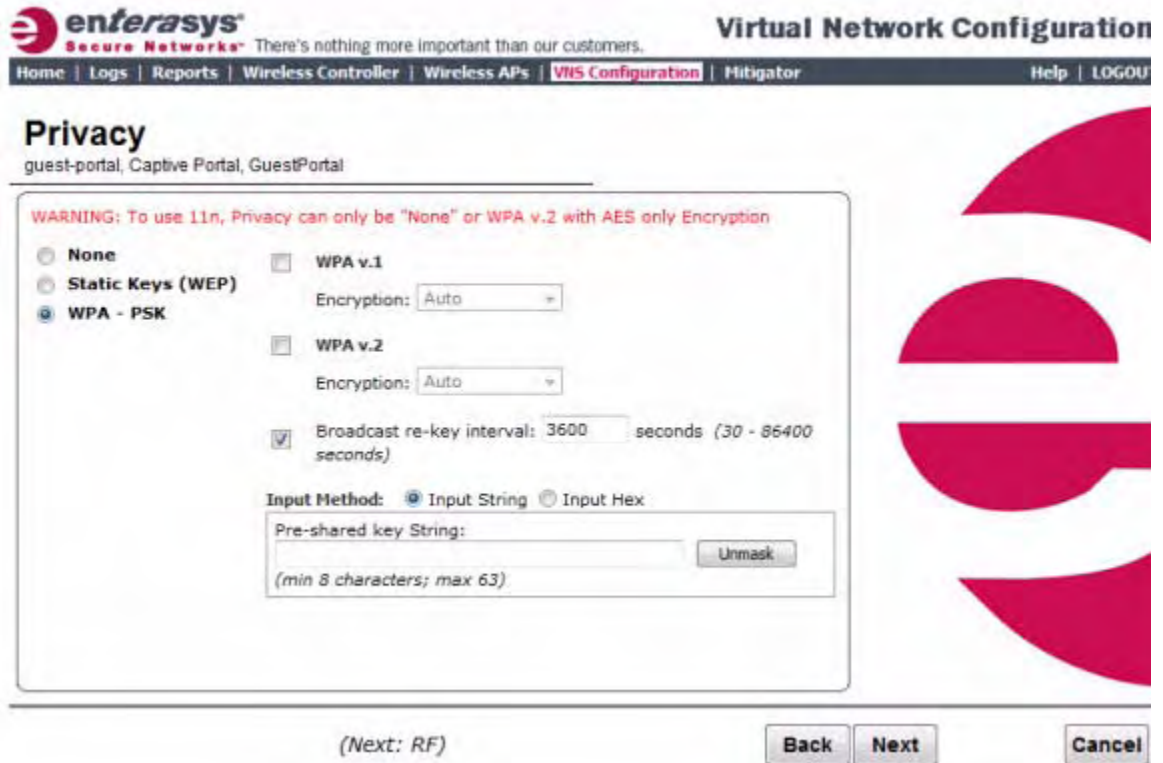
- To enable WPA v1 encryption, select **WPA v.1**. If WPA v.1 is enabled, click one of the following encryption types from the **Encryption** drop-down list:
 - **Auto** — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
 - **TKIP only** — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.
- To enable WPA v2-type encryption, select **WPA v.2**. The other options for this drop-down list are:
 - **Auto** — If you click **Auto**, the Wireless AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
 - **AES only** — If you click **AES**, the Wireless AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.
- To enable re-keying after a time interval, select **Broadcast re-key interval**. If this checkbox is not selected, the Broadcast encryption key is never changed and the Wireless AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.
- In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.
- To enable the group key power save retry, select **Group Key Power Save Retry**.



Note: The group key power save retry is only supported for AP36XX Wireless APs.

- In the **Pre-shared key** box, type the shared secret key to be used between the wireless device and Wireless AP. The shared secret key is used to generate the 256-bit key.
- **Mask/Unmask** — Click to display or hide your shared secret key.

17. Click **Next**. The **Radio Assignment** screen is displayed.



18. Configure the radio assignments:

- In the **AP Default Settings** section, select the radios of the AP default settings profile that you want to broadcast the VNS.
- In the **AP Selection** section, select the group of APs that will broadcast the VNS:
 - **all radios** – Click to assign all of the APs’ radios.
 - **radio 1** – Click to assign only the APs’ Radio 1.
 - **radio 2** – Click to assign only the APs’ Radio 2.
 - **local APs - all radios** – Click to assign only the local APs.
 - **local APs - radio 1** – Click to assign only the local APs’ Radio 1.
 - **local APs - radio 2** – Click to assign only the local APs’ Radio 2.
 - **foreign APs - all radios** – Click to assign only the foreign APs.
 - **foreign APs - radio 1** – Click to assign only the foreign APs’ Radio 1.
 - **foreign APs - radio 2** – Click to assign only the foreign APs’ Radio 2.
- If applicable, select the **WMM** checkbox. WMM (Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.

19. Click **Next**. The **Summary** screen is displayed.

enterasys
Secure Networks™ There's nothing more important than our customers.

Virtual Network Configuration

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

Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: guest-portal
- Category: Captive Portal
- SSID: guest-portal
- Type: GuestPortal
- Mode: Bridge Traffic Locally at HWC
- Interface: esa0
- IP Address: 192.168.1.1
- Mask: 255.255.255.0
- VLAN TAG: Tagged
- VLAN ID: 1

DHCP:

- DHCP Option: Local DHCP Server

Back Finish Cancel

20. Confirm your VNS configuration. To revise your configuration, click **Back**.

21. To create your VNS, click **Finish**, and then click **Close**.

If the Enterasys Wireless Controller is configured to be part of an availability pair, you can choose to synchronize the VNS on the secondary Enterasys Wireless Controller.

22. If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Enabling and Disabling a VNS

By default, when a new VNS is created, the VNS is added to the system as an enabled VNS. A VNS can be enabled or disabled. Disabling a VNS provides the ability to temporarily stop wireless service on a VNS. The disabled VNS configuration remains in the database for future use.

A Enterasys Wireless Controller can support the following VNSs:

Table 7-1 Enterasys Wireless Controller Active and Defined VNS Support

Platform	Active VNSs	Defined VNSs
C5110	128	256
C4110	64	128
C20	8	16
C25	16	32
V2110	48	64

To Enable or Disable a VNS:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **Virtual Networks** pane and select the VNS to enable or disable.
3. On the **Core** tab, in the Status box, select or de-select the **Enable** checkbox.
4. Click **Save**. The VNS is enabled or disabled accordingly.

Renaming a VNS

To Rename a VNS:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **Virtual Networks** pane, then select the VNS you want to rename.
3. On the **Core** tab, in the **VNS Name** field, enter the new name.
4. Click **Save**. The VNS is renamed.

Deleting a VNS

You can delete a VNS that is no longer necessary.

To delete a VNS:

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane expand the **Virtual Networks** pane, then select the VNS you want to rename.
3. On the **Core** tab, click the **Delete** button. A pop-up window prompts you to confirm you want to delete the VNS. Click **OK**.
4. Click **Save**. The VNS is deleted.

Configuring Classes of Service

This chapter describes classes of service configuration, including:

For information about...	Refer to page...
Classes of Service Overview	8-1
Configuring Classes of Service	8-1
CoS Rule Classification	8-4
Priority and ToS/DSCP Marking	8-5
Rate Limiting	8-6

Classes of Service Overview

In general, Class of Service (CoS) refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a station or port assigned to a specific policy is permitted. For more information on configuring policies, see “[Configuring VLAN and Class of Service for a Policy](#)” on page 5-1.

The CoS defines actions to be taken when rate limits are exceeded.

All incoming packets may follow these steps to determine a CoS:

- Classification - identifies the first matching rule that defines a CoS.
- Marking - modifies the L2 802.1p and/or L3 ToS based on CoS definition.
- Rate limiting (drop) is set.

The system limit for the number of CoS profiles on a controller is identical to the number of policies. For example, a C5110 can have 1024 policies and 1024 CoS profiles.

Configuring Classes of Service

The Classes of Service (CoS) feature is a configuration entity containing QoS Marking (802.1p and ToS/DSCP), Inbound/Outbound Rate Limiting and Transmit Queue Assignments. The CoS ToS marking capability allows for NAC-based redirection to different captive portals on the same WLAN Service.

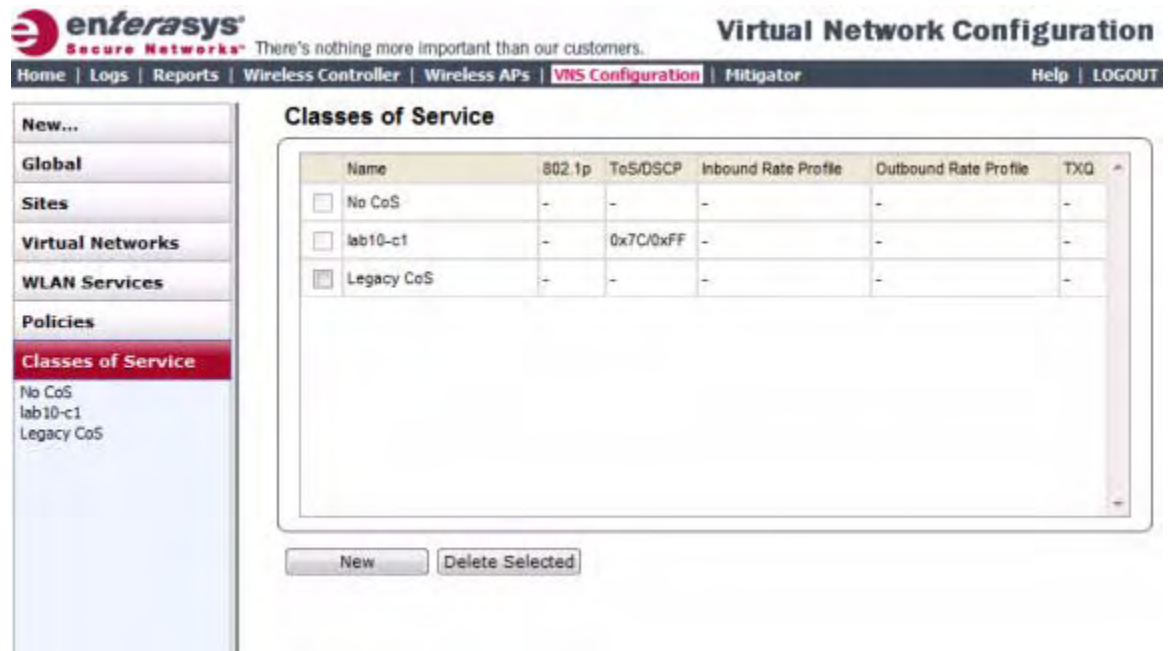
The supported CoS attributes are enforced on the Wireless Controller (data plane) and on the APs.

To configure Classes of Service:

1. From the top menu, click **VNS Configuration**.

The **Virtual Network Configuration** screen displays.

- In the left pane click Classes of Service.
The **Classes of Service** screen displays.



Note: "No CoS" means that the traffic to which it is assigned will not be remarked, the controller software will decide the appropriate transmit queue and no rate limits will be applied on traffic traveling to or from the station to which the CoS is applied. The "No CoS" CoS is predefined and cannot be removed.

- In the left pane, click the name of the Classes of Service that you want to edit, or click the **New** button to create a new CoS. The **Class of Service** configuration page displays. By default, the **General** tab displays. [Table 8-1](#) describes the fields and buttons on the General tab.

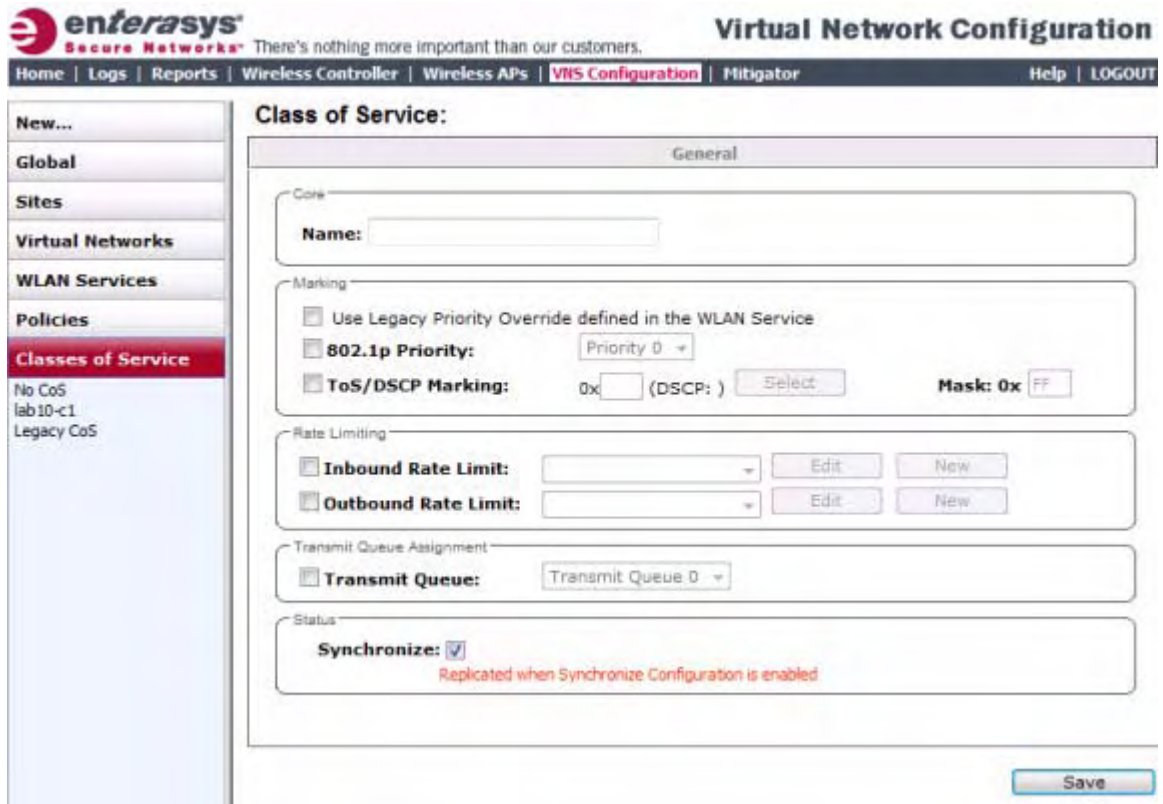


Table 8-1 General Tab - Fields and Buttons

Field/Button	Description
Core	
Name	Enter a name to assign to this class of service.
Marking	
Use Legacy Priority Override defined in the WLAN Service	Priority override allows you to define and force the traffic to a desired priority level. Priority override can be used with any combination. You can configure the service class and the DSCP values. Select this checkbox to use Priority Override defined in the WLAN as in previous releases. For more information, see Configuring the Priority Override .
802.1p Priority	Select this checkbox to define how the Layer 2 priority of the packet will be marked. From the drop-down list, select Priority 0 to Priority 7. For more information, see Priority and ToS/DSCP Marking . Note: This selection is not available if Legacy Priority Override is checked.
ToS/DSCP Marking	Select this checkbox to define how the Layer 3 ToS/DSCP will be marked. Enter a hexadecimal value in the 0x (DSCP:) field, or Click the Select button to open the ToS/DSCP Configuration dialog. For more information, see Configuring ToS/DSCP Marking . Note: This selection is not available if Legacy Priority Override is checked.

Table 8-1 General Tab - Fields and Buttons (continued)

Field/Button	Description
Mask: 0x	Displays the hexadecimal value to use for the ToS/DSCP value. For example, if the mask is 0xF0, then only the four most significant bits of the ToS of the received packets are marked. So, if the received ToS is 0x33 and the ToS marking is set to 0x2A, then the resulting ToS is 0x23.
Rate Limiting	
Inbound Rate Limit	Select this checkbox, and then select an inbound rate limit from the drop-down list or click the New button to create a new inbound rate limit profile. To edit an existing inbound rate limit profile, select the profile from the drop-down list and then click the Edit button. For more information, see Rate Limiting .
Outbound Rate Limit	Select this checkbox, and then select an outbound rate limit from the drop-down list or click the New button to create a new outbound rate limit profile. To edit an existing outbound rate limit profile, select the profile from the drop-down list and then click the Edit button. For more information, see Rate Limiting .
Transmit Queue Assignment	
Transmit Queue	Select this checkbox, and select a Transmit Queue from the drop-down list. The Transmit Queue assignment is an override to the default TXQ assignment specified in the 802.1p priority, but without remarking the actual 802.1p field.
Status	
Synchronize	Click to enable synchronization of this CoS to the peer controller in the availability pair.

CoS Rule Classification

Classification is the process of finding the first matching rule that defines a CoS for an incoming packet. The order of classification is as follows:

1. Use the CoS assigned by the first policy rule matched by the packet that explicitly assigns a CoS.
2. If no CoS found, use the default CoS of the Policy.
3. If still no CoS found, use the default CoS of the WLAN (for non-auth policy).

For inbound traffic, classification is done at the AP (if AP Filtering is enabled), otherwise it is done at the controller. For outbound traffic, classification is always done at the controller.

The Rule that assigns authorization (Access Control) may not be the same rule that assigns CoS. Therefore, up to two passes are made through the filter rules for each packet. If the first pass results in the packet being allowed a second pass will take place to classify the packet for CoS.

- The first pass looks for authorization (allow, deny)
- The second pass classifies and assigns the CoS.

The number of rules reported to Policy Manager are limited to the number of rules allowed on the controller. On the controller, a single rule can contain different classification types whereas for Policy Manager this rule may be split into several rules. For example, if a rule defines an IP source address and also a ToS value, then this rule would be split into an IP type and a ToS type. Rules exceeding the limit after splitting will be dropped.

Priority and ToS/DSCP Marking

After packets are classified, they are assigned a final User Priority (UP) value. The Priority and ToS/DSCP Marking bits to be applied to the packet is taken from the CoS and if not set, the received value (ToS/DSCP) is used. ToS/DSCP Marking rewrites the Layer 3 Type of Service (ToS) byte.

Configuring ToS/DSCP Marking

To configure ToS/DSCP Marking:

1. From the Class of Service General tab, click ToS/DSCP Marking.
2. Click the **Select** button. The ToS/DSCP Configuration dialog displays:



Note: Select either Type of Service (ToS) or Diffserv Codepoint (DSCP) from this dialog. You cannot configure both types.

3. Click Type of Service (ToS):
 - Select a Precedence value from the drop-down list,
 - Select a specific ToS from the following list:
 - Delay Sensitive
 - High Throughput
 - High Reliability
 - Explicit Congestion Notification
4. Click Diffserv Codepoint (DSCP):

- Select a Well-known Value or
 - Enter a Raw Binary Value.
5. Close the Configuration dialog.

The logic used to find the final UP depends on the CoS, the received UP, or the final ToS/DSCP value. Here are the steps followed to determine the final UP:

1. Use UP markings defined in CoS (directly or via Legacy UP override).
2. If still no UP, use UP from the received packet.
3. If still no UP, use DSCP marking defined in CoS and map to UP with WLANs DSCP-to-UP mapping table.
4. If still no UP, use received DSCP value and map to UP with WLANs DSCP-to-UP mapping table.

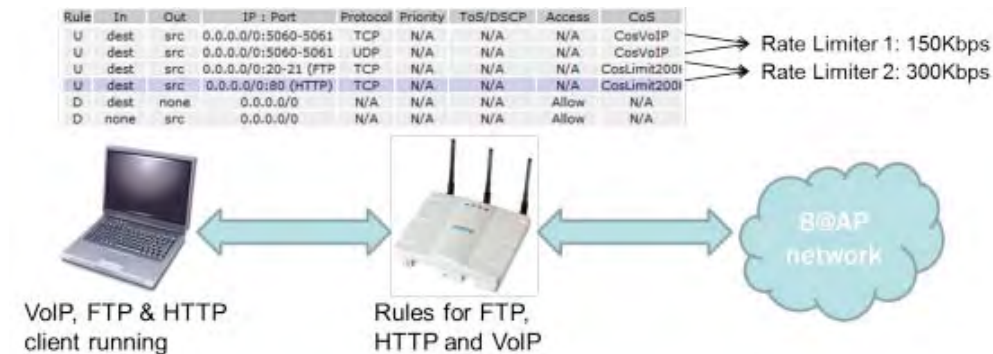
Rate Limiting

The Inbound and Outbound Rate Limit is enforced on a per-station basis whether the rate limit is assigned to a rule, policy or WLAN. Each station has its own set of counters that are used to monitor its wireless network utilization. Traffic from other stations never count against a station's rate limits.

- Controllers support up to 128 system wide rate profiles when managed from the controller.
- Each policy can use a maximum of 9 inbound rate profiles and 9 outbound rate profiles. For each direction there can be one rate profile assigned by the policy's default CoS and 8 other rate profiles assigned by the policy's rules.
- There is no limit to how many rules allow CoS assignments as long as there are never more than 8 + 8 rate profiles assigned by Classes of Service.

If two or more rules in the same policy assign the same named rate profile to a station's packets, then those rules "share" the rate profile. In [Figure 8-1](#), a policy's rules assign both HTTP and FTP traffic to the same rate limiter. The sum of the amounts of HTTP and FTP traffic determine whether the rate limit is being exceeded. Each station gets its own set of rate limiters. So the HTTP and FTP traffic of other stations never gets counted against a station's own rate profile limits.

Figure 8-1 Rate Limiter Example



Working with a Mesh Network

This chapter describes a Wireless Distribution System (Mesh), including:

For information about...	Refer to page...
About Mesh	9-1
Simple Mesh Configuration	9-2
Wireless Repeater Configuration	9-2
Wireless Bridge Configuration	9-3
Examples of Deployment	9-4
Mesh WLAN Services	9-4
Key Features of Mesh	9-7
Deploying the Mesh System	9-10
Changing the Pre-shared Key in a Mesh WLAN Service	9-15

About Mesh

Mesh networks enable you to expand the wireless network by interconnecting the Wireless APs through wireless links in addition to the traditional method of interconnecting Wireless APs via a wired network. In a Mesh deployment, each node not only captures and disseminates its own data, but it also serves as a relay for other nodes, that is, it collaborates to propagate the data in the network.

A Mesh deployment is ideally suited for locations where installing Ethernet cabling is too expensive, or physically impossible.

The Mesh network can be deployed in three configurations:

- Simple Mesh Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration



Note: Mesh is supported on all AP36xx models only, excluding the AP3605.

Simple Mesh Configuration

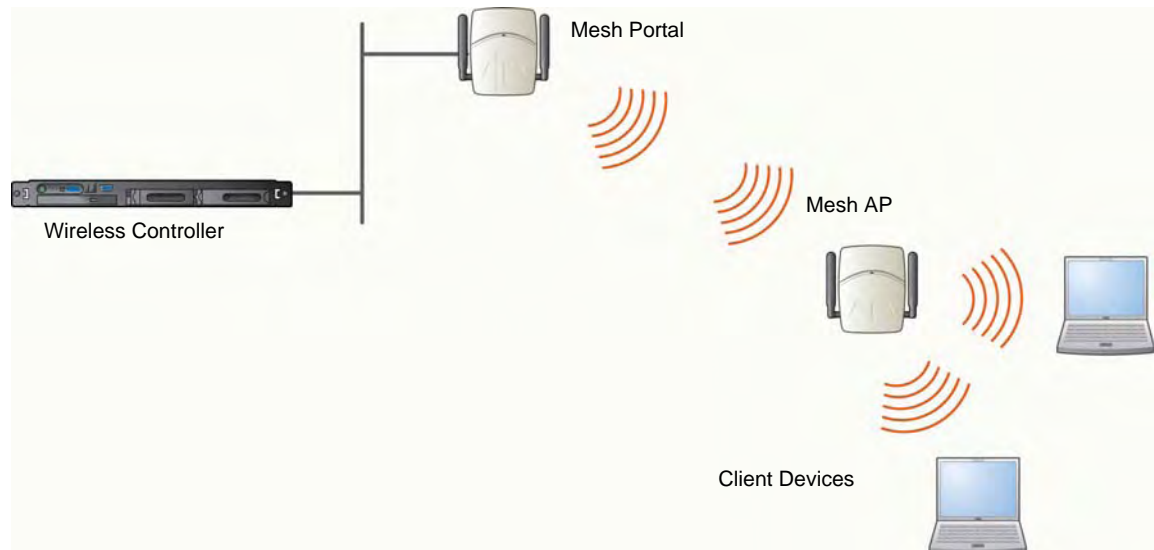
In a typical Mesh configuration, the Wireless APs are connected to the distribution system via an Ethernet network, which provides connectivity to the Enterasys Wireless Controller.

However, when a Wireless AP is installed in a remote location and can't be wired to the distribution system, an intermediate Wireless AP is connected to the distribution system via the Ethernet link. This intermediate Wireless AP forwards and receives the user traffic from the remote Wireless AP over a radio link.

The intermediate Wireless AP that is connected to the distribution system via the Ethernet network is called Mesh portal, and the Wireless AP that is remotely located is called the Mesh AP.

The following figure illustrates the Simple Mesh configuration:

Figure 9-1 Simple Mesh Configuration

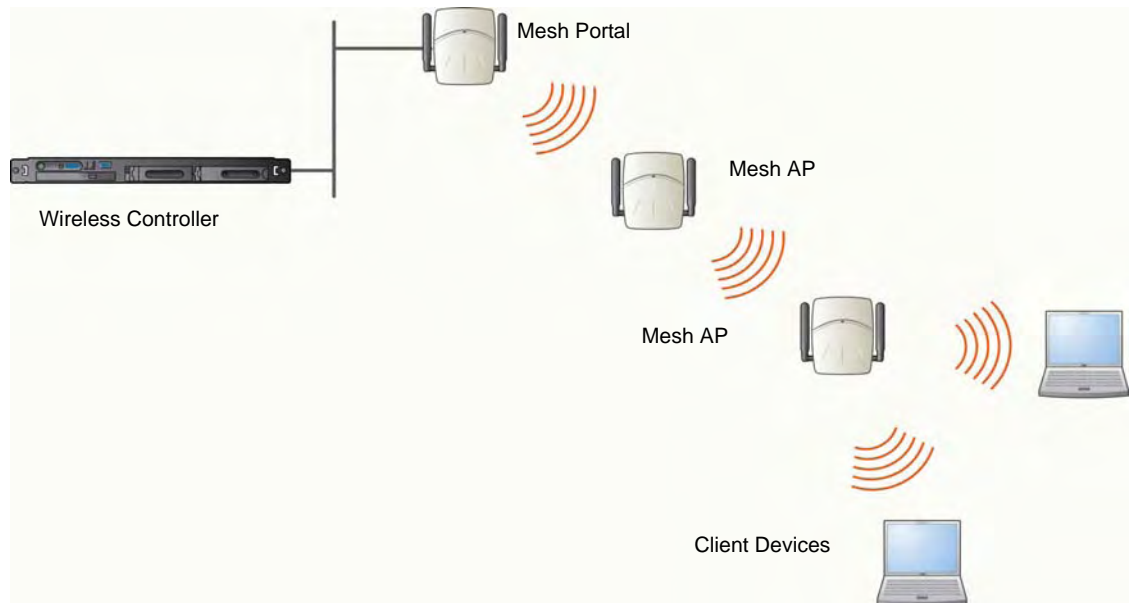


Wireless Repeater Configuration

In Wireless Repeater configuration, a Mesh AP is installed between the Mesh Portal and the destination Mesh AP. The Mesh AP relays the user traffic between the Mesh Portal and the destination Mesh AP. This increases the WLAN range.

The following figure illustrates the Wireless Repeater configuration:

Figure 9-2 Wireless Repeater Configuration

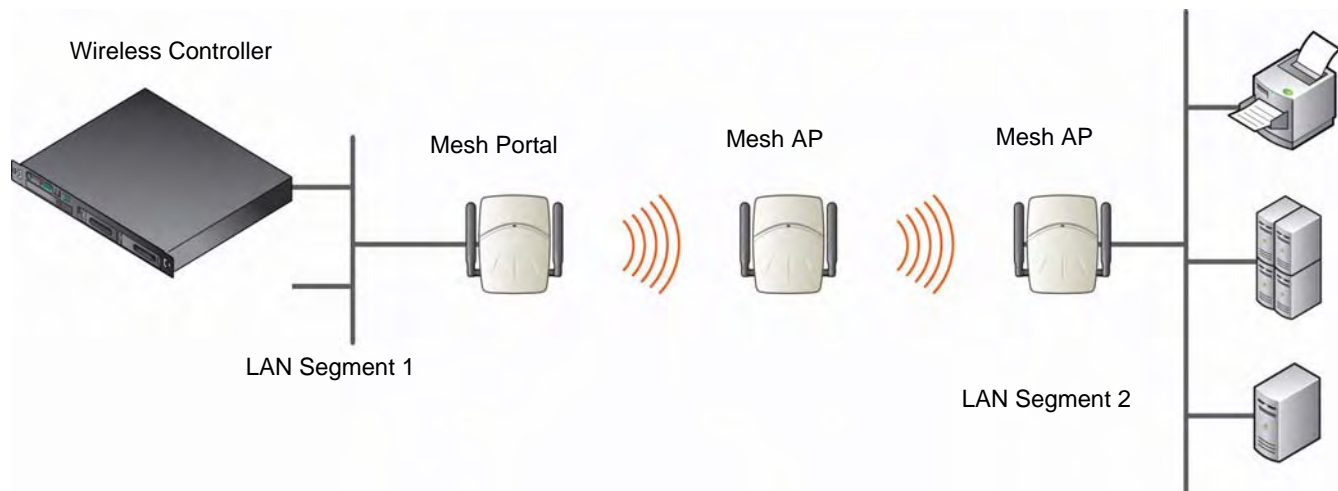


Note: You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge Configuration

In Wireless Bridge configuration, the traffic between two Wireless APs that are connected to two separate wired LAN segments is bridged via Mesh link. You may also install a Mesh AP between the two Wireless APs connected to two separate LAN segments.

Figure 9-3 Wireless Bridge Configuration

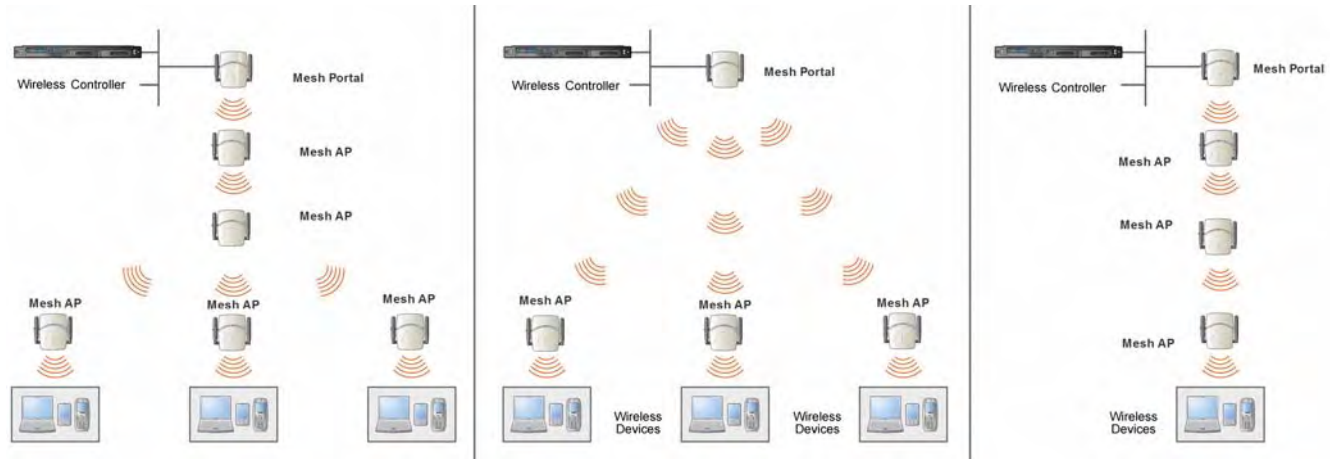


When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Mesh AP is connected to the wired LAN.

Examples of Deployment

The following illustration depicts a few examples of Mesh deployment.

Figure 9-4 Examples of Mesh Deployment



Mesh WLAN Services

In a traditional WLAN deployment, each radio of the Wireless AP can interact with the client devices on a maximum of eight networks.

In Mesh deployment, one of the radios of every Mesh Wireless AP establishes a Mesh link on an exclusive WLAN Service. The Mesh Wireless AP is therefore limited to seven network WLAN Services on the Mesh radio. The other radio can interact with the client-devices on a maximum of eight WLAN Services.

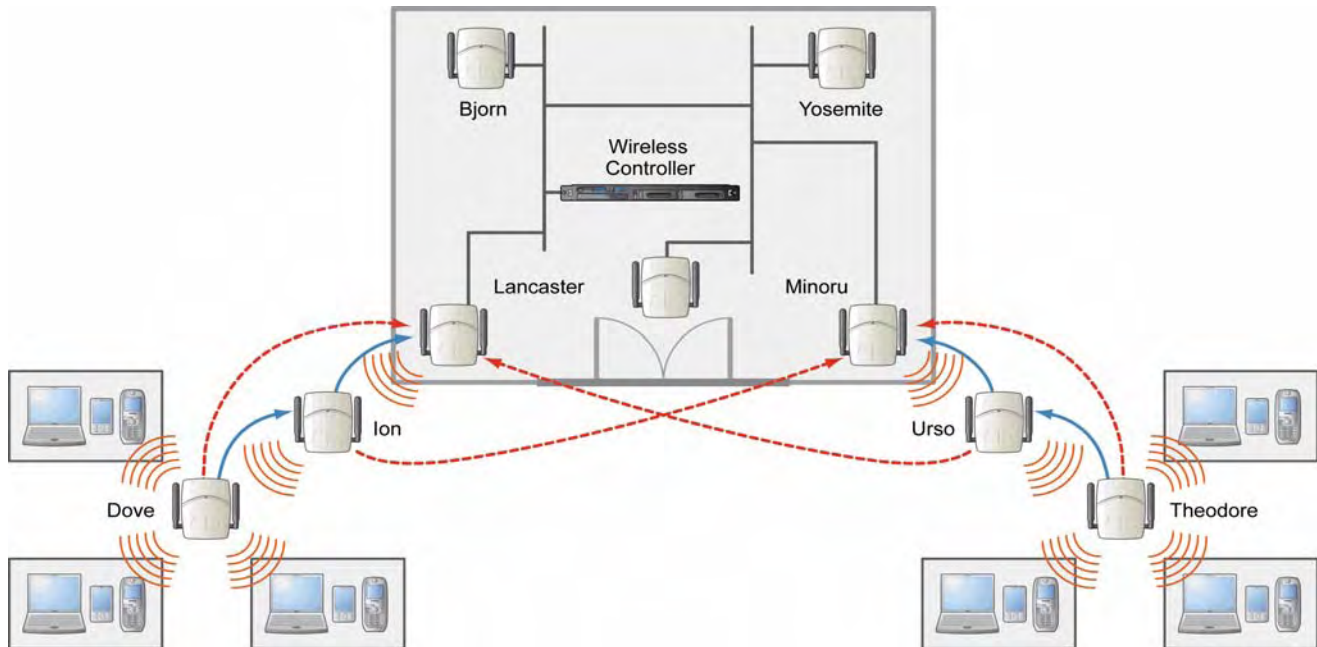
The WLAN Service on which the Wireless APs establish the Mesh link is called the Mesh WLAN Service.

A Mesh can be setup either by using either a single Mesh WLAN Service or multiple Mesh WLAN Services. The following figures illustrate the point.

In [Figure 9-5](#) on page 9-5:

- The rectangular enclosure denotes an office building.
- The four Wireless APs — Minoru, Yosemite, Bjorn and Lancaster — are within the confines of the building and are connected to the wired network.
- The space around the office building is a warehouse.
- The solid arrows point towards Current Parents.
- The dotted arrows point towards Alternative Parents.

Figure 9-5 Deployment Example

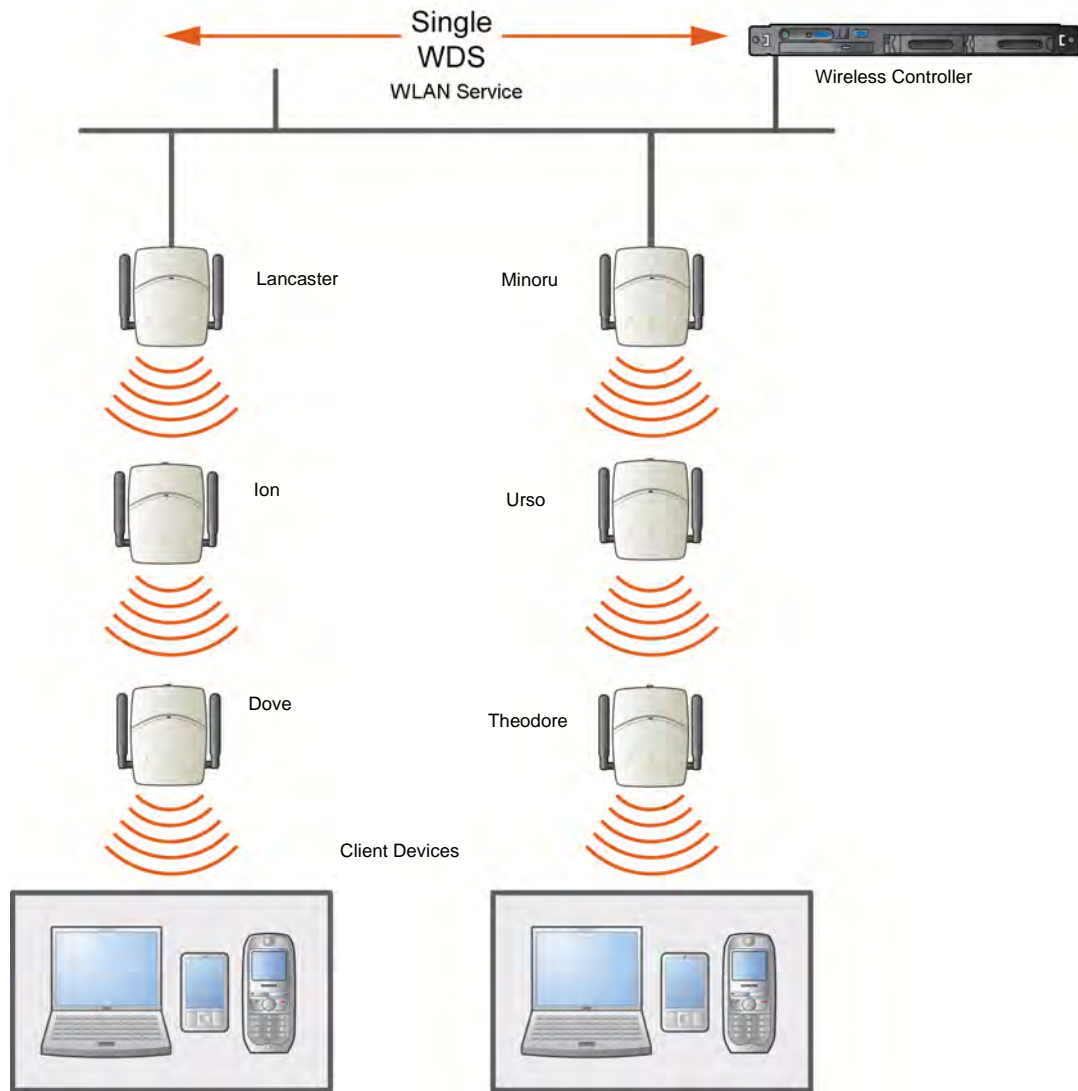


Mesh Setup with a Single Mesh WLAN Service

Deploying the Mesh for the above example using a single Mesh WLAN Service results in the following structure shown in [Figure 9-6](#) on page 9-6.

The tree will operate as a single Mesh entity. It will have a single Mesh SSID and a single pre-shared key for Mesh links. This tree will have multiple roots. For more information, see [“Multi-Root Mesh Topology”](#) on page 9-9.

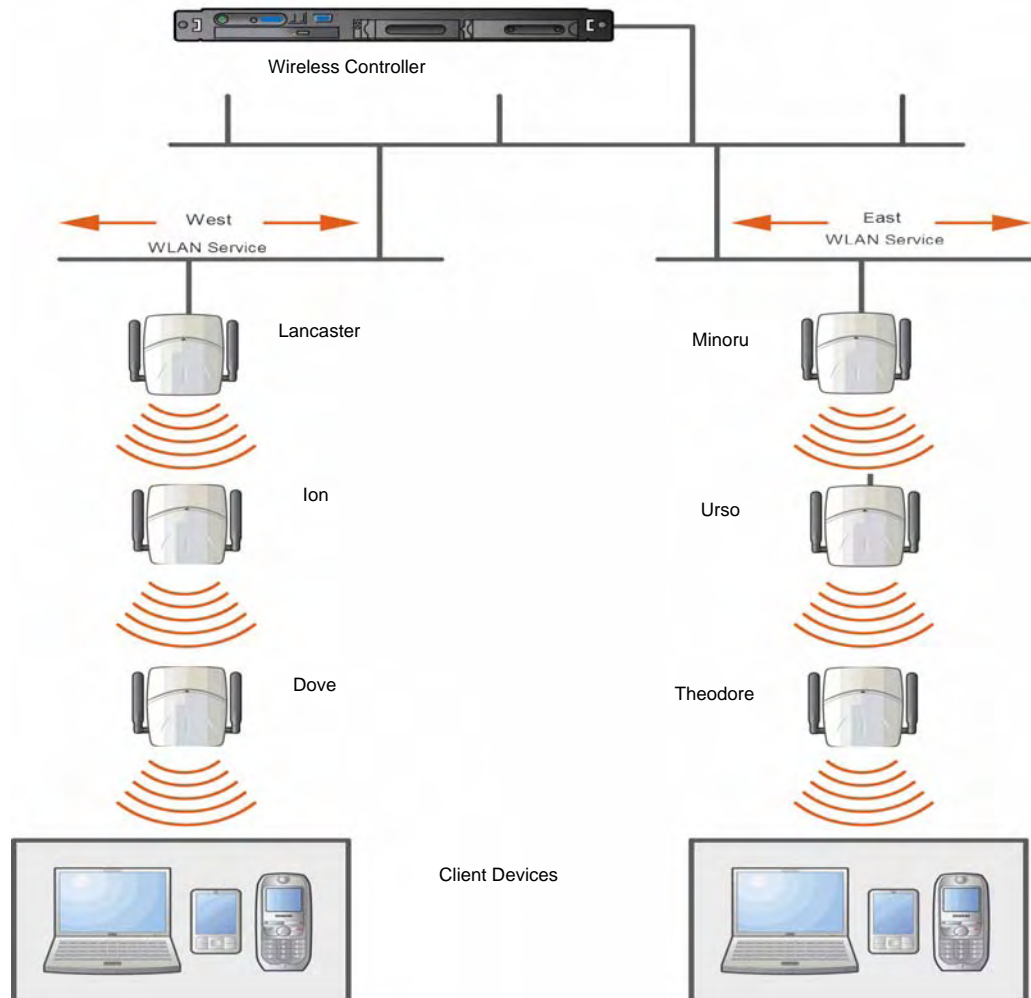
Figure 9-6 Mesh Setup with a Single Mesh WLAN Service



Mesh Setup with Multiple Mesh WLAN Services

You can also deploy the same Mesh in [Figure 9-5](#) using two Mesh WLAN Services. The Two Mesh WLAN Services will create two independent Mesh trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

Figure 9-7 Mesh Setup with Multiple Mesh WLAN Services



Key Features of Mesh

Some key features of Mesh are:

- [Self-Healing Network](#)
- [Tree-like Topology](#)
- [Radio Channels](#)
- [Multi-Root Mesh Topology](#)
- [Link Security](#)

Self-Healing Network

Data in a Mesh network propagates along a path, by hopping from node to node until the destination is reached. To ensure that all its paths' availability, the Mesh network allows for continuous connections and reconfiguration around broken or blocked paths, referred to as self-healing. The self-healing capability enables a routing based network to operate when one node breaks down or a connection goes bad.

Tree-like Topology

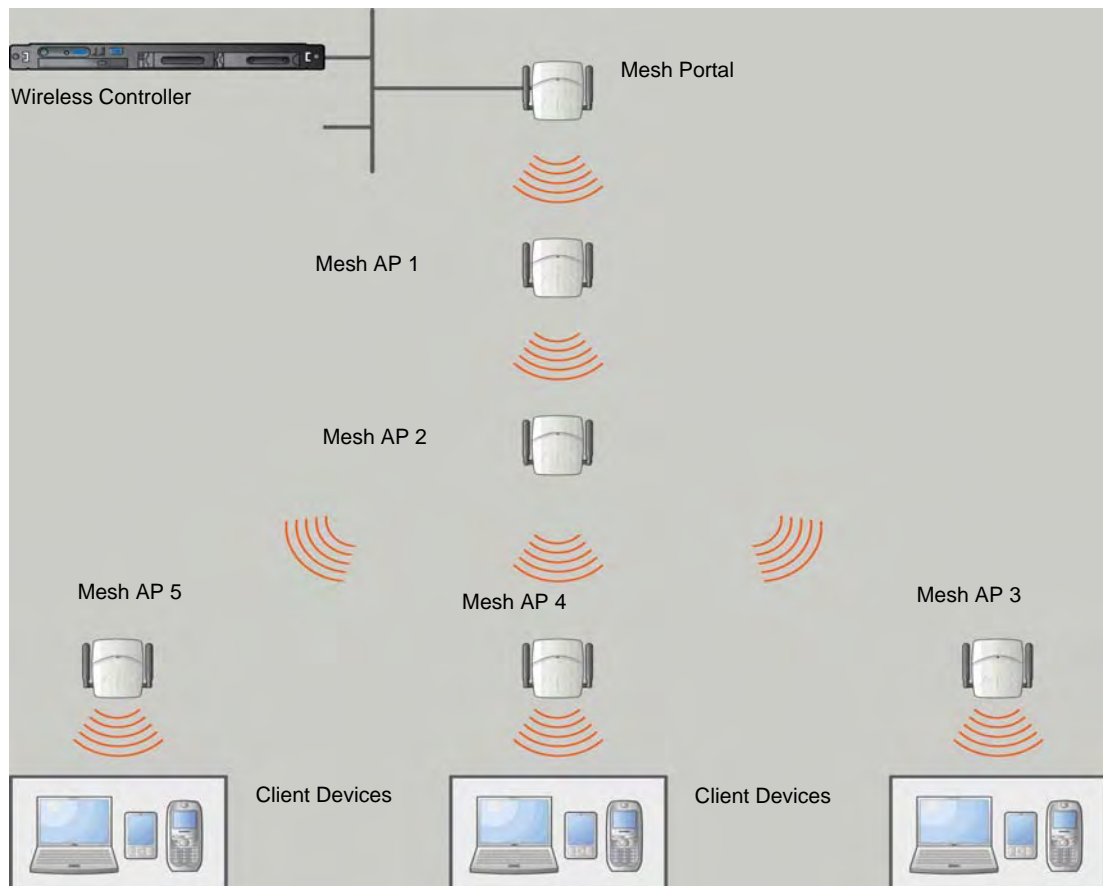
The Wireless APs in Mesh configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Mesh Portal being the tree root, and the Mesh AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The Mesh AP dynamically selects the best parent for connecting to the Mesh portal. A Mesh AP can have the role of both parent and child at the same time and the AP's role can change dynamically.

Figure 9-8 illustrates the parent-child relationship between the nodes in a Mesh topology.

- Mesh Portal is the parent of Mesh AP 1.
- Mesh AP 1 is the child of Mesh Portal.
- Mesh AP 1 is the parent of Mesh AP 2.
- Mesh AP 2 is the child of Mesh AP 1.
- Mesh AP 2 is the parent of the following Wireless APs:
 - Mesh AP 5
 - Mesh AP 4
 - Mesh AP 3
- All the three Mesh APs are the children of Mesh AP 2.

Figure 9-8 Parent-Child Relationship Between Wireless APs in Mesh Configuration





Note: Enterasys recommends that you limit the number of APs participating in a Mesh tree to 50. This limit guarantees decent performance in most typical situations.



Note: If a Wireless AP is configured to serve as a scanner in Mitigator, it cannot be used in a Mesh tree. For more information, see [Chapter 14, Working with the Mitigator](#).

Radio Channels

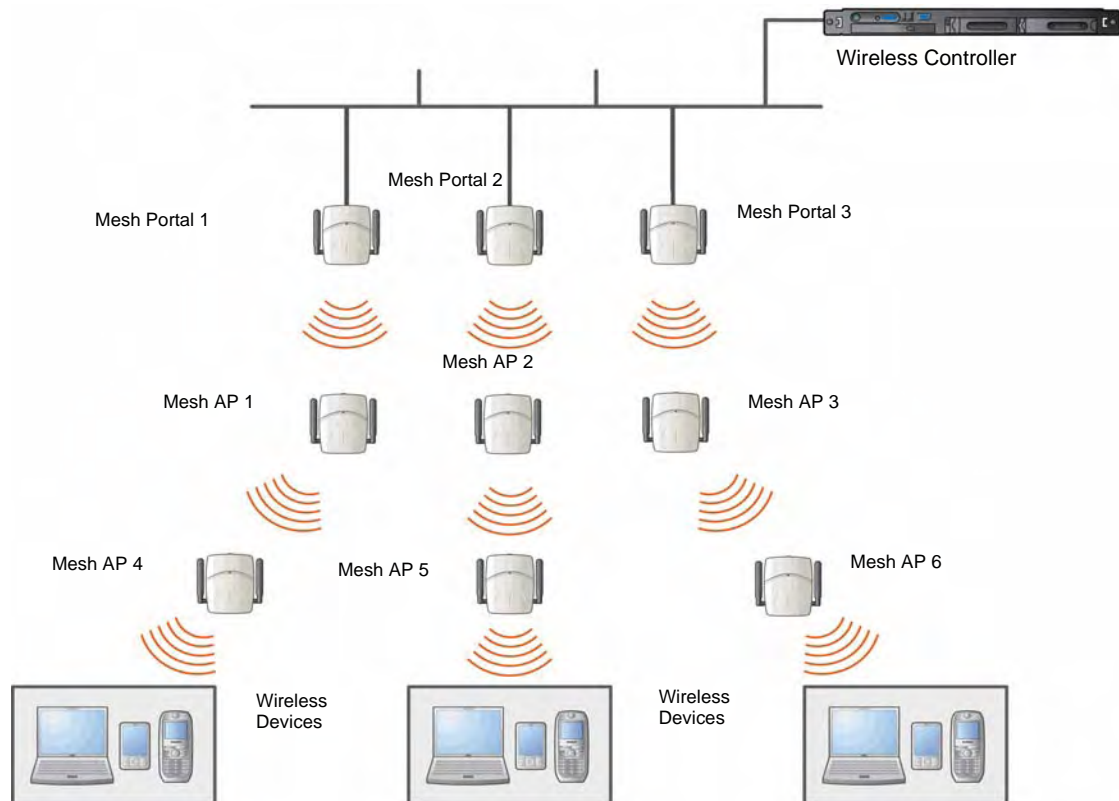
All APs in a mesh deployment must have Mesh configured on the same radio. On the backhaul radio, the following settings must be set the same way for all APs in the Mesh:

- Radio mode
- Minimum Basic Rate

Multi-Root Mesh Topology

A Mesh topology can have multiple Mesh Portals. [Figure 9-9](#) illustrates the multiple-root Mesh topology.

Figure 9-9 Multiple-Root Mesh Topology



Link Security

The Mesh link is encrypted using Advance Encryption Standard (AES).



Note: The keys for AES are configured prior to deploying the Repeater or Mesh APs.

Deploying the Mesh System

Before you start configuring the Mesh Wireless APs, you must ensure the following:

- The Wireless APs that are part of the wired WLAN are connected to the wired network.
- The wired Wireless APs that will serve as the Mesh Portal of the proposed Mesh topology are operating normally.
- The WLAN is operating normally.

Planning the Mesh Topology

You may sketch the proposed WLAN topology on paper before you start the Mesh deployment process. You should clearly identify the following in the sketch:

- Mesh Wireless APs with their names
- Radios that you will choose to link the Wireless APs

Provisioning the Mesh Wireless APs

This step is of crucial importance and involves connecting the Mesh Wireless APs to the enterprise network via the Ethernet link. This is done to enable the Mesh Wireless APs to connect to the Enterasys Wireless Controller so that they can derive their Mesh configuration.

The Mesh Wireless AP's configuration includes pre-shared key and its role, preferred parent name and the backup parent name.



Note: The provisioning of Mesh Wireless APs must be done before they are deployed at the target location. If the Wireless APs are not provisioned, they will not work at their target location.

Mesh Deployment Overview

The following is the high-level overview of the Mesh deployment process:

1. Connecting the Mesh Wireless APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the Enterasys Wireless Controller. For more information, see "[Discovery and Registration Overview](#)" on page 3-10.
2. Disconnecting the Mesh Wireless APs from the enterprise network after they have discovered and registered with the Enterasys Wireless Controller.
3. Creating a Mesh VNS.
4. Assigning roles, parents and backup parents to the Mesh Wireless APs.
5. Assigning the Mesh APs' radios to the network VNSs.
6. Connecting the Mesh Wireless APs to the enterprise network via the Ethernet link for provisioning. For more information, see "[Provisioning the Mesh Wireless APs](#)" on page 9-10.
7. Disconnecting the Mesh Wireless APs from the enterprise network and moving them to the target location.



Note: During the Mesh deployment process, the Mesh Wireless APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the Enterasys Wireless Controller, and then the second time to enable them to obtain the provisioning from the Enterasys Wireless Controller.

Connecting the Mesh Wireless APs to the Enterprise Network for Discovery and Registration

Connect each Mesh Wireless AP to the enterprise network to enable it to discover and register itself with the Enterasys Wireless Controller.



Note: Before you connect the Mesh Wireless APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the Enterasys Wireless Controller is defined according to your security needs. The **Security mode** property dictates how the Enterasys Wireless Controller behaves when registering new and unknown devices. For more information, see [“Defining Properties for the Discovery Process”](#) on page 3-26. If the **Security mode** is set to **Allow only approved Wireless APs to connect** (this is also known as secure mode), you must manually approve the Mesh Wireless APs after they are connected to the network for the discovery and registration. For more information, see [“Adding and Registering a Wireless AP Manually”](#) on page 3-28.

Depending upon the number of Ethernet ports available, you may connect one or more Mesh Wireless APs at a time, or you may connect all of them together.

Once a Mesh Wireless AP has discovered and registered itself with the Enterasys Wireless Controller, disconnect it from the enterprise network.

Configuring the Mesh Wireless APs Through the Enterasys Wireless Controller

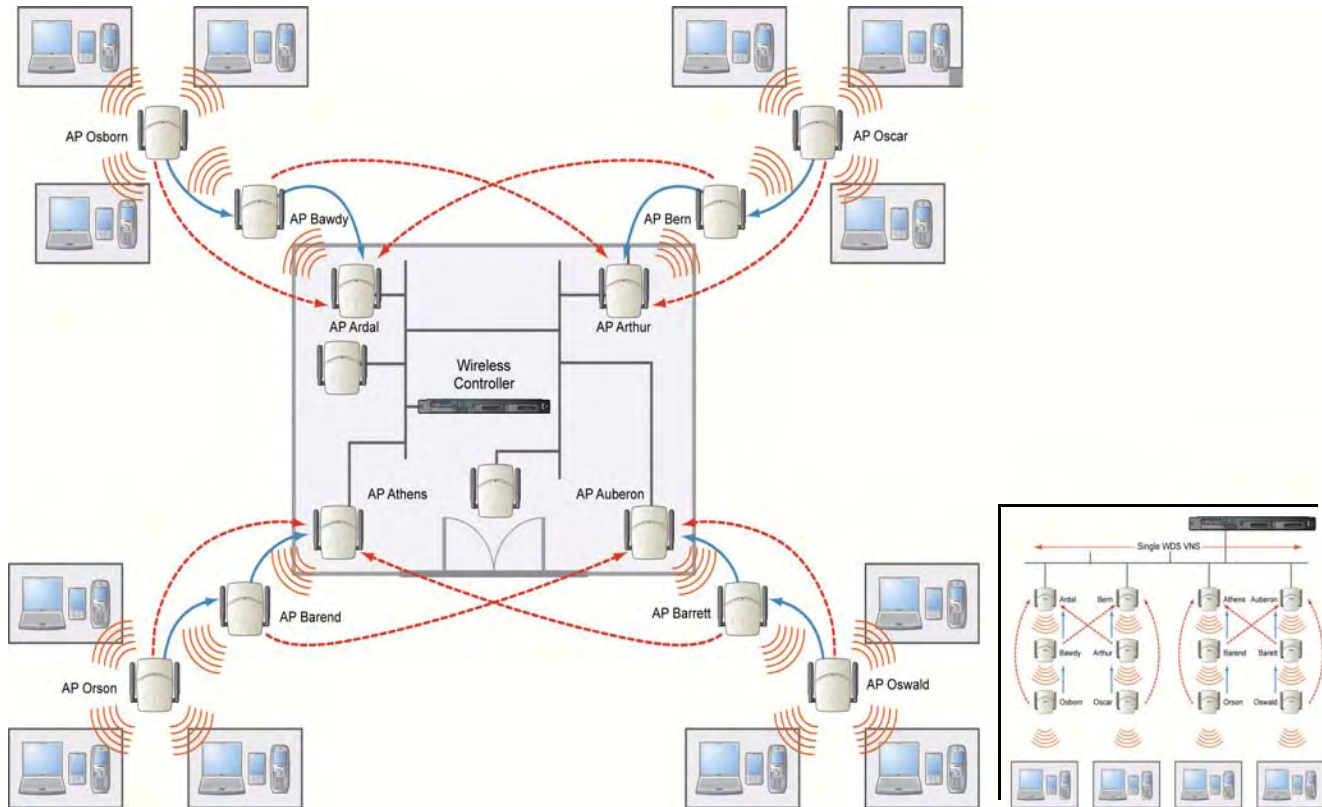
Configuring the Mesh Wireless APs involves the following steps:

1. Creating a Mesh WLAN Service.
2. Defining the SSID name and the pre-shared key.

For ease of understanding, the Mesh configuration process is explained with an example. [Figure 9-10](#) depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four Wireless APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the warehouse.
- The solid arrows point toward Current Parents.
- The dotted arrows point toward Alternative Parents.

Figure 9-10 Mesh Deployment



Note: With the single Mesh VNS, the tree structure for the Mesh deployment will be as depicted on the bottom right of [Figure 9-10](#). You can also implement the same deployment using four Mesh VNSs, each for a set of Wireless APs in the four corners of the building. Each set of Wireless APs will form an isolated topology and will operate using a separate **SSID** and a separate **Pre-shared** key. For more information, see [“Mesh WLAN Services”](#) on page 9-4.

To Configure the Mesh Wireless APs Through the Enterasys Wireless Controller:

Before configuring Mesh, be sure that the following conditions are met:

- Energy Save is set to Off
- Beacon Interval is set to 100 msec
- AP names are 32 characters or less for statistics display purposes
- ATPC and DCS are both disabled.

If possible, follow these guidelines for the backhaul radio to achieve a balance of stability, throughput, and latency:

- Use a 5.2 GHz band for backhaul
- Select a non-DFS channel for the Mesh Portal
- Use a 40 MHz Channel Width and Short guard interval
- Disable Aggregate MSDUs
- Enable Aggregate MPDUs
- Enable ADDBA support
- Configure the settings on the Radio configuration page the same for all APs in the Mesh.

- Set the Poll Timeout to be at least 60 seconds.
1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
 2. In the left pane, expand the **WLAN Services** pane and select a Mesh service to edit or click the **New** button.
 3. Enter a name for the service in the **Name** field.
 4. The **SSID** field is automatically filled in with the name, but you can change it if desired.
 5. For **Service Type**, select **Mesh**.

The screenshot displays the Enterasys Virtual Network Configuration interface. The top navigation bar includes the Enterasys logo, the tagline "Secure Networks. There's nothing more important than our customers.", and the title "Virtual Network Configuration". The navigation menu contains links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. A Help and LOGOUT link is also present.

The left sidebar shows a tree view of the configuration hierarchy: New..., Global, Virtual Networks, WLAN Services (selected), CNL-91-0-0, CNL-91-0-1, CNL-91-0-2, CNL-91-0-3, CNL-91-0-4, CNL-91-0-5-wds, CNL-91-0-6, CNL-91-WDS, Policies, Classes of Service, and Topologies.

The main content area is titled "WLAN:" and contains a "WLAN Services" section. The "Core" configuration box shows the following fields:

- Name:** Mesh_WLAN_Svc
- Service Type:** Radio buttons for Standard, WDS, Mesh (selected), Third Party AP, and Remote.
- SSID:** Mesh_WLAN_Svc

Below the Core configuration is a "Status" section with an "Enable:" checkbox that is checked.

A "Save" button is located at the bottom right of the configuration area.

- To save your changes, click **Save**. The WLAN configuration window is re-displayed to show additional configuration fields.

enterasys
Secure Networks® There's nothing more important than our customers.

Virtual Network Configuration

Home | Logs | Reports | Wireless Controller | Wireless APs | **WNS Configuration** | Mitigator | Help | LOGOUT

New...

Global

Virtual Networks

WLAN Services

CNL-91-0-0
CNL-91-0-1
CNL-91-0-2
CNL-91-0-3
CNL-91-0-4
CNL-91-0-5-wds
CNL-91-0-6
CNL-91-WDS
Mesh_WLAN_Svc

Policies

Classes of Service

Topologies

WLAN: Mesh_WLAN_Svc

WLAN Services

Core

Name: Mesh_WLAN_Svc

Service Type: Mesh

SSID: Mesh_WLAN_Svc

Mesh Settings

Pre-shared Key:

Backhaul Radio: a (5 GHz)

Status

Enable:

Wireless APs services

AP Name	Mesh Service	Bridge to LAN	Radio #
70000000000000111	none	<input type="checkbox"/>	1

New Delete Save

- In the **Mesh Pre-shared Key** box, type the key.



Note: The pre-shared key must be 8 to 63 characters long. The Mesh Wireless APs use this pre-shared key to establish a Mesh link between them.



Note: Changing the pre-shared key after the Mesh is deployed can be a lengthy process. For more information, see [“Changing the Pre-shared Key in a Mesh WLAN Service”](#) on page 9-15.

- Assign a backhaul radio.



Note: After you save the configuration, you cannot change the backhaul radio. Please configure this setting wisely.

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



Note: The **Mesh Bridge** feature on the user interface relates to Mesh Bridge configuration. When you are configuring the Mesh Bridge topology, you must select **Mesh Bridge** for Mesh AP that is connected to the wired network. For more information, see [“Wireless Bridge Configuration”](#) on page 9-3.

Connecting the Mesh Wireless APs to the Enterprise Network for Provisioning

You must connect the Mesh Wireless APs to the enterprise network once more to enable them to obtain their configuration from the Enterasys Wireless Controller. The configuration includes the pre-shared key, the Wireless AP's role, preferred parent and backup parent. For more information, see [Provisioning the Mesh Wireless APs](#) on 9-10.



Warning: If you skip this step, the Mesh Wireless APs will not work at their target location.

Moving the Mesh Wireless APs to the Target Location

1. Disconnect the Mesh Wireless APs from the enterprise network, and move them to the target location.
2. Install the Mesh Wireless APs at the target location.
3. Connect the Wireless APs to a power source. The discovery and registration processes are initiated.



Note: If you change any of the following radio properties of a Mesh Wireless AP, the Mesh Wireless AP will reject the change:

- Disabling the radio on which the Mesh link is established
- Changing the radio's Tx Power of a radio on which the Mesh link is established
- Changing the country

Changing the Pre-shared Key in a Mesh WLAN Service

To Change the Pre-shared Key in a Mesh WLAN Service

1. Create a new Mesh WLAN Service with a new pre-shared key.
2. Assign the RF of the Wireless APs from the old Mesh to the new Mesh WLAN Service.
3. Wait at least 30 seconds to ensure that all APs got the configuration, then disable the old Mesh WLAN service.
4. Check the **Mesh Statistics** report page to ensure that all the Mesh Wireless APs have connected to the Enterasys Wireless Controller via the new Mesh VNS. For more information, see "[Viewing Statistics for Wireless APs](#)" on page 15-4.
5. Delete the old Mesh WLAN Service. For more information, see "[Deleting a VNS](#)" on page 7-48.

Working with a Wireless Distribution System

This chapter describes a Wireless Distribution System (WDS), including:

For information about...	Refer to page...
About WDS	10-1
Simple WDS Configuration	10-2
Wireless Repeater Configuration	10-2
Wireless Bridge Configuration	10-3
Examples of Deployment	10-4
WDS WLAN Services	10-4
Key Features of WDS	10-7
Deploying the WDS System	10-11
Changing the Pre-shared Key in a WDS WLAN Service	10-19

About WDS

The Wireless Distribution System (WDS) enable you to expand the wireless network by interconnecting the Wireless APs through wireless links in addition to the traditional method of interconnecting Wireless APs via a wired network.



Note: The Scalance AP W788-2 and AP2605 do not support WDS.

A WDS deployment is ideally suited for locations, where installing Ethernet cabling is too expensive, or physically impossible.

The WDS can be deployed in three configurations:

- Simple WDS Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

Simple WDS Configuration

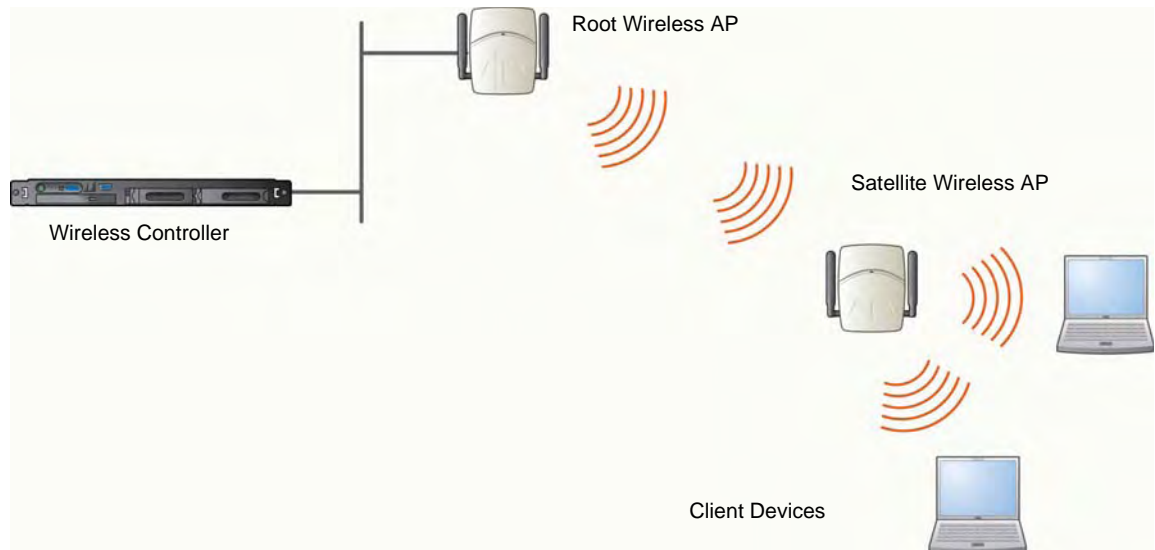
In a typical WDS configuration, the Wireless APs are connected to the distribution system via an Ethernet network, which provides connectivity to the Enterasys Wireless Controller.

However, when a Wireless AP is installed in a remote location and can't be wired to the distribution system, an intermediate Wireless AP is connected to the distribution system via the Ethernet link. This intermediate Wireless AP forwards and receives the user traffic from the remote Wireless AP over a radio link.

The intermediate Wireless AP that is connected to the distribution system via the Ethernet network is called Root AP, and the Wireless AP that is remotely located is called the Satellite AP.

The following figure illustrates the Simple WDS configuration:

Figure 10-1 Simple WDS Configuration

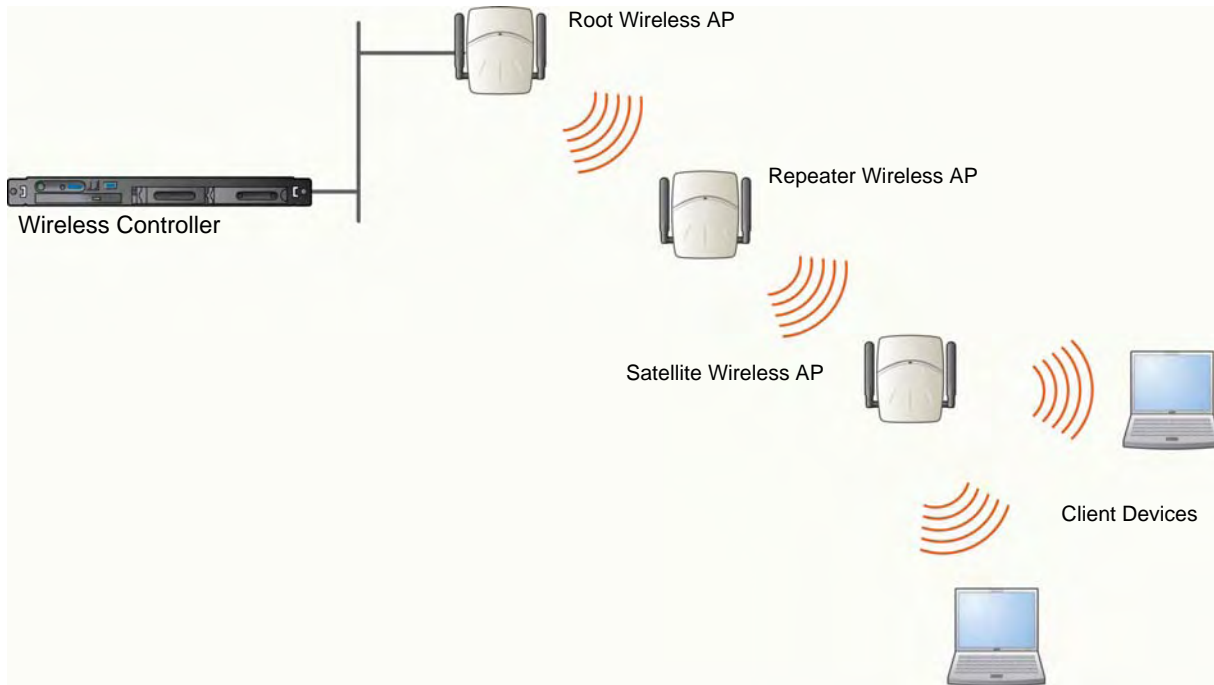


Wireless Repeater Configuration

In Wireless Repeater configuration, a Repeater Wireless AP is installed between the Root Wireless AP and the Satellite Wireless AP. The Repeater Wireless AP relays the user traffic between the Root Wireless AP and the Satellite Wireless AP. This increases the WLAN range.

The following figure illustrates the Wireless Repeater configuration:

Figure 10-2 Wireless Repeater Configuration

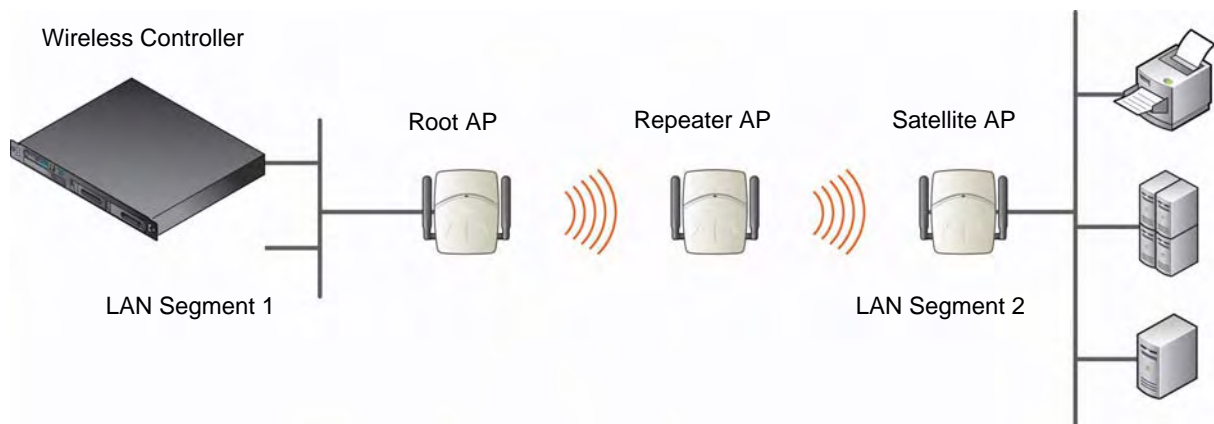


Note: You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge Configuration

In Wireless Bridge configuration, the traffic between two Wireless APs that are connected to two separate wired LAN segments is bridged via WDS link. You may also install a Repeater Wireless AP between the two Wireless APs connected to two separate LAN segments.

Figure 10-3 Wireless Bridge Configuration

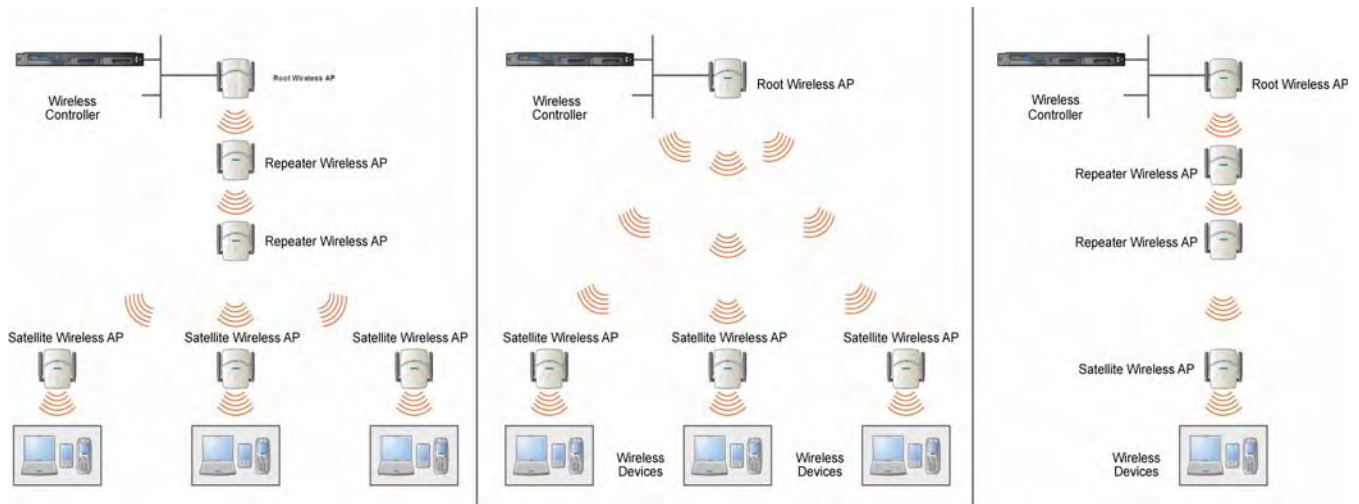


When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Satellite AP is connected to the wired LAN.

Examples of Deployment

The following illustration depicts a few examples of WDS deployment.

Figure 10-4 Examples of WDS Deployment



WDS WLAN Services

In a traditional WLAN deployment, each radio of the Wireless AP can interact with the client devices on a maximum of eight networks.

In WDS deployment, one of the radios of every WDS Wireless AP establishes a WDS link on an exclusive WLAN Service. The WDS Wireless AP is therefore limited to seven network WLAN Services on the WDS radio. The other radio can interact with the client-devices on a maximum of eight WLAN Services.



Note: The Root Wireless AP and the Repeater Wireless APs can also be configured to interact with the client-devices. For more information, see “[Assigning the Satellite Wireless APs’ Radios to the Network WLAN Services](#)” on page 10-17.

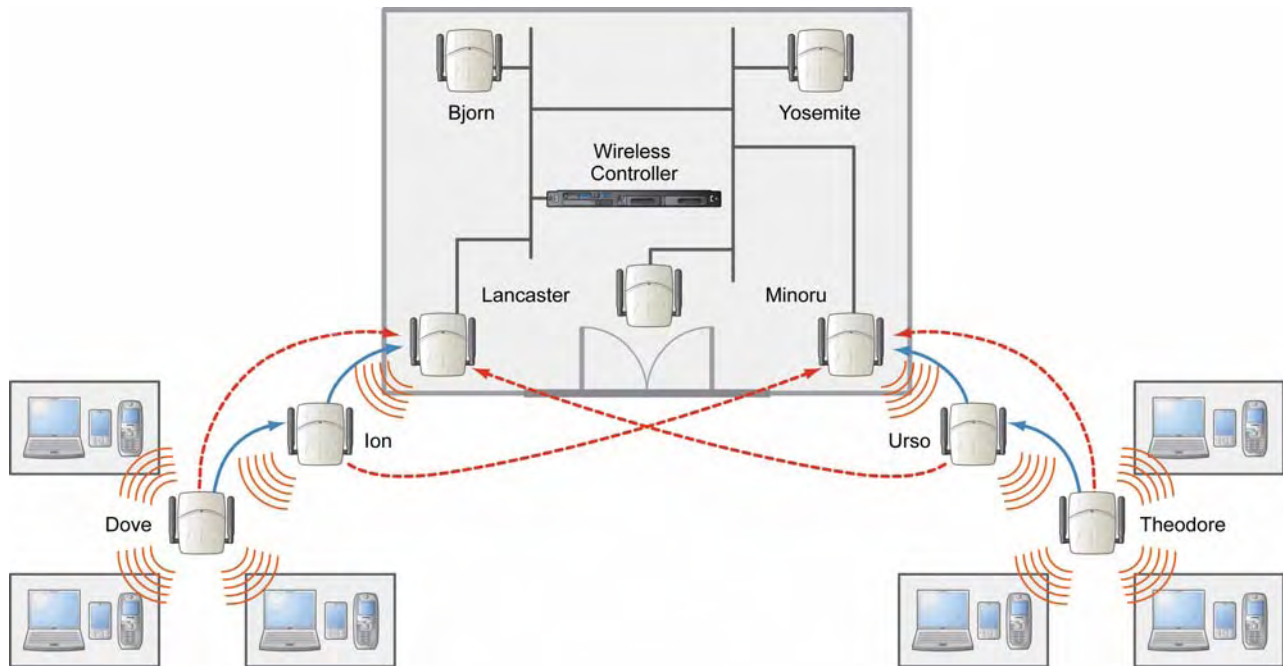
The WLAN Service on which the Wireless APs establish the WDS link is called the WDS WLAN Service.

A WDS can be setup either by using either a single WDS WLAN Service or multiple WDS WLAN Services. The following figures illustrate the point.

Figure 10-5 on page 10-5:

- The rectangular enclosure denotes an office building.
- The four Wireless APs — Minoru, Yosemite, Bjorn and Lancaster — are within the confines of the building and are connected to the wired network.
- The space around the office building is a ware house.
- The solid arrows point towards Preferred Parents.
- The dotted arrows point towards Backup Parents.

Figure 10-5 Deployment Example

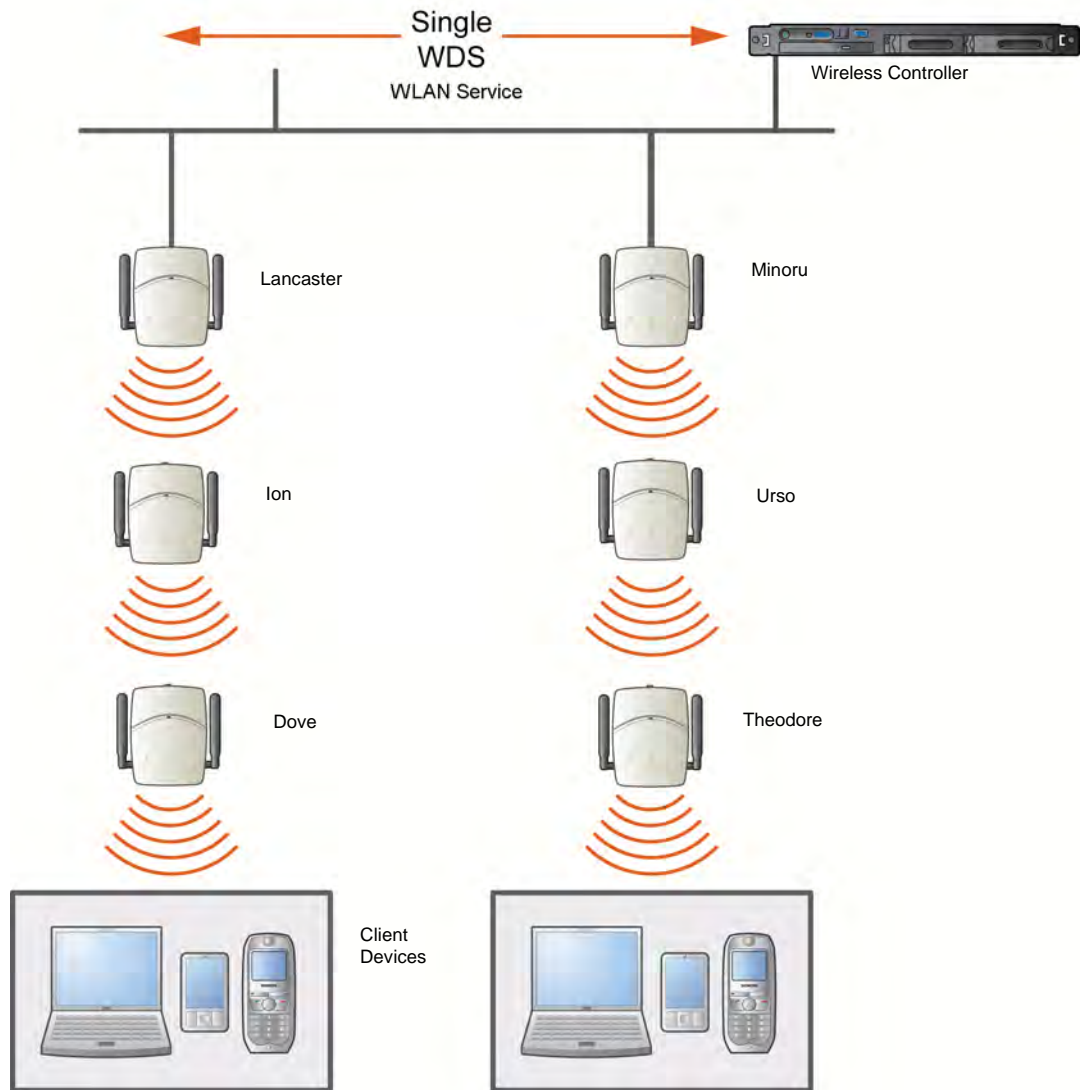


WDS Setup with a Single WDS WLAN Service

Deploying the WDS for the above example using a single WDS WLAN Service results in the following structure.

The tree will operate as a single WDS entity. It will have a single WDS SSID and a single pre-shared key for WDS links. This tree will have multiple roots. For more information, see [“Multi-Root WDS Topology”](#) on page 10-9.

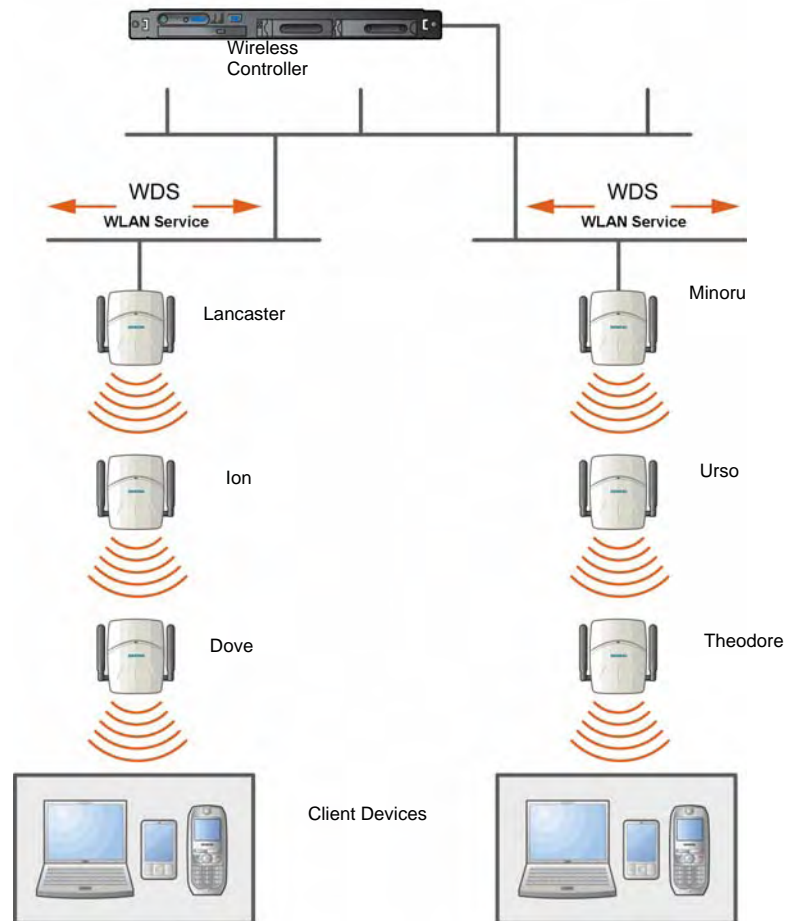
Figure 10-6 WDS Setup with a Single WDS WLAN Service



WDS Setup with Multiple WDS WLAN Services

You can also deploy the same WDS in [Figure 10-5](#) using two WDS WLAN Services. The Two WDS WLAN Services will create two independent WDS trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

Figure 10-7 WDS Setup with Multiple WDS WLAN Services



Key Features of WDS

Some key features of WDS are:

- [Tree-like Topology](#)
- [Radio Channels](#)
- [Multi-Root WDS Topology](#)
- [Automatic Discovery of Parent and Backup Parent Wireless APs](#)
- [Link Security](#)

Tree-like Topology

The Wireless APs in WDS configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Root Wireless AP being the tree root, and the Satellite Wireless AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The Wireless AP that provides the WDS service to the other Wireless APs in the downstream direction is a parent. The Wireless APs that establish a link with the Wireless AP in the upstream direction for WDS service are children.

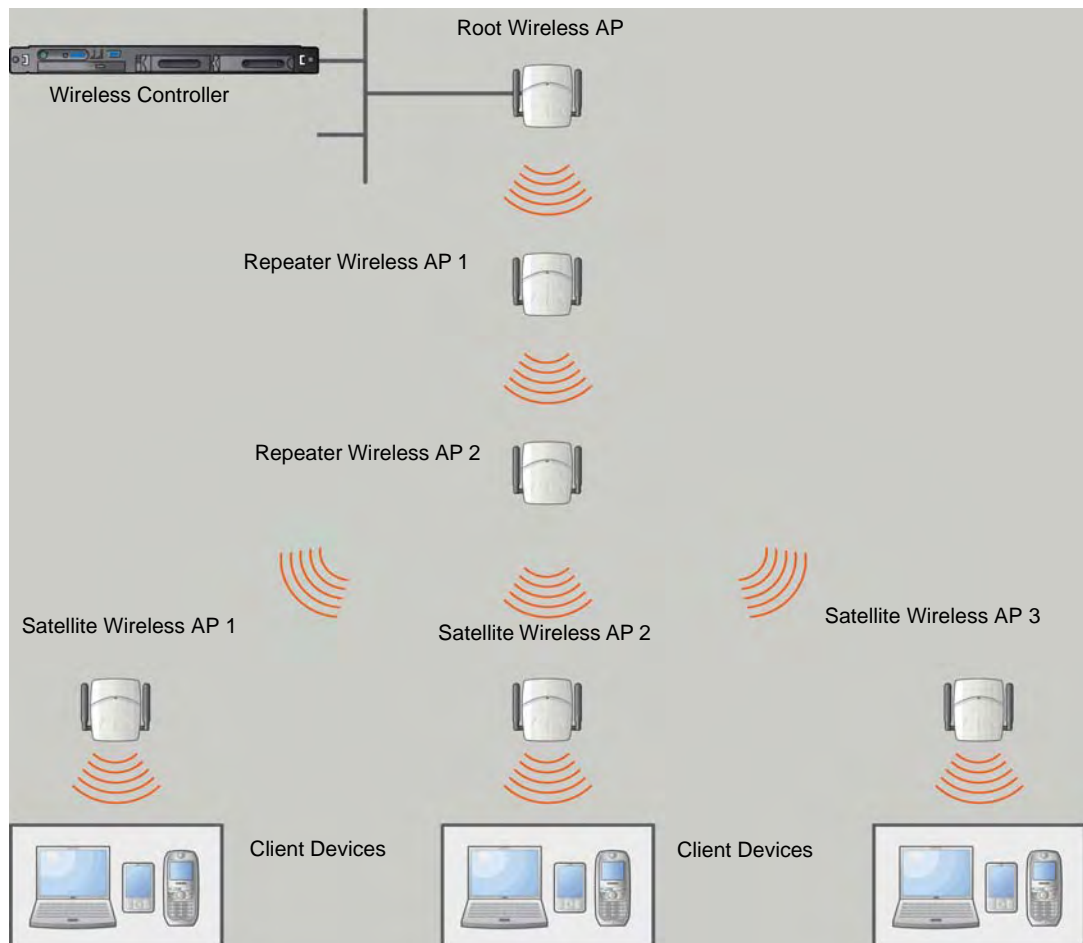


Note: If a parent Wireless AP fails or stops to act a parent, the children Wireless APs will attempt to discover their backup parents. If the backup parents are not defined, the children Wireless APs will be left stranded.

The following figure illustrates the parent-child relationship between the nodes in a WDS topology. In [Figure 10-8](#):

- Root Wireless AP is the parent of Repeater Wireless AP 1.
- Repeater Wireless AP 1 is the child of Root Wireless AP.
- Repeater Wireless AP 1 is the parent of Repeater Wireless AP 2.
- Repeater Wireless AP 2 is the child of Repeater Wireless AP 1.
- Repeater Wireless AP 2 is the parent of the following Wireless APs:
 - Satellite Wireless AP 1
 - Satellite Wireless AP 2
 - Satellite Wireless AP 3
- All the three Satellite APs are the children of Repeater Wireless AP 2.

Figure 10-8 Parent-Child Relationship Between Wireless APs in WDS Configuration



The WDS system enables you to configure the Wireless AP's role — **parent**, **child** or **both** — from the Enterasys Wireless Controller's interface. If the WDS Wireless AP will be serving as a parent and a child in a given topology, its role is configured as **both**.



Note: Enterasys recommends that you limit the number of APs participating in a WDS tree to 8. This limit guarantees decent performance in most typical situations.



Note: If a Wireless AP is configured to serve as a scanner in Mitigator, it cannot be used in a WDS tree. For more information, see [Chapter 14, Working with the Mitigator](#).

Radio Channels

The radio channel on which the child Wireless AP operates is determined by the parent Wireless AP.

A Wireless AP may connect to its parent Wireless AP and children Wireless APs on the same radio, or on different radios. Similarly, a Wireless AP can have two children operating on two different radios.

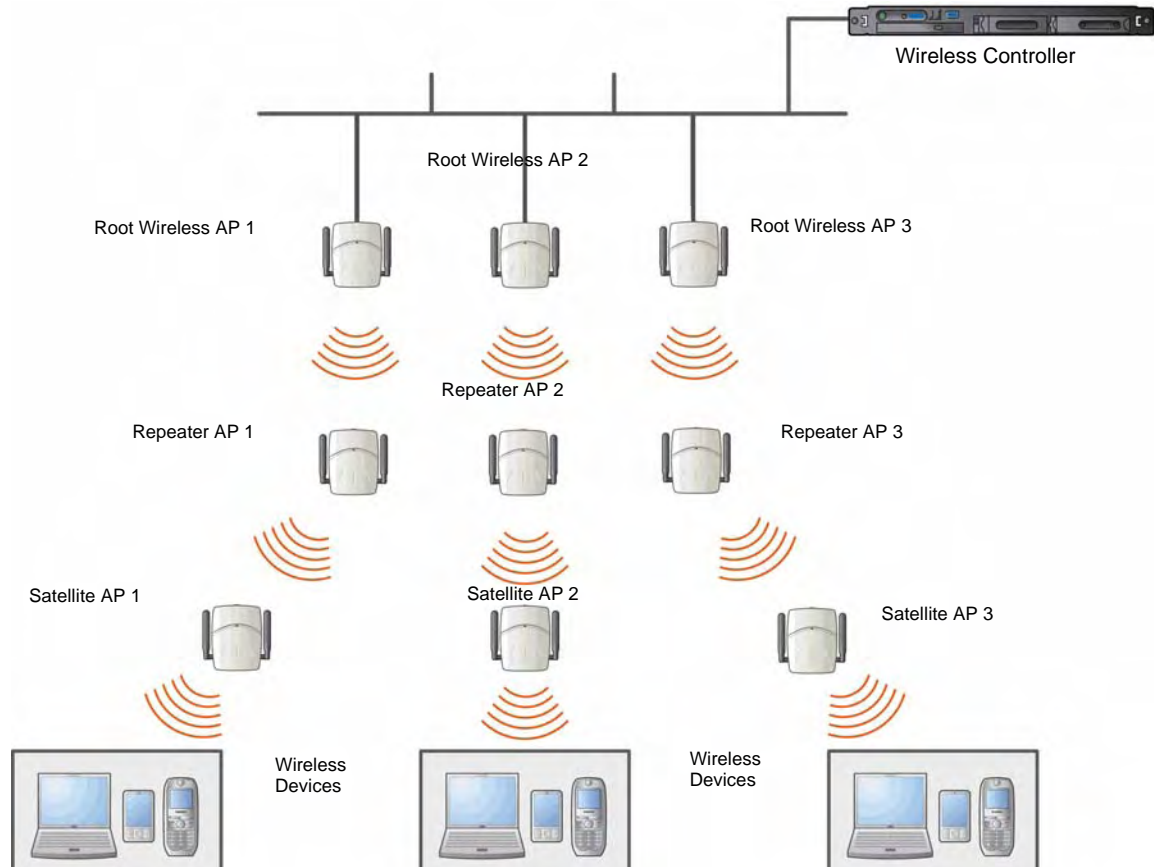


Note: When a Wireless AP is connecting to its parent Wireless AP and children APs on the same radio, it uses the same channel for both the connections.

Multi-Root WDS Topology

A WDS topology can have multiple Root Wireless APs. [Figure 10-9](#) illustrates the multiple-root WDS topology.

Figure 10-9 Multiple-root WDS Topology



Automatic Discovery of Parent and Backup Parent Wireless APs

The children Wireless APs, including the Repeater Wireless AP and the Satellite Wireless APs, scan for their respective parents at a startup.

You can manually configure a parent and backup parent for the children Wireless APs or you can enable the children Wireless APs to automatically select the best parent out of all of the available APs. If you choose automatic parent Wireless AP selection, a child Wireless AP selects a parent Wireless AP based on its received signal strength and the number of hops to the root Wireless AP. After a parent Wireless AP and backup parent Wireless AP is selected, the Wireless controller will first try to negotiate a WDS link with the parent Wireless controller. If the WDS link negotiation is unsuccessful, the Wireless controller will try to negotiate a link with the backup parent.

Link Security

The WDS link is encrypted using Advance Encryption Standard (AES).



Note: The keys for AES are configured prior to deploying the Repeater or Satellite Wireless APs.

Deploying the WDS System

Before you start configuring the WDS Wireless APs, you must ensure the following:

- The Wireless APs that are part of the wired WLAN are connected to the wired network.
- The wired Wireless APs that will serve as the Root AP/Root APs of the proposed WDS topology are operating normally.
- The WLAN is operating normally.

Planning the WDS Topology

You may sketch the proposed WLAN topology on paper before you start the WDS deployment process. You should clearly identify the following in the sketch:

- WDS Wireless APs with their names
- Parent-child relationships between Wireless APs
- Radios that you will choose to link the Wireless AP's parents and children

Provisioning the WDS Wireless APs

This step is of crucial importance and involves connecting the WDS Wireless APs to the enterprise network via the Ethernet link. This is done to enable the WDS Wireless APs to connect to the Enterasys Wireless Controller so that they can derive their WDS configuration.

The WDS Wireless AP's configuration includes pre-shared key, its role, preferred parent name and the backup parent name.



Note: The provisioning of WDS Wireless APs must be done before they are deployed at the target location. If the Wireless APs are not provisioned, they will not work at their target location.

WDS Deployment Overview

The following is the high-level overview of the WDS deployment process:

1. Connecting the WDS Wireless APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the Enterasys Wireless Controller. For more information, see "[Discovery and Registration Overview](#)" on page 3-10.
2. Disconnecting the WDS Wireless APs from the enterprise network after they have discovered and registered with the Enterasys Wireless Controller.
3. Creating a WDS VNS.
4. Assigning roles, parents and backup parents to the WDS Wireless APs.
5. Assigning the Satellite Wireless APs' radios to the network VNSs.
6. Connecting the WDS Wireless APs to the enterprise network via the Ethernet link for provisioning. For more information, see "[Provisioning the WDS Wireless APs](#)" on page 10-11.
7. Disconnecting the WDS Wireless APs from the enterprise network and moving them to the target location.



Note: During the WDS deployment process, the WDS Wireless APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the Enterasys Wireless Controller, and then the second time to enable them to obtain the provisioning from the Enterasys Wireless Controller.

Connecting the WDS Wireless APs to the Enterprise Network for Discovery and Registration

Connect each WDS Wireless AP to the enterprise network to enable it to discover and register itself with the Enterasys Wireless Controller.



Note: Before you connect the WDS Wireless APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the Enterasys Wireless Controller is defined according to your security needs. The **Security mode** property dictates how the Enterasys Wireless Controller behaves when registering new and unknown devices. For more information, see [“Defining Properties for the Discovery Process”](#) on page 3-26. If the **Security mode** is set to **Allow only approved Wireless APs to connect** (this is also known as secure mode), you must manually approve the WDS Wireless APs after they are connected to the network for the discovery and registration. For more information, see [“Adding and Registering a Wireless AP Manually”](#) on page 3-28.

Depending upon the number of Ethernet ports available, you may connect one or more WDS Wireless APs at a time, or you may connect all of them together.

Once a WDS Wireless AP has discovered and registered itself with the Enterasys Wireless Controller, disconnect it from the enterprise network.

Configuring the WDS Wireless APs Through the Enterasys Wireless Controller

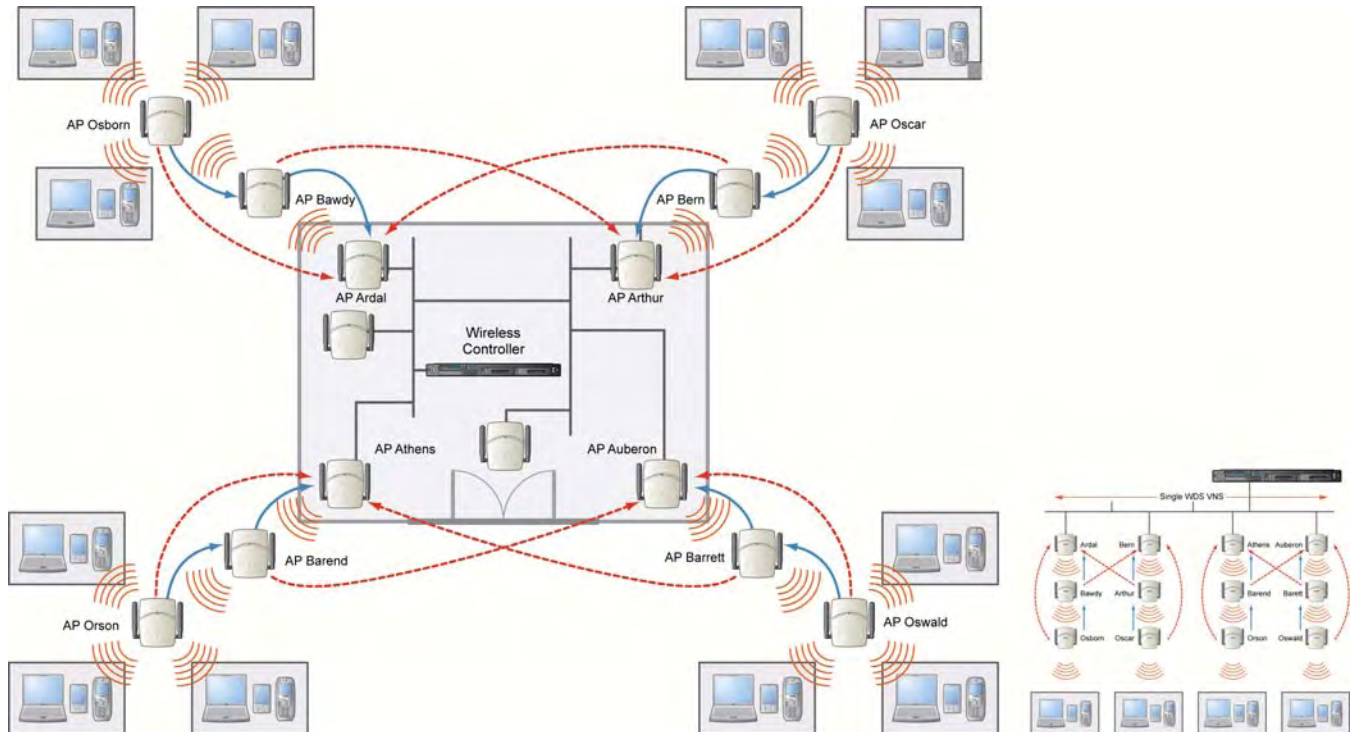
Configuring the WDS Wireless APs involves the following steps:

1. Creating a WDS WLAN Service.
2. Defining the SSID name and the pre-shared key.
3. Assigning roles, parents and backup parents to the WDS Wireless APs.

For ease of understanding, the WDS configuration process is explained with an example. [Figure 10-10](#) depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four Wireless APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the warehouse.
- The solid arrows point toward Preferred Parents.
- The dotted arrows point toward Backup Parents.

Figure 10-10 WDS Deployment



Note: With the single WDS VNS, the tree structure for the WDS deployment will be as depicted on the bottom right of Figure 10-10. You can also implement the same deployment using four WDS VNSs, each for a set of Wireless APs in the four corners of the building. Each set of Wireless APs will form an isolated topology and will operate using a separate **SSID** and a separate **Pre-shared** key. For more information, see “WDS WLAN Services” on page 10-4.

To Configure the WDS Wireless APs Through the Enterasys Wireless Controller:



Note: You must identify and mark the Preferred Parents, Backup Parents and the Child Wireless APs in the proposed WDS topology before starting the configuration process.

1. From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
2. In the left pane, expand the **WLAN Services** pane and select a WDS service to edit or click the **New** button.
3. Enter a name for the service in the **Name** field.
4. The **SSID** field is automatically filled in with the name, but you can change it if desired.

5. For **Service Type**, select **WDS**.

The screenshot displays the Enterasys Virtual Network Configuration web interface. The top navigation bar includes the Enterasys logo, the tagline "Secure Networks. There's nothing more important than our customers.", and the page title "Virtual Network Configuration". The navigation menu contains links for Home, Logs, Reports, Wireless Controller, Wireless APs, **WDS Configuration**, Mitigator, Help, and LOGOUT.

The left sidebar contains a tree view with the following categories and items:

- New...
- Global
- Virtual Networks
 - WLAN Services** (highlighted)
 - CNL-91-0-0
 - CNL-91-0-1
 - CNL-91-0-2
 - CNL-91-0-3
 - CNL-91-0-4
 - CNL-91-0-5-wds
 - CNL-91-0-6
 - CNL-91-WDS
 - Mesh_WLAN_Svc
- Policies
- Classes of Service
- Topologies

The main content area is titled "WLAN:" and "WLAN Services". It contains a configuration form with the following fields:

- Name:** [Text input field]
- Service Type:** Radio button selection with options: Standard, **WDS** (selected), Mesh, Third Party AP, and Remote.
- SSID:** [Text input field]
- Status:** **Enable:**

A "Save" button is located at the bottom right of the configuration area.

- To save your changes, click **Save**. The WLAN configuration window is re-displayed to show additional configuration fields.

The screenshot shows the 'Virtual Network Configuration' interface for 'WLAN: mtest'. The left sidebar contains a tree view with 'WLAN Services' selected. The main area is titled 'WLAN Services' and contains the following fields:

- Name:** mtest
- Service Type:** WDS
- SSID:** mtest
- WDS Pre-shared key:** (empty text box)
- Status:** Enable:

Below these fields is a table titled 'Wireless APs services':

AP Name	Radio 1	Mode	Radio 2	Mode	Preferred Parent	Backup Parent
0500006072051204	none	a	none	b/g		
1000005480080188	none	a	none	b/g		
7000000000000111	none	a/n	none	b/g/n		

At the bottom of the configuration area are buttons for 'New', 'Delete', and 'Save'.

- In the **WDS Pre-shared Key** box, type the key.



Note: The pre-shared key must be 8 to 63 characters long. The WDS Wireless APs use this pre-shared key to establish a WDS link between them.



Note: Changing the pre-shared key after the WDS is deployed can be a lengthy process. For more information, see [“Changing the Pre-shared Key in a WDS WLAN Service”](#) on page 10-19.

- Assign the roles, preferred parents and backup parents to the Wireless AP Radios.



Note: The roles — **parent**, **child**, and **both** — are assigned to the Radios of the Wireless APs. A Wireless AP may connect to its parent Wireless AP and children Wireless APs on the same Radio, or on a different Radio. Similarly, a Wireless AP can have two children operating on two different Radios.

The Radio on which the child Wireless AP operates is determined by the parent Wireless AP. If the Wireless AP will be serving both as parent and child, you must select **both** as its role.

To configure the WDS as illustrated in [Figure 10-10](#) with a single WDS VNS, you must assign the roles, preferred parents and backup parents to the Wireless APs according to [Table 10-1](#).

Table 10-1 Wireless APs and Their Roles

Wireless AP	Radio b/g	Radio a	Preferred Parent	Backup Parent
Ardal	Parent	Parent	See the note below.	See the note below.
Arthur	Parent	Parent	See the note below.	See the note below.

Table 10-1 Wireless APs and Their Roles (continued)

Wireless AP	Radio b/g	Radio a	Preferred Parent	Backup Parent
Athens	Parent	Parent	See the note below.	See the note below.
Auberon	Parent	Parent	See the note below.	See the note below.
Bawdy	Both	Child	Ardal	Arthur
Bern	Both	Child	Arthur	Ardal
Barend	Both	Child	Athens	Auberon
Barett	Both	Child	Auberon	Athens
Osborn	Child	Child	Bawdy	Ardal
Oscar	Child	Child	Bern	Arthur
Orson	Child	Child	Barend	Athens
Oswald	Child	Child	Barett	Auberon



Note: Since the Root Wireless APs — Ardal, Arthur, Athens and Auberon — are the highest entities in the tree structure, they do not have parents. Therefore, the **Preferred Parent** and **Backup Parent** drop-down lists of the Root Wireless APs do not display any Wireless AP. You must leave these two fields blank.



Note: You must first assign the ‘parent’ role to the Wireless APs that will serve as the parents. Unless this is done, the Parent Wireless APs will not be displayed in the **Preferred Parent** and **Backup Parent** drop-down lists of other Wireless APs.



Note: The **WDS Bridge** feature on the user interface relates to WDS Bridge configuration. When you are configuring the WDS Bridge topology, you must select **WDS Bridge** for Satellite Wireless AP that is connected to the wired network. For more information, see “[Wireless Bridge Configuration](#)” on page 10-3.

To assign the roles, preferred parent and backup parent:

- From the radio **b/g** drop-down list of the Root Wireless APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
- From the radio **a** drop-down list of the Root Wireless APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
- From the radio **a** and radio **b/g** drop-down list of other Wireless APs, click the roles according to [Table 10-1](#).
- From the **Preferred Parent** drop-down list of other Wireless APs, click the parents according to [Table 10-1](#).
- From the **Backup Parent** drop-down list of other Wireless APs, click the backup parents according to [Table 10-1](#).

Wireless APs services						
AP Name	Radio 1	Mode	Radio 2	Mode	Preferred Parent	Backup Parent
Ardal	parent	a	parent	b/g		
Arthur	parent	a	parent	b/g		
Athens	parent	a	parent	b/g		
Auberon	parent	a	parent	b/g		
Bawdy	both	a	child	b/g		
Bern	both	a	child	b/g		
Barend	both	a	child	b/g		
Barett	both	a	child	b/g		
Osborn	child	a	child	b/g		
Oscar	child	a	child	b/g		
Orson	child	a	child	b/g		
Oswald	child	a	child	b/g		

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

Assigning the Satellite Wireless APs' Radios to the Network WLAN Services

You must assign the Satellite Wireless APs' radios to the network WLAN Services.



Note: Network WLAN Services are the typical WLAN Services on which the Wireless APs service the client devices: **Routed**, **Bridge Traffic Locally at HWC**, and **Bridge Traffic Locally at AP**. For more information, see "[VNS Global Settings](#)" on page 7-3.

To Assign the Satellite Wireless APs' Radios to the Network WLAN Service:

- From the top menu, click **VNS Configuration**. The **Virtual Network Configuration** screen is displayed.
- In the left pane, expand the **WLAN Services** pane and select a network WDS service to edit

Wireless APs:

Select APs:

Radio 1	Radio 2	AP Name
<input type="checkbox"/> a	<input type="checkbox"/> b/g	Arthur
<input type="checkbox"/> a	<input type="checkbox"/> b/g	Athens
<input type="checkbox"/> a	<input type="checkbox"/> b/g	Auberon
<input type="checkbox"/> a	<input type="checkbox"/> b/g	Barett
<input type="checkbox"/> a	<input type="checkbox"/> b/g	Bawdy
<input checked="" type="checkbox"/> a	<input checked="" type="checkbox"/> b/g	Orson
<input checked="" type="checkbox"/> a	<input checked="" type="checkbox"/> b/g	Osborn
<input checked="" type="checkbox"/> a	<input checked="" type="checkbox"/> b/g	Oscar
<input checked="" type="checkbox"/> a	<input checked="" type="checkbox"/> b/g	Oswald

- In the **Wireless APs** list, select the radios of the Satellite APs — Osborn, Oscar, Orson and Oswald.



Note: If you want the Root Wireless AP and the Repeater Wireless APs to service the client devices, you must select their radios in addition to the radios of the Satellite Wireless APs.

4. To save your changes, click **Save**.
5. Log out from the Enterasys Wireless Controller.

Connecting the WDS Wireless APs to the Enterprise Network for Provisioning

You must connect the WDS Wireless APs to the enterprise network once more to enable them to obtain their configuration from the Enterasys Wireless Controller. The configuration includes the pre-shared key, the Wireless AP's role, preferred parent and backup parent. For more information, see [Provisioning the WDS Wireless APs](#) on 10-11.



Warning: If you skip this step, the WDS Wireless APs will not work at their target location.

Moving the WDS Wireless APs to the Target Location

1. Disconnect the WDS Wireless APs from the enterprise network, and move them to the target location.
2. Install the WDS Wireless APs at the target location.
3. Connect the Wireless APs to a power source. The discovery and registration processes are initiated.



Note: If you change any of the following configuration parameters of a WDS Wireless AP, the WDS Wireless AP will reject the change:

- Reassigning the WDS Wireless AP's role from **Child** to **None**
- Reassigning the WDS Wireless AP's role from **Both** to **Parent**
- Changing the **Preferred Parent** of the WDS Wireless AP

However, the Enterasys Wireless Controller will display your changes, as these changes will be saved in the database. To enable the WDS Wireless AP to obtain your changes, you must remove it from the WDS location and then connect it to the Enterasys Wireless Controller via the wired network.



Note: If you change any of the following radio properties of a WDS Wireless AP, the WDS Wireless AP will reject the change:

- Disabling the radio on which the WDS link is established
- Changing the radio's Tx Power of a radio on which the WDS link is established
- Changing the country

Changing the Pre-shared Key in a WDS WLAN Service

To Change the Pre-shared Key in a WDS WLAN Service

1. Create a new WDS WLAN Service with a new pre-shared key.
2. Assign the RF of the Wireless APs from the old WDS to the new WDS WLAN Service.
3. Check the **WDS Wireless AP Statistics** report page to ensure that all the WDS Wireless APs have connected to the Enterasys Wireless Controller via the new WDS VNS. For more information, see [“Viewing Statistics for Wireless APs”](#) on page 15-4.
4. Delete the old WDS WLAN Service. For more information, see [“Deleting a VNS”](#) on page 7-48.

Availability and Session Availability

This chapter describes the availability feature, including:

For information about...	Refer to page...
Availability	11-1
Session Availability	11-9
Viewing the Wireless AP Availability Display	11-17
Viewing SLP Activity	11-18

Availability

The Enterasys Wireless Controller Software system provides the availability feature to maintain service availability in the event of a Enterasys Wireless Controller outage.



Note: During the failover event, the maximum number of failover APs the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

Wireless APs that attempt to connect to the secondary controller during a failover event are assigned to the WLAN Service that is defined in the system's default AP configuration, provided the administrator has not assigned the failover Wireless APs to one or more VNSs. If a system default AP configuration does not exist for the controller (and the administrator has not assigned the failover Wireless APs to any WLAN Service), the APs will not be assigned to any WLAN Service during the failover.

A Enterasys Wireless Controller will not accept a connection by a foreign AP if the Enterasys Wireless Controller believes its availability partner controller is in service. Also, the default Wireless AP configuration assignment is only applicable to new APs that failover to the backup controller. Any Wireless AP that has previously failed over and is already known to the backup system will receive the configuration already present on that system. For more information, see "[Configuring the Default Wireless AP Settings](#)" on page 3-76.

During the failover event when the Wireless AP connects to the secondary controller, the users are disassociated from the Wireless AP. Consequently, the users must log on again and be authenticated on the secondary controller before the wireless service is restored.



Note: If you want the mobile user's session to be maintained, you must use the 'session availability' feature that enables the primary controller's Wireless APs to failover to the secondary controller fast enough to maintain the session availability (user session). For more information, see "[Session Availability](#)" on page 11-9.

The availability feature provides Wireless APs with a list of local active interfaces for the active controller as well as the active interfaces for the backup controller. The list is sorted by top-down priority.

If the connection with an active controller link is lost (poll failure), the Wireless AP automatically scans (pings) all addresses in its availability interface list. The Wireless AP then connects to the highest priority interface that responds to its probe.

Events and Actions in Availability

If one of the Enterasys Wireless Controllers in a pair fails, the communication between the two Enterasys Wireless Controllers stops. This triggers a failover condition and a critical message is displayed in the information log of the secondary Enterasys Wireless Controller.

The screenshot shows the Enterasys 'Logs & Traces' interface. At the top, there is a navigation bar with links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration, Mitigator, Help, and LOGOUT. Below this is a breadcrumb trail: HWC: Events | Restore/Import | S/W Upgrade | AP: Logs | Traces | Audit: UI | Services: DHCP | NTP | Login. The main content area displays a table of log messages with columns for Timestamp, Type, Component, and Log Message. The messages are filtered by severity 'Critical'. The first message at 06/13/11 17:10:21 states: 'Cannot establish an Availability Link: Incompatible configuration. AC role Primary is configured the same as availability peer.' Subsequent messages at 06/06/11 15:48:23 and 06/02/11 11:14:39 report 'No radius server available for WLAN service'. A series of messages from 05/19/11 onwards report 'Config Manager has suffered a critical error and will halt' due to 'Failed to connect to database 'controllerConfig''.

Timestamp	Type	Component	Log Message
06/13/11 17:10:21	Critical	RU Manager	Cannot establish an Availability Link: Incompatible configuration. AC role Primary is configured the same as availability peer.
06/06/11 15:48:23	Critical	Radius Client	No radius server available for WLAN service : Lab126-12-AAA. Client [00:13:ce:c7:4c:91].
06/02/11 11:14:39	Critical	Startup Manager	Initiating Reboot. Cause: MU Session Manager Not Responding.
05/24/11 10:34:10	Critical	Radius Client	No radius server available for WLAN service : Lab126-10-Ext-CP. Client [00:00:00:00:00:00].
05/19/11 11:34:53	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
05/19/11 11:34:50	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
05/10/11 09:34:31	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
05/05/11 11:40:09	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
05/05/11 11:40:06	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
05/05/11 11:32:49	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
05/05/11 11:32:46	Critical	Config Manager	Config Manager has suffered a critical error and will halt. Error Details: Failed to connect to database 'controllerConfig': Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)

At the bottom of the log view, it indicates '314 critical log messages found' and 'Total pages: 1'. There are navigation buttons for 'Tech Support', 'Export', and 'Refresh'.

After a Wireless AP on the failed Enterasys Wireless Controller loses its connection, it will try to connect to all enabled interfaces on both controllers without rebooting. If the Wireless AP is not successful, it will begin the discovery process. If the Wireless AP is not successful in connecting to the Enterasys Wireless Controller after five minutes of attempting, the Wireless AP will reboot if there is no **Bridge traffic locally at the AP** topology associated to it.

All mobile user's sessions using the failover Wireless AP will terminate except those associated to a **Bridge traffic locally at the AP** and if the **Maintain client sessions in event of poll failure** option is enabled on the **AP Properties** tab or **AP Default Settings** screen.

When the Wireless APs connect to the second Enterasys Wireless Controller, they are either assigned to the VNS that is defined in the system's default AP configuration or manually configured by the administrator. The mobile users log on again and are authenticated on the second Enterasys Wireless Controller.

When the failed Enterasys Wireless Controller recovers, each Enterasys Wireless Controller in the pair goes back to normal mode. They exchange information including the latest lists of registered Wireless APs. The administrator must release the Wireless APs manually on the second Enterasys

Wireless Controller, so that they may re-register with their home Enterasys Wireless Controller. Foreign APs can now all be released at once by using the **Foreign** button on the **Access Approval** screen to select all foreign APs, and then clicking **Release**.

To support the availability feature during a failover event, you need to do the following:

1. Monitor the critical messages for the failover mode message, in the information log of the remaining Enterasys Wireless Controller (in the **Logs & Traces** section of the Enterasys Wireless Assistant).
2. After recovery, on the Enterasys Wireless Controller that did not fail, select the foreign Wireless APs, and then click **Release** on the **Access Approval** screen.

Availability Prerequisites

Before you configure availability, you must do the following:

- Choose the primary and secondary Enterasys Wireless Controllers.
- Verify the network accessibility for the UDP connection between the two controllers. The availability link is established as a UDP session on port 13911.
- Set up a DHCP server for AP subnets to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both the Enterasys Wireless Controllers.
- Ensure that the **Poll Timeout** value on the **AP Properties** tab **Advanced** dialog is set to 1.5 to 2 times of **Detect link failure** value on the Enterasys Wireless Controller > **Availability** screen. For more information, see “[Configuring a Wireless AP’s Properties](#)” on page 3-31.

If the **Poll Timeout** value is less than 1.5 to 2 times of **Detect link failure value**, the Wireless AP failover will not succeed because the secondary controller will not be 'ready' to accept the failover APs.

On the other hand, if the **Poll Timeout** value is more than 1.5 to 2 times of **Detect link failure value**, the Wireless APs failover will be unnecessarily delayed, because the Wireless APs will continue polling the primary controller even though the secondary controller is ready to accept them as the failover APs.

- To achieve ideal availability behavior, you must set the **Poll Timeout** value for all Wireless APs to 15 seconds, and the **Detect link failure** on the Enterasys Wireless Controller > **Availability** screen to ten seconds.

Configuring Availability Using the Availability Wizard


The availability wizard allows you to create an availability pair from one of the Enterasys Wireless Controllers that will be in the availability pair. When creating the availability pair, you also have the option to synchronize VNS definitions and GuestPortal user accounts between the paired Enterasys Wireless Controllers.

To Configure Availability Using the Availability Wizard:

1. From the top menu, click **Wireless Controller**. The Enterasys Wireless Controller **Configuration** screen is displayed.
2. In the left pane, click **Availability**. The availability configuration screen is displayed.

3. In the **Availability Wizard** section, click **Start**. The **Availability Pair Wizard** screen is displayed.

The screenshot shows the 'Availability Pair Wizard' configuration page. At the top, the Enterasys logo and tagline 'Secure Networks' are visible, along with the page title 'Wireless Controller Configuration'. A navigation bar includes links for Home, Logs, Reports, Wireless Controller (highlighted), Wireless APs, VNS Configuration, Mitigator, Help, and LOGOUT. The main heading is 'Availability Pair Wizard'. Below it, a descriptive paragraph states: 'This wizard enables you to quickly configure an Availability Pair from one controller. This controller will become the primary connection point.' The form is divided into two sections: 'Connection Details' and 'Synchronization Options'. The 'Connection Details' section includes a 'Select Port' dropdown menu (set to 'eth0 (192.168.3.10)'), a 'Peer Controller IP' text field (set to '0.0.0.0'), 'Peer Controller Login' fields for 'User' and 'Password', and a 'Fast Failover' checkbox. The 'Synchronization Options' section features a red warning message: '* Please note that this will replace ALL of the selected definitions on the target controller'. Below this are two checkboxes: 'Synchronize System Configuration' and 'Synchronize Guest Portal Accounts'. At the bottom right of the form, there are three buttons: 'Back', 'Next', and 'Cancel'.

4. In the **Connection Details** section, do the following:
 - **Select Port** — Select the port and IP address of the primary controller that is to be used to establish the availability link.
 - **Peer Controller IP** — Type the IP address of the peer (secondary) controller.
 - **User** — Type the login user name credentials of an account that has full administrative privileges on the peer controller.
 - **Password** — Type the login password used with the user ID to login to the peer controller.
 - **Enable Fast Failover** — Select this checkbox to enable Fast Failover for the availability pair.
 5. In the **Synchronize Options** section, do the following:
 - **Synchronize System Configuration** — Select this checkbox to push the configured **Routed** and **Bridge Traffic Locally at Controller** VNS definitions from the primary controller to the peer controller. **WDS** and **3rd Party AP** VNS definitions are ignored and not synchronized.
-  **Note:** Synchronizing the VNS definitions will delete and replace existing VNS definitions on the peer controller.
- **Synchronize Guest Portal Accounts** — Select this checkbox to push GuestPortal user accounts to the peer controller.
6. Click **Next**.
 7. If you are synchronizing topology definitions, the **Topology Definitions** screen is displayed. Do the following:

-
- a. In the **Synchronization Settings** section, complete the topology properties that are missing. Any topology that did not already exist on the peer controller will have missing properties on the Topology Definitions screen.

The fields configured are actual parameter values that are configured at the remote Controller with respect to associated topologies chosen for synchronization. Some of these parameters are: Interface IP address, Netmask, L2 port, VLAN ID, DHCP range, etc.

- b. Click **Finish**.
8. If you are not synchronizing topology definitions, the availability wizard completes the configuration.
9. Click **Close**.

This operation marks the desired topologies for synchronization. The two controllers exchange information and the configuration is applied to the remote controller.

On the local controller, the “Enable Synchronization of System Configuration” becomes selected. This can be double checked by navigating to VNS Configuration, Global and then Sync Summary. This tab also lists all topologies, policies, WLAN Services and VNSes with their synchronization status (on or off).

The Sync status for any of these elements can also be changed from this tab.

All these configurable elements have a **Synchronize** check box (on their main/general configuration tab) that allows for individual control and selection of availability from the main element configuration page.

Configuring Availability Manually

When configuring availability manually, you configure each Enterasys Wireless Controller separately.

1. On the Enterasys Wireless Controller Configuration **Availability** screen, set up the Enterasys Wireless Controller in **Paired Mode**.
2. On the **VNS** configuration window, define a VNS (through topology, WLAN service, policy and VNS configuration) on each Enterasys Wireless Controller with the same SSID. The IP addresses must be unique. For more information, see “[Manually Creating a VNS](#)” on page 7-18. A Enterasys Wireless Controller VLAN Bridged topology can permit two controllers to share the same subnet. This setup provides support for mobility users in a VLAN Bridged VNS.
3. On both Enterasys Wireless Controllers, on the Wireless AP Registration screen, select the Security Mode **Allow only approved Wireless APs to connect** option so that no more Wireless APs can register unless they are approved by the administrator.
4. On each Enterasys Wireless Controller, on the Wireless AP configuration **Access Approval** screen, check the status of the Wireless APs and approve any APs that should be connected to that controller.

System AP defaults can be used to assign a group of VNSs to the foreign APs:

- If the APs are not yet known to the system, the AP will be initially configured according to AP default settings. To ensure better transition in availability, Enterasys recommends that the AP default settings match the desired assignment for failover APs.
- AP assignment to WLAN Services according to the AP default settings can be overwritten by manually modifying the AP assignment. (For example, select and assign each WLAN service that the AP should connect to.)

- If specific foreign APs have been assigned to a WLAN service, those specific foreign AP assignments are used.

An alternate method to setting up APs includes:

1. Add each Wireless AP manually to each Enterasys Wireless Controller.
2. On the **AP Properties** screen, click **Add Wireless AP**.
3. Define the Wireless AP, and then click **Add Wireless AP**.

Manually defined APs will inherit the default AP configuration settings.



Caution: If two Enterasys Wireless Controllers are paired and one has the **Allow All** option set for Wireless AP registration, all Wireless APs will register with that Enterasys Wireless Controller.

Setting the Primary or Secondary Enterasys Wireless Controllers for Availability

To Set the Primary or Secondary Enterasys Wireless Controllers for Availability:

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

enterasys
Secure Networks™ There's nothing more important than our customers.

Wireless Controller Configuration

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

Availability Pair Wizard

This wizard enables you to quickly configure an Availability Pair from one controller. This controller will become the primary connection point.

Connection Details

Select Port: eth0 (192.168.3.10) ▼

Peer Controller IP: 0.0.0.0

Peer Controller Login: User: [text box] Password: [text box]

Fast Failover:

Synchronization Options

* Please note that this will replace ALL of the selected definitions on the target controller

Synchronize System Configuration

Synchronize Guest Portal Accounts

Back Next Cancel

3. To enable availability, select the **Paired** option.
4. Do one of the following:
 - For a primary controller, in the **Wireless Controller IP Address** box, type the **IP address** of the data interface of the secondary Enterasys Wireless Controller. This IP address must be on a routable subnet between the two Enterasys Wireless Controllers.
 - For a secondary controller, in the **Wireless Controller IP Address** box, type the IP address of the Management port or data interface of the primary Enterasys Wireless Controller.

-
5. Set this Enterasys Wireless Controller as the primary or secondary connection point:
 - To set this Enterasys Wireless Controller as the **primary connection point**, select the **Current Wireless Controller is primary connect point** checkbox.
 - To set this Enterasys Wireless Controller as the **secondary connection point**, clear the **Current Wireless Controller is primary connect point** checkbox.

If the **Current Wireless Controller is primary connect point** checkbox is selected, the specified controller sends a connection request. If the **Current Wireless Controller is primary connect point** checkbox is cleared, the specified controller waits for a connection request. Confirm that one controller has this checkbox selected, and the second controller has this checkbox cleared, since improper configuration of this option will result in incorrect network configuration.

6. On both the primary and secondary controllers, type the **Detect link failure value**.



Note: Ensure that the **Detect link failure** value on both the controllers is identical.

7. On both the primary and secondary controllers, select the **Synchronize GuestPortal Guest Users** option to synchronize GuestPortal guest accounts between the controllers.
8. From the top menu, click **Wireless APs**. The Enterasys Wireless **AP Configuration** screen is displayed.
9. In the left pane, click **AP Registration**. To set the **security mode** for the Enterasys Wireless Controller, select one of the following options:
 - **Allow all Wireless APs to connect** — If the Enterasys Wireless Controller does not recognize the serial number, it sends a default configuration to the Wireless AP. Or, if the Enterasys Wireless Controller recognizes the serial number, it sends the specific configuration (port and binding key) set for that Wireless AP.
 - **Allow only approved Wireless APs to connect** — If the Enterasys Wireless Controller does not recognize the serial number, the Wireless APs will be in pending mode and the administrator must manually approve them. Or, if the Enterasys Wireless Controller recognizes the serial number, it sends the configuration for that Wireless AP.
10. To save your changes, click **Save**.



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

Once the initial setup is complete, Enterasys recommends that you reset the security mode to the **Allow only approved Wireless APs to connect** option. This option ensures that no unapproved Wireless APs are allowed to connect. For more information, see [“Configuring Wireless AP Settings”](#) on page 3-29.



Note: When two Enterasys Wireless Controllers have been paired as described above, each Enterasys Wireless Controller's registered Wireless APs will appear as foreign on the other controller in the list of available Wireless APs when configuring a VNS topology.

11. Verify that availability is configured correctly.

Verifying Availability

To verify that availability is configured correctly:

- a. From the top menu of either of the two controllers, click **Reports**. The **Reports & Displays** screen is displayed.

The screenshot shows the Enterasys web interface. At the top left is the Enterasys logo with the tagline "Secure Networks" and "There's nothing more important than our customers." The top right says "Reports & Displays". Below the logo is a navigation bar with links: Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration, Mitigator, Help, and LOGOUT. Underneath is a sub-menu for "Reports" with links: List of Displays, Forwarding Table, OSPF Neighbor, OSPF Linkstate, and AP Inventory. The main content area lists various reports and statistics:

- 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
- Mesh Statistics
- Active Wireless Load Groups
- Admission Control Statistics by Wireless AP
- Remotable VNS Information
- External Connections Statistics
- System Information
- Manufacturing Information

- b. From the **Reports and Displays** menu, click **Wireless AP Availability**. The **Wireless Availability Report** is displayed.

The screenshot shows the "Wireless AP Availability - 192.168.4.207" report. At the top right, there are controls for refreshing: "No refresh" (selected) and "Refresh every 200 secs" with an "Apply" button. The main status is "Availability Link is UP" in green. Below this is a "Color Legend" with four categories: "Wireless AP has active tunnel passing data" (green), "Wireless AP has backup tunnel" (blue), "Wireless AP not connected" (orange), and "No information" (grey). The "Wireless APs List" section shows four entries:

Foreign	Foreign	Local	Foreign
00000012CF737033	0002000810004623	0409920201201282	0409920201202222
00000012CF737033	0002000810004623	0409920201201282	0409920201202222
00:12:CF:73:70:33	00:02:00:08:10:00:46:23	00:0F:C8:F0:13:CB	00:0F:C8:F0:13:CB
uptime: n/a	uptime: n/a	uptime: 9 d, 19:07:03	uptime: n/a
		10.209.1.232	

At the bottom left, it says "Data as of Feb 23, 2009 11:08:58 am". At the bottom right, there are "Refresh" and "Close" buttons.

- c. Check the statement at the top of the screen.

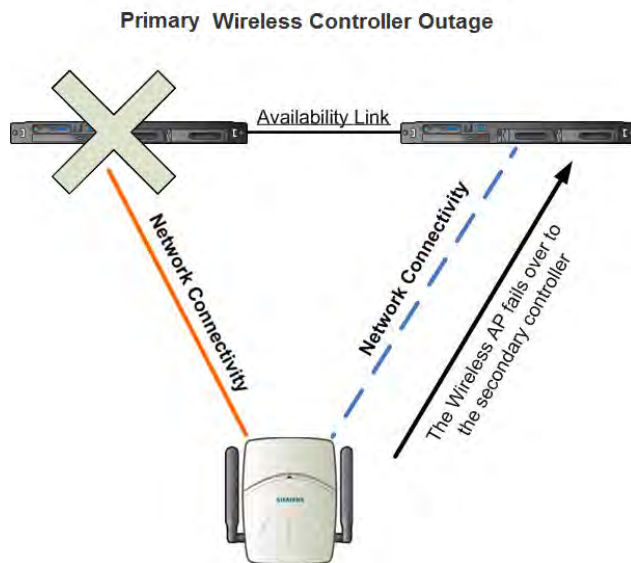
If the statement reads **Availability link is up**, the availability feature is configured correctly. If the statement reads **Availability link is down**, check the configuration error logs. For more information on logs, see the *Enterasys Wireless Convergence Software Maintenance Guide*.

Session Availability

Session availability enables Wireless APs to switch over to a standby (secondary) Enterasys Wireless Controller fast enough to maintain the mobile user's session availability in the following scenarios:

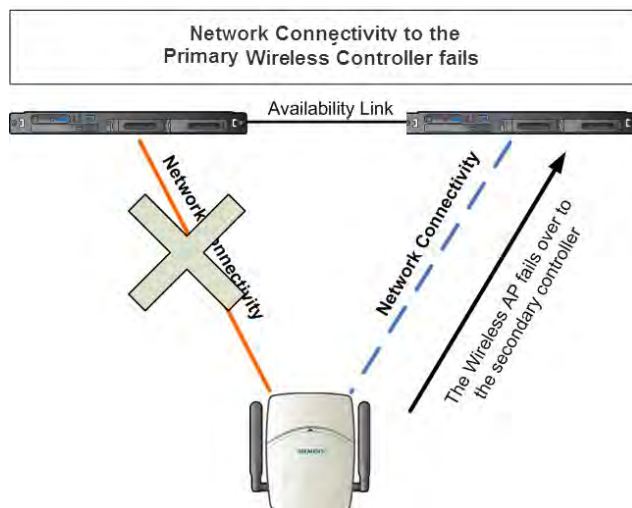
- The primary Enterasys Wireless Controller goes down (Figure 11-1).

Figure 11-1 AP Fail Over to 2ndary Controller When Primary Goes Down



- The Wireless AP's network connectivity to the primary Enterasys Wireless Controller fails (Figure 11-2).

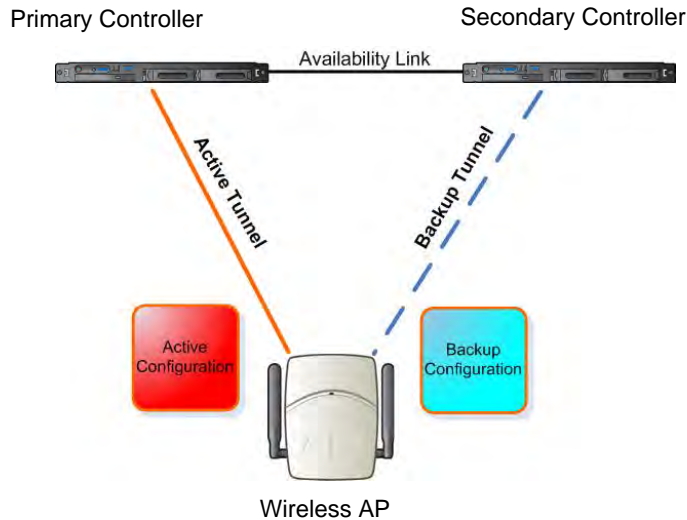
Figure 11-2 AP Fail Over to 2ndary Controller When Connectivity to Primary Fails



The secondary Enterasys Wireless Controller does not have to detect its link failure with the primary Enterasys Wireless Controller for the session availability to kick in. If the Wireless AP loses five consecutive polls to the primary controller either due to the controller outage or connectivity failure, it fails over to the secondary controller fast enough to maintain the user session.

In session availability mode (Figure 11-3), the Wireless APs connect to both the primary and secondary Enterasys Wireless Controllers. While the connectivity to the primary Enterasys Wireless Controller is via the “active” tunnel, the connectivity to the secondary Enterasys Wireless Controller is via the “backup” tunnel.

Figure 11-3 Session Availability Mode



The following is the traffic flow of the topology illustrated in Figure 11-3:

- The Wireless AP establishes the active tunnel to connect to the primary Enterasys Wireless Controller.
- The Enterasys Wireless Controller sends the configuration to the Wireless AP. This configuration also contains the port information of the secondary Enterasys Wireless Controller.
- On the basis of the secondary Enterasys Wireless Controller’s port information, the Wireless AP connects to the secondary controller via the backup tunnel.
- After the connection is established via the backup tunnel, the secondary Enterasys Wireless Controller sends the backup configuration to the Wireless AP.
- The Wireless AP receives the backup configuration and stores it in its memory to use it for failing over to the secondary controller. All this while, the Wireless AP is connected to the primary Enterasys Wireless Controller via the ‘active’ tunnel.

Session availability applies only to the following topologies:

- Bridge Traffic Locally at Controller
- Bridge Traffic Locally at AP

Events and Actions in Session Availability

In the event of a primary Enterasys Wireless Controller outage, or the network connectivity failure to the primary controller, the Wireless AP:

- Sends a 'tunnel-active-req' request message to the secondary Enterasys Wireless Controller.
- The secondary Enterasys Wireless Controller accepts the request by sending the 'tunnel-activate-response' message.
- The Wireless AP applies the backup configuration and starts sending the data. The client devices' authentication state is not preserved during failover.

When the fast failover takes place, a critical message is displayed in the information log of the secondary Enterasys Wireless Controller.



Note: In session availability, the maximum number of failover APs that the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

When the failed Enterasys Wireless Controller recovers, each Enterasys Wireless Controller in the pair goes back to normal mode. They exchange information that includes the latest lists of registered Wireless APs. The administrator must release the Wireless APs manually on the second Enterasys Wireless Controller, so that they may re-register with their home Enterasys Wireless Controller. Foreign APs can now all be released at once by using the **Foreign** button on the **Access Approval** screen to select all foreign APs, and then clicking **Released**.

To support the availability feature during a failover event, administrators need to do the following:

1. Monitor the critical messages for the failover mode message, in the information log of the secondary Enterasys Wireless Controller (in the **Logs & Traces** section of the Enterasys Wireless Assistant).
2. After recovery, on the secondary Enterasys Wireless Controller, select the foreign Wireless APs, and then click **Release** on the **Access Approval** screen.

After the Wireless APs are released, they establish the active tunnel to their home controller and backup tunnel to the secondary controller.

Enabling Session Availability

Session availability is supported when fast failover is enabled and when "Synchronize System Configuration" is selected. For more information, see "[Configuring Fast Failover and Enabling Session Availability](#)" on page 11-12.

In session availability, mobile user devices are able to retain their IP address. In addition, the mobile user device does not have to re-associate after the failover. These characteristics ensure that the failover is achieved within 5 seconds, which is fast enough to maintain the mobile user's session.



Note: In session availability, the fast failover is achieved within 5 seconds only if there is at least one client device (mobile unit) associated to the Wireless AP. In the absence of any client device, the Wireless AP takes more time to failover since there is no need to preserve the user session.

The authentication state is not preserved during fast failover. If a WLAN Service requires authentication, the client device must re-authenticate. However, in such a case, the session availability is not guaranteed because authentication may require additional time during which the user session may be disrupted.

Session availability is not supported in a WLAN Service that uses Captive Portal (CP) authentication.

Session availability does not support user-specific filters as these filters are not shared between the primary and secondary Enterasys Wireless Controllers.

Configuring Fast Failover and Enabling Session Availability

Before you configure the fast failover feature, ensure the following:

- The primary and secondary Enterasys Wireless Controllers are properly configured in availability mode. For more information, see [“Availability”](#) on page 11-1.
- The pair of Enterasys Wireless Controllers in availability mode is formed by one of the following combinations:
 - C5110 and C5110
 - C4110 and C4110
 - C20 and C20
 - C5110 and C4110
 - C25 and C25
- Both the primary and secondary Enterasys Wireless Convergence Software Controllers are running the most recent Enterasys Wireless Convergence Software Convergence Software releases.
- A network connection exists between the two Enterasys Wireless Controllers.
- The Wireless APs are operating in availability mode.
- The deployment is designed in such a way that the service provided by the Wireless APs is not dependent on which Enterasys Wireless Controller the APs associate with. For example, the fast failover feature will not support the deployment in which the two Enterasys Wireless Controllers in availability mode are connected via a WAN link.
- Both the primary and secondary Enterasys Wireless Controllers have equivalent upstream access to the servers on which they depend. For example, both the controllers must have access to the same RADIUS and DHCP servers.
- The users (client devices) that use DHCP must obtain their addresses from a DHCP Server that is external to the Enterasys Wireless Controller.
- Time on all the network elements (both the Enterasys Wireless Controllers in availability pair, Wireless APs, DHCP and RADIUS servers etc.) is synchronized. For more information, see [“Configuring Network Time”](#) on page 2-48.



Note: The fast failover feature works optimally in fast networks (preferably switched networks).

To Configure Fast Failover and Enable Session Availability:

1. Log on to both the primary and secondary Enterasys Wireless Controllers.
2. From the top menu of the primary Enterasys Wireless Controller, click **Wireless Controller**. The **Wireless Controller Configuration** screen is displayed.

- In the left pane, click **Availability**.

The screenshot shows the Enterasys Wireless Controller Configuration interface. The left sidebar contains a navigation menu with the following items: Availability (highlighted), Check Point, Flash, Host Attributes, Installation Wizard, L2 Ports, Location-based Service, Login Management, Mitigator, Mobility Manager, Network Time, Routing Protocols, Secure Connections, SNMP, Software Maintenance, System Maintenance, Topologies, Utilities, and Web Settings. The main content area is titled "Availability Wizard" and includes a "Start" button. Below this is the "Controller Availability Settings" section, which has two radio buttons: "Stand-alone" and "Paired" (selected). The "Paired" option includes a text field for "Wireless IP Address" containing "192.168.3.11", a checkbox for "Current Wireless is primary connection point" (unchecked), a checked checkbox for "Fast Failover", and a "Detect link failure in:" field with the value "2" and a note "(2 - 30 seconds)". The "Synchronization Option" section has two checkboxes: "Synchronize System Configuration" (checked) and "Synchronize Guest Portal Accounts" (unchecked). A "Save" button is located at the bottom right of the configuration area.

- Under **Controller Availability Settings**, select **Paired**.
- Select the **Fast Failover** checkbox.
- Type the appropriate value in the **Detect link failure** box.

The **Detect link failure** field specifies the period within which the system detects link failure after the link has failed. For fast failover configuration, this parameter is tied closely to the **Poll Timeout** parameter on the **AP Properties** tab **Advanced** dialog. The **Poll Timeout** field specifies the period for which the Wireless AP waits before re-attempting to establish a link when its polling to the primary Enterasys Wireless Controller fails.

For the fast failover feature to work within 5 seconds, the **Poll Timeout** value should be 1.5 to 2 times the **Detect link failure** value. For example, if you have set the **Detect link failure** value to 2 seconds, the **Poll Timeout** value should be set to 3 or 4 seconds.

- In the **Synchronization Option** area, select **Synchronize System Configuration**.

This is a global parameter that enables synchronization of VNS configuration components (topology, policy, WLAN Service, VNS) on both controllers paired for availability and/or fast failover.

For more information about synchronization, see [“Using the Sync Summary”](#) on page 7-16.

- Click **Save**.
- Set the Wireless APs' **Poll Timeout** value for fast failover.
 - From the top menu of the primary Enterasys Wireless Controller, click **Wireless APs**. The **Wireless APs Properties** screen is displayed.

- b. In the left pane, click **AP Multi-edit**. The **AP Multi-edit** screen is displayed.

- c. In the **Hardware Types** list, select the hardware type of the Wireless APs that are part of your deployment. You can select multiple hardware types by pressing the **CTRL** key and clicking the hardware in the **Hardware Types** list.
- d. In the **Wireless APs** list, select the Wireless APs for which you want to set the **Poll Timeout** value. You can select multiple Wireless APs by pressing the **CTRL** key and clicking the Wireless APs in the **Wireless APs** list.
- e. In the **Poll Timeout** box, type/edit the appropriate value.
- f. To save your changes, click **Save**.



Note: The fast failover configuration must be identical on both the primary and secondary Enterasys Wireless Controllers. Logs are generated if the configuration is not identical. For more information, see the Enterasys Wireless Convergence Software *Maintenance Guide*.

After you have configured fast failover, you can verify session availability to preserve the user session during the failover.

Verifying Session Availability

To have session availability, you must ensure the following:

- The primary and secondary Enterasys Wireless Controllers are properly configured in 'availability' mode. For more information, see "[Availability](#)" on page 11-1.
- The fast failover feature is properly configured. For more information, see "[Configuring Fast Failover and Enabling Session Availability](#)" on page 11-12.



Note: If you haven't configured the fast failover feature, the **Enable Session Availability** checkbox is not displayed.

- Time on all the network elements — both the Enterasys Wireless Controllers in availability pair, Wireless APs, DHCP and RADIUS servers etc. — is synchronized. For more information, see “[Configuring Network Time](#)” on page 2-48.
- Both the Enterasys Wireless Controllers in fast failover mode must be running the most recent Enterasys Wireless Convergence Software release.
- If you are using **Bridge Traffic Locally at Controller** topology, you must select **None** from the **DHCP Option** drop-down menu.
- The **Bridge Traffic Locally at Controller** must be mapped to the same VLAN on both the primary and secondary Enterasys Wireless Controllers.

To Verify the Session Availability Feature Is Configured Correctly:

1. From the top menu of either of the two controllers, click **Reports**. The **Reports & Displays** screen is displayed.

The screenshot shows the Enterasys web interface for the Reports & Displays section. The header includes the Enterasys logo and tagline "Secure Networks. There's nothing more important than our customers." The navigation bar contains links for Home, Logs, Reports (highlighted), Wireless Controller, Wireless APs, VNS Configuration, Mitigator, Help, and LOGOUT. Below the navigation bar, there are sub-sections for Displays (List of Displays) and Reports (Forwarding Table, OSPF Neighbor, OSPF Linkstate, AP Inventory). The main content area lists various reports and statistics, organized into two columns:

Active Wireless APs	Mesh Statistics
Active Clients by Wireless AP	Active Wireless Load Groups
Active Clients by VNS	Admission Control Statistics by Wireless AP
All Active Clients	Remotable VNS Information
Policy Filter Statistics	External Connections Statistics
Topology Filter Statistics	System Information
Topology Statistics	Manufacturing Information
RADIUS Statistics	
Wireless Controller Port Statistics	
Wireless AP Availability	
Wired Ethernet Statistics by Wireless AP	
Wireless Statistics by Wireless AP	

- From the **Reports and Displays** menu, click **Wireless AP Availability**. The **Wireless Availability Report** is displayed.

Wireless AP Availability - 192.168.4.207 No refresh Refresh every secs

Availability Link is UP

Color Legend:
Wireless AP has active tunnel passing data Wireless AP has backup tunnel Wireless AP not connected No information

Wireless APs List:

[Foreign] 00000012CF737033 00:12:CF:73:70:33 uptime: 2:36:54 10.109.0.254 Connected	[Local] 0409920201201282 0409920201201282 uptime: n/a	[Foreign] 0409920201202222 0409920201202222 00:0F:C8:F0:19:4D uptime: n/a	[Local] 0409920201203211 0409920201203211 00:0F:C8:F0:1B:3D uptime: 2:36:58 10.209.0.33 Connected
[Foreign] 0500005230001257 0500005230001257 00:0F:BB:04:EB:9D uptime: n/a	[Local] 0500006072051386 0500006072051386 uptime: n/a	[Local] 0500006072051389 0500006072051389 uptime: n/a	[Local] 0500006072051392 0500006072051392 uptime: n/a
[Local] 0500006072051395 0500006072051395 uptime: n/a	[Local] 0500006072051399 0500006072051399 uptime: n/a	[Local] 0500006072051400 0500006072051400 uptime: n/a	[Local] 0500006072051404 0500006072051404 uptime: n/a
[Local] 0500006072051405 0500006072051405 uptime: n/a	[Local] 0500006072051406 0500006072051406 uptime: n/a	[Local] 0500006072051416 0500006072051416 uptime: n/a	[Local] 0500006072051427 0500006072051427 uptime: n/a
[Local] 0500006072051428 0500006072051428 uptime: n/a	[Local] 0500006072051431 0500006072051431 uptime: n/a	[Local] 0500006072051434 0500006072051434 uptime: n/a	[Local] 0500006072051452 0500006072051452 uptime: n/a
[Local] 0500006072051459 0500006072051459 uptime: n/a	[Local] 0500006072051479 0500006072051479 uptime: n/a	[Local] 0500006072051491 0500006072051491 uptime: n/a	[Foreign] 1111111111111111 11111 1111111111111111 uptime: n/a
[Local] J302000007515346 0002000007515346 uptime: n/a			

- Check the statement at the top of the screen.

If the statement reads **Availability link is up**, the availability feature is configured correctly. If the statement reads **Availability link is down**, check the configuration error in logs. For more information on logs, see the Enterasys Wireless Convergence Software *Maintenance Guide*.

Verify Synchronization

To verify that all elements have been synchronized correctly, navigate to the VNS tab on both the primary and secondary Enterasys Wireless Controllers, and confirm that the topologies, WLAN services, policies and desired VNSs are displayed as **[synchronized]**.

You can verify this by selecting the appropriate tabs and then inspecting the Synchronized flags or by navigating to VNS Configuration > Global > Sync Summary.

The screenshot shows the 'Virtual Network Configuration' interface for 'Global' settings. The 'Synchronize System Configuration' checkbox is checked. The 'Global Settings' section shows 'Global Settings' as 'Unknown'. The 'Virtual Networks' section contains a table with the following data:

Name	Sync Status	Action
anV1	<input type="checkbox"/>	Synchronize Now
anV2	<input type="checkbox"/>	Synchronize Now
lab10-aaa	<input checked="" type="checkbox"/> Unknown	

The 'WLAN Services' section contains a similar table:

Name	Sync Status	Action
anV1WLAN	<input type="checkbox"/>	Synchronize Now
anV2WLAN	<input type="checkbox"/>	Synchronize Now
lab10-aaa	<input checked="" type="checkbox"/> Unknown	

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

Configuration synchronization:

- VNS configuration related synchronization will be supported with legacy or fast failover availability configuration as long as there is an availability link established.
- Synchronization for VNS, WLAN Services, Policies, Topologies, and Rate Limit Profiles can be enabled/disabled individually.
- VNS, WLAN Service, Policy, Topology, and Rate Limit Profile configuration will be dynamically synchronized when synchronization is enabled individually between a pair of Enterasys Wireless Controllers.

MU session synchronization:

- MU session synchronization will be supported only when there is fast failover configured between two Enterasys Wireless Controllers.
- If mobility is disabled, MU session with Bridge Traffic Locally at AP, Bridge Traffic Locally at Controller, and Routed topologies will all be synchronized between a pair of Enterasys Wireless Controllers.
- If mobility is enabled, an MU session with Routed topologies will not be synchronized.

Viewing the Wireless AP Availability Display

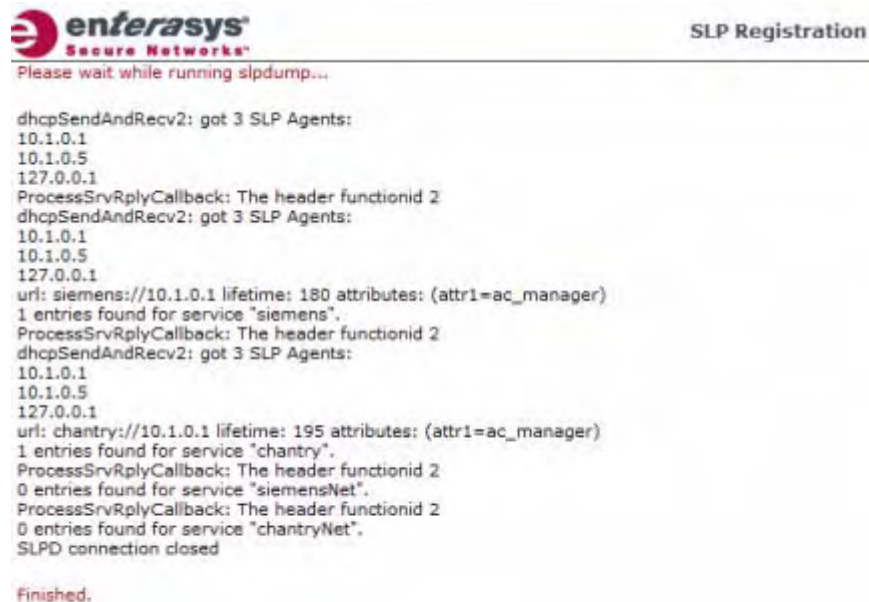
For more information, see [“Viewing the Wireless AP Availability Display”](#) on page 15-3.

Viewing SLP Activity

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

To View SLP Activity:

1. From the top menu, click **Wireless APs**. 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.



```
dhcpcSendAndRecv2: got 3 SLP Agents:
10.1.0.1
10.1.0.5
127.0.0.1
ProcessSrvRplyCallback: The header functionid 2
dhcpcSendAndRecv2: got 3 SLP Agents:
10.1.0.1
10.1.0.5
127.0.0.1
url: siemens://10.1.0.1 lifetime: 180 attributes: (attr1=ac_manager)
1 entries found for service "siemens".
ProcessSrvRplyCallback: The header functionid 2
dhcpcSendAndRecv2: got 3 SLP Agents:
10.1.0.1
10.1.0.5
127.0.0.1
url: chantry://10.1.0.1 lifetime: 195 attributes: (attr1=ac_manager)
1 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.
```

Configuring Mobility

This chapter describes the mobility concept, including:

For information about...	Refer to page...
Mobility Overview	12-1
Mobility Domain Topologies	12-3
Configuring Mobility Domain	12-4

Mobility Overview

The Enterasys Wireless Convergence Software system allows up to 12 Enterasys 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 Enterasys Wireless Controllers.

The solution introduces the concept of a mobility manager; one Enterasys 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 Enterasys Wireless Controller—the Enterasys Wireless Controller that it first connected to. The WLAN Service on each Enterasys 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 Enterasys 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 EnterasysNet.

-
- 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 Enterasys 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 Enterasys Wireless Controllers and the Wireless APs is called the **Mobility Domain**.



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

Mobility Domain Topologies

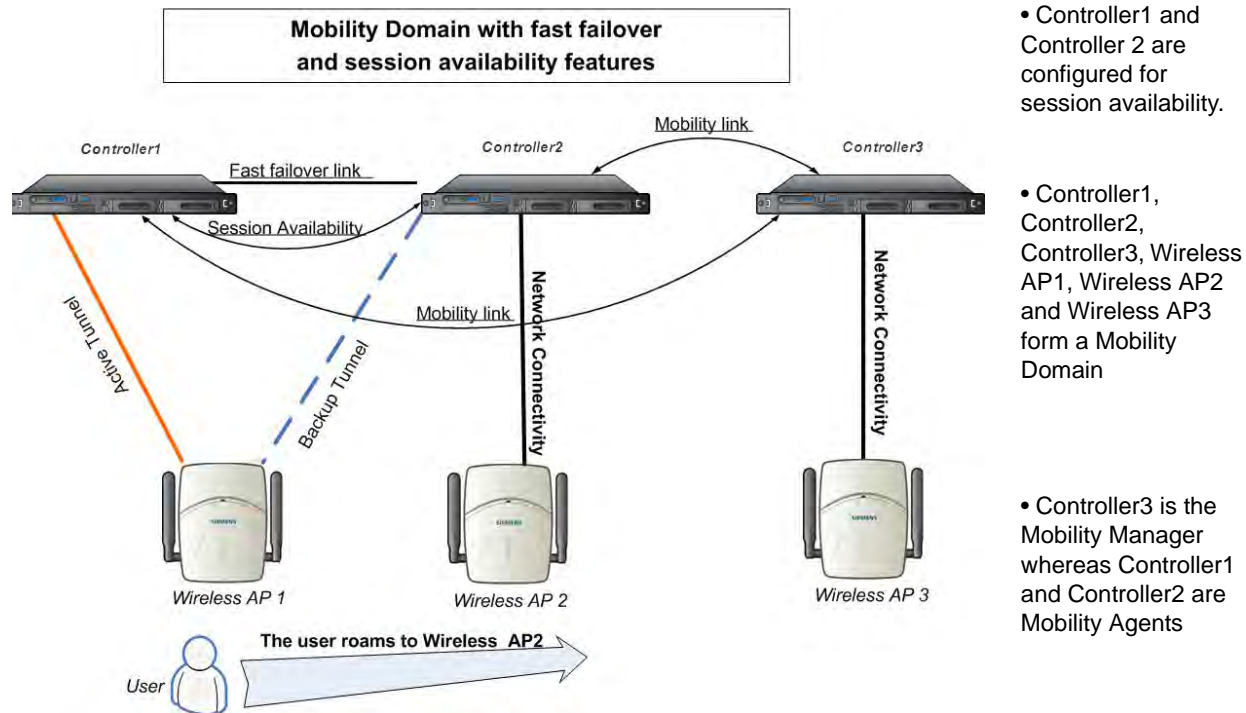
You can configure a mobility domain in the following scenarios:

- 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 Enterasys Wireless Controllers that are part of the mobility domain. For more information, see “[Configuring Network Time](#)” on page 2-48.

Figure 12-1 Mobility Domain with Fast Failover and Session Availability Features



- Controller1 and Controller 2 are configured for session availability.

- Controller1, Controller2, Controller3, Wireless AP1, Wireless AP2 and Wireless AP3 form a Mobility Domain

- Controller3 is the Mobility Manager whereas Controller1 and Controller2 are Mobility Agents

- The user’s home session is with Controller1.
- When the user roams from Wireless AP 1 to Wireless AP 2, he establishes his home session with Controller2.
- 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 Controller1 for that user.
- In response to the heart beat message from the mobility manager (Controller3), the Controller2 sends updates that the user has a new home on Controller2. 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 Controller2.
 - In response to the heart beat message from the mobility manager (Controller3), the Controller2 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 Controller1 to Controller2.
 - Wireless AP 1 establishes active session with Controller2. Wireless AP 2 is not impacted by the failover.

Configuring Mobility Domain

If you are configuring a mobility domain with availability or session availability, you must synchronize time on all the Enterasys Wireless Controllers that are part of your mobility domain. For more information, see “[Configuring Network Time](#)” on page 2-48.

Designating a Mobility Manager

To Designate a Mobility Manager:

1. From the top menu, click **Wireless Controller**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.

The screenshot shows the Enterasys Wireless Controller Configuration interface. The top navigation bar includes Home, Logs, Reports, **Wireless Controller**, Wireless APs, WNS Configuration, Mitigator, Help, and LOGOUT. The left sidebar lists various configuration options, with **Mobility Manager** highlighted in red. The main content area is titled **Mobility Manager Settings** and features a **Mobility** checkbox that is checked. Below this, there are two radio button options: **This Wireless Controller is a Mobility Manager** (selected) and **This Wireless Controller is a Mobility Agent**. The selected option is expanded to show settings: Port (physical 2 (1,2,3,4)), Heartbeat (1 seconds), SLP Registration (Disabled), and Permission List (Agent IP Address (State)). There are buttons for Approve, Delete, and Add next to the Permission List. The Security Mode is set to **Allow all mobility agents to connect**. A Save button is located at the bottom right of the settings area.

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 Enterasys 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 Enterasys Wireless Controller on the network as a mobility manager, all other Enterasys Wireless Controllers must be set up as mobility agents.

Designating a Mobility Agent

To Designate a Mobility Agent:

1. From the top menu, click **Wireless Controller**. 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.

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

The screenshot shows the 'Wireless Controller Configuration' interface. The 'Mobility Manager Settings' section is active, with the 'Mobility' checkbox checked. Under 'Mobility', the radio button for 'This Wireless Controller is a Mobility Agent' is selected. The 'Port' dropdown is set to 'physical 2 (1.2.3.4)' and the 'Discovery Method' dropdown is set to 'SLPD'. A 'Save' button is visible at the bottom right of the configuration area.

- From the **Port** drop-down list, select the **port** on the Enterasys Wireless Controller to be used for the mobility agent process. Ensure that the port selected is routable on the network.
- 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 EnterasysNET 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.
- To save your changes, click **Save**.

For information about viewing mobility manager displays, see [“Viewing Displays for the Mobility Manager”](#) on page 15-12.

Working with Third-party APs

You can set up the Enterasys 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:

For information about...	Refer to page...
Define Authentication by Captive Portal for the Third-party AP WLAN Service	13-1
Define the Third-party APs List	13-1
Define Filtering Rules for the Third-party APs	13-2

Define Authentication by Captive Portal for the Third-party AP WLAN Service

802.1x Authentication is not supported directly by the Enterasys 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 “[Configuring Captive Portal for Internal or External Authentication](#)” on page 6-24.

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.

Define Filtering Rules for the Third-party APs

1. Because the third-party APs are mapped to a physical topology, you must define the Exception filters on the physical topology, using the **Exception Filters** tab. For more information, see “[Exception Filtering](#)” on page 4-9.
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 “[Multicast Filtering](#)” on page 4-13.

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 Enterasys 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 Enterasys Wireless Controller system:

- A third-party AP exchanges data with the Enterasys 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 Enterasys 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.

Working with the Mitigator

This chapter describes Mitigator concepts, including:

For information about...	Refer to page...
Mitigator Overview	14-1
Analysis Engine Overview	14-2
Enabling the Analysis and Data Collector Engines	14-2
Viewing the Mitigator Logs	14-4
Running Mitigator Scans	14-5
Working with Mitigator Scan Results	14-7
Working with Friendly APs	14-10
Maintaining the Mitigator List of APs	14-11
Viewing the Scanner Status Report	14-12

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 Enterasys 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 Enterasys 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.

Analysis Engine Overview

The Analysis engine relies on a database of known devices on the Enterasys Wireless 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 Enterasys Wireless Controller with its RF Data Collector enabled and associated with the Analysis Engine on this Enterasys 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 Enterasys Wireless Controller that has its RF Data Collector enabled and has been associated with the Analysis Engine on this Enterasys 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.

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 top menu, click **Wireless Controller**. The **Wireless Controller Configuration** screen is displayed.

- In the left pane, click **Mitigator**. The **Mitigator Configuration** screen is displayed.

The screenshot shows the 'Mitigator Configuration' page. On the left is a navigation menu with 'Mitigator' highlighted. The main content area has a title 'Mitigator Configuration' and a checkbox for 'Mitigator Analysis Engine'. Below this is a section for 'Remote Collection Engines' which is currently empty, with a message 'There are no Remote Collection Engine configured'. To the right of this section are input fields for 'IP Address', 'Poll interval' (set to 5 seconds), and 'Poll retry count' (set to 3). At the bottom of the configuration area are 'Add' and 'Delete' buttons. A 'Save' button is located at the bottom right of the page. A red link 'Add New Collection Engine' is visible at the bottom left of the configuration area.

- Enable the Mitigator Analysis Engine, by selecting the **Mitigator Analysis Engine** checkbox.

To Add a New Remote Collection Engine:

- In the **IP Address** box, enter the IP address of the remote collection engine.
- In the **Poll interval** box, enter the poll time interval in seconds.
- In the **Poll retry count**, enter the number of poll retries.
- Click **Add**.
- To save the list of collection engines, click **Save**.

Viewing the Mitigator Logs

To View Mitigator Logs:

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

The screenshot shows the Mitigator web interface. At the top, there is a navigation bar with the Enterasys logo and the text "Secure Networks. There's nothing more important than our customers." The navigation menu includes: Home | Logs | Reports | Wireless Controller | Wireless APs | VMS Configuration | **Mitigator** | Help | LOGOUT. Below the navigation bar, there is a breadcrumb trail: Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace.

The main content area is titled "Rogue Detection" and contains three tabs: Scan Groups, Friendly APs, and AP Maintenance. The "Rogue Detection" tab is active, displaying a table of detected rogue devices. The table has four columns: MAC Address, First Detected, Threat Type, and Beacon Summary.

MAC Address	First Detected	Threat Type	Beacon Summary										
00:1F:45:6E:2D:23 [a]	11/04/04 16:17:34 (NGAP-0013)	Unknown AP; Invalid SSID	SSID=Wireless; Ch=48; Enc=WEP										
<table border="1"> <thead> <tr> <th>Last Reported by</th> <th>Time</th> <th># Rpts</th> <th>Scan Group</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td>NGAP-0013</td> <td>11/04/04 16:17:34</td> <td>1</td> <td>CNL-208</td> <td>SSID=Wireless; Ch=48; RSSI=37; Enc=WEP</td> </tr> </tbody> </table> <p>Manufacturer: Enterasys Add to Friendly List Delete</p>				Last Reported by	Time	# Rpts	Scan Group	Details	NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=Wireless; Ch=48; RSSI=37; Enc=WEP
Last Reported by	Time	# Rpts	Scan Group	Details									
NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=Wireless; Ch=48; RSSI=37; Enc=WEP									
00:1F:45:6D:84:46 [a]	11/04/04 16:17:34 (NGAP-0013)	Unknown AP; Invalid SSID	SSID=C200-05-WPA2-short-rekey; Ch=36; Enc=WEP										
<table border="1"> <thead> <tr> <th>Last Reported by</th> <th>Time</th> <th># Rpts</th> <th>Scan Group</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td>NGAP-0013</td> <td>11/04/04 16:17:34</td> <td>1</td> <td>CNL-208</td> <td>SSID=C200-05-WPA2-short-rekey; Ch=36; RSSI=44; Enc=WEP</td> </tr> </tbody> </table> <p>Manufacturer: Enterasys Add to Friendly List Delete</p>				Last Reported by	Time	# Rpts	Scan Group	Details	NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=C200-05-WPA2-short-rekey; Ch=36; RSSI=44; Enc=WEP
Last Reported by	Time	# Rpts	Scan Group	Details									
NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=C200-05-WPA2-short-rekey; Ch=36; RSSI=44; Enc=WEP									
00:1F:45:47:A5:F0 [a]	11/04/04 16:17:34 (NGAP-0013)	Unknown AP; Invalid SSID	SSID=CNL-20#BAP1; Ch=40; Enc=None										
<table border="1"> <thead> <tr> <th>Last Reported by</th> <th>Time</th> <th># Rpts</th> <th>Scan Group</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Last Reported by	Time	# Rpts	Scan Group	Details					
Last Reported by	Time	# Rpts	Scan Group	Details									

At the bottom of the interface, there are controls for refreshing the data: No refresh Refresh every seconds Apply Refresh Clear Detected Rogues Rogue Summary

1. To filter the log events by severity, **Critical**, **Major**, **Minor**, **Info**, **All**, and **Trace**, click the appropriate log severity. The log messages are displayed in chronological order.

The screenshot shows the Mitigator web interface. At the top, there is a navigation bar with links for Home, Logs, Reports, Wireless Controller, Wireless APs, VMS Configuration, and Mitigator. Below the navigation bar, there is a status bar indicating 'Mitigator Analysis Engine Disabled' and 'Logs: Critical'. The main content area displays a table with columns for Timestamp, Type, Component, and Log Message. The table is currently empty, displaying the message 'There are no rogue critical log messages found.' At the bottom of the interface, there are buttons for 'Clear Rogue Logs', 'Export', and 'Refresh', along with a pagination control showing '0 rogue critical log messages found' and 'Total pages: 1'.

2. To sort the events by **Timestamp**, **Type**, **Component**, or **Log Message**, click the appropriate column heading.
3. To refresh the Mitigator log screen, click **Refresh**.
4. To export the Mitigator log screen, click **Export**. The **File Download** dialog is displayed.
5. Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

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 top menu, click **Mitigator**. The **Mitigator** screen is displayed.

- Click the **Scan Groups** tab.

The screenshot shows the 'Add New Scan Group' interface in the Mitigator web application. The scan group name is 'CNL-208'. The configuration includes: Radio: Both; Channel List: All; Scan Type: Active; Channel Dwell Time: 300 milliseconds; Scan Time Interval: 10 (10-120) minutes; Scan Activity: Running. A table of Wireless APs is displayed, listing MAC addresses and radio types (R1, R2). A red warning message at the bottom states: '* Enable scanning on a Wireless AP can disrupt client service'.

- In the **Scan Group Name** box, type a unique name for this scan group.
- 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. Enterasys recommends that the Scan Groups represent geographical groupings of Wireless APs.

- 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.
- 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.
- 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**.

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.

Viewing Mitigator Scan Results

To View Mitigator Scan Results:

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

- Click the **Rogue Detection** tab.

enterasys
Secure Networks™ There's nothing more important than our customers.

Home | Logs | Reports | Wireless Controller | Wireless APs | VMS 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										
00:1F:45:6E:2D:23 [a]	11/04/04 16:17:34 (NGAP-0013)	Unknown AP; Invalid SSID	SSID=Wireless; Ch=48; Enc=WEP										
<table border="1"> <thead> <tr> <th>Last Reported by</th> <th>Time</th> <th># Rpts</th> <th>Scan Group</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td>NGAP-0013</td> <td>11/04/04 16:17:34</td> <td>1</td> <td>CNL-208</td> <td>SSID=Wireless; Ch=48; RSSI=37; Enc=WEP</td> </tr> </tbody> </table> <p>Manufacturer: Enterasys Add to Friendly List Delete</p>				Last Reported by	Time	# Rpts	Scan Group	Details	NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=Wireless; Ch=48; RSSI=37; Enc=WEP
Last Reported by	Time	# Rpts	Scan Group	Details									
NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=Wireless; Ch=48; RSSI=37; Enc=WEP									
00:1F:45:6D:84:46 [a]	11/04/04 16:17:34 (NGAP-0013)	Unknown AP; Invalid SSID	SSID=C200-05-WPA2-short-rekey; Ch=36; Enc=WEP										
<table border="1"> <thead> <tr> <th>Last Reported by</th> <th>Time</th> <th># Rpts</th> <th>Scan Group</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td>NGAP-0013</td> <td>11/04/04 16:17:34</td> <td>1</td> <td>CNL-208</td> <td>SSID=C200-05-WPA2-short-rekey; Ch=36; RSSI=44; Enc=WEP</td> </tr> </tbody> </table> <p>Manufacturer: Enterasys Add to Friendly List Delete</p>				Last Reported by	Time	# Rpts	Scan Group	Details	NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=C200-05-WPA2-short-rekey; Ch=36; RSSI=44; Enc=WEP
Last Reported by	Time	# Rpts	Scan Group	Details									
NGAP-0013	11/04/04 16:17:34	1	CNL-208	SSID=C200-05-WPA2-short-rekey; Ch=36; RSSI=44; Enc=WEP									
00:1F:45:47:A5:F0 [a]	11/04/04 16:17:34 (NGAP-0013)	Unknown AP; Invalid SSID	SSID=CNL-20-#BAP1; Ch=40; Enc=None										
<table border="1"> <thead> <tr> <th>Last Reported by</th> <th>Time</th> <th># Rpts</th> <th>Scan Group</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Last Reported by	Time	# Rpts	Scan Group	Details					
Last Reported by	Time	# Rpts	Scan Group	Details									

No refresh
 Refresh every seconds
 Apply Refresh Clear Detected Rogues Rogue Summary

- To modify the page's refresh rate, type a time (in seconds) in the **Refresh every __ seconds** box.
- Click **Apply**. The new refresh rate is applied.



Note: The refresh rate only applies to information contained on the Rogue Detection tab screen. Actual new results will be changed after the Scan Time Interval has been reached.

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

enterasys [®] Secure Networks [®]		Rogue Summary
Number of potential Rogues detected:		491
Number of Infrastructure Threats:		491
Unknown AP; Invalid SSID	487	
Unknown AP; Valid SSID	3	
Known AP; Invalid SSID Mapping	0	
Known AP; Invalid SSID	0	
Known AP; Valid SSID; Suppress Conflict	0	
Inactive AP; Valid SSID	1	
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		
Refresh		Close

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



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

Adding an AP from the Scan Results to the List of Friendly APs

To Add an AP from the Mitigator Scan Results to the List of Friendly APs:

- From the top menu, click **Mitigator**. The **Mitigator** screen is displayed.
- Click the **Rogue Detection** tab.
- 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.

Deleting an AP from the Scan Results

To Delete an AP from the Mitigator Scan Results:

- From the top menu, click **Mitigator**. The **Mitigator** screen is displayed.
- Click the **Rogue Detection** tab.
- To delete a specific AP from the Mitigator scan results, click the corresponding **Delete** button. The AP is removed from the list.

- To clear all rogue access points from the Mitigator scan results, click **Clear Detected Rogues**. All APs are removed from the list.

Working with Friendly APs

Viewing Friendly APs

To View the Friendly APs:

- From the top menu, click **Mitigator**. The **Mitigator** screen is displayed.
- Click the **Friendly APs** tab.

The screenshot shows the Mitigator web interface. At the top, there is a navigation bar with the Enterasys logo and the text "Secure Networks™ There's nothing more important than our customers." The navigation bar includes links for Home, Logs, Reports, Wireless Controller, Wireless APs, VMS Configuration, Mitigator, Help, and LOGOUT. Below the navigation bar, there is a breadcrumb trail: Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace. The main content area has four tabs: Rogue Detection, Scan Groups, Friendly APs (which is selected), and AP Maintenance. Under the Friendly APs tab, there is a section titled "Friendly AP Definitions" with a table. The table has five columns: MAC Address, SSID, Channel, Description, and Manufacturer. The table is currently empty, and the text "There are no Friendly AP defined" is displayed below the table. Below the table, there are input fields for MAC Address, SSID, Channel, and Description, along with Add, Delete, and Save buttons.

Adding Friendly APs Manually

To Add Friendly APs Manually:

- From the top menu, click **Mitigator**. The **Mitigator** screen is displayed.
- Click the **Friendly APs** tab.
- 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.

Deleting Friendly APs

To Delete a Friendly AP:

1. From the top 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**.

Modifying Friendly APs

To Modify a Friendly AP:

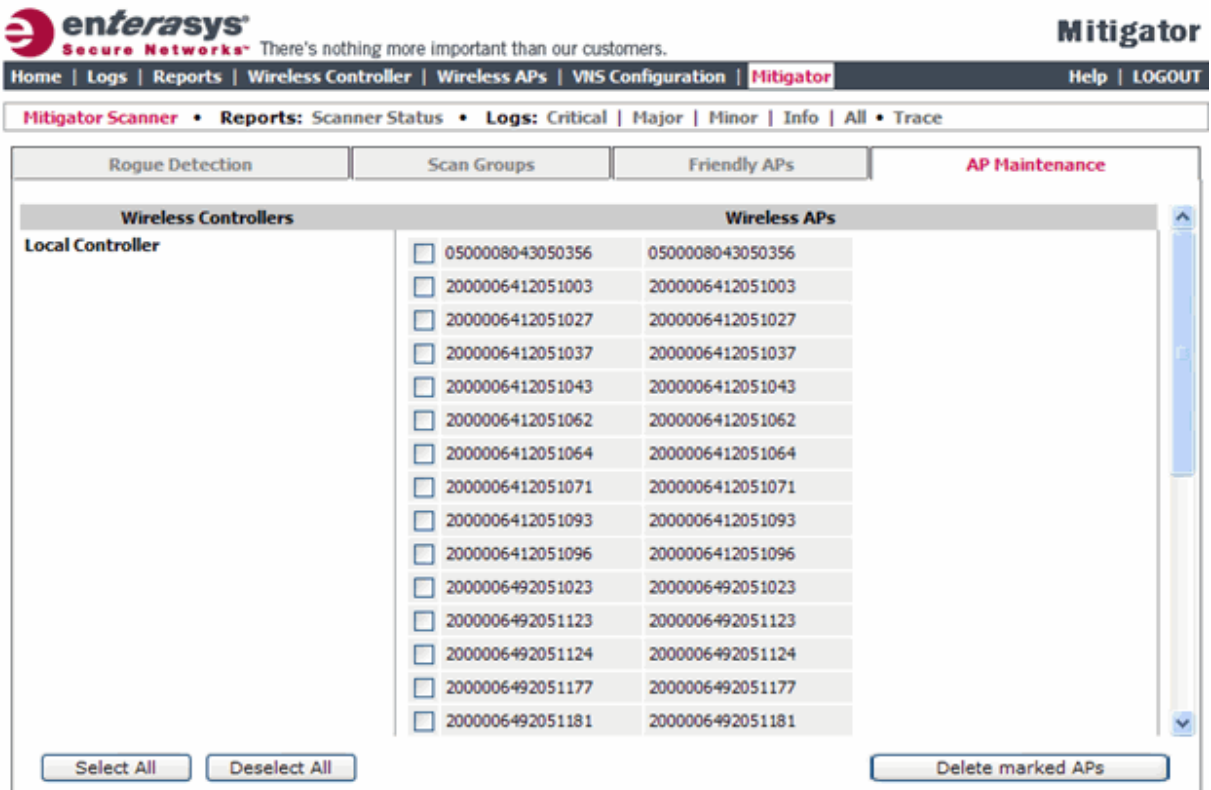
1. From the top menu, click **Mitigator**. The **Mitigator** screen is displayed.
2. Click the **Friendly APs** tab.
3. In the **Friendly AP Definitions** list, click the access point you want to modify.
4. Modify the access point by making the appropriate changes.
5. To save your changes, click **Save**.

Maintaining the Mitigator List of APs

To Maintain the Wireless APs:

1. From the top 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.



The screenshot shows the Mitigator Scanner interface. At the top, there is a navigation bar with the Enterasys logo and the text "Secure Networks™ There's nothing more important than our customers." The navigation bar includes links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration, Mitigator, Help, and LOGOUT. Below the navigation bar, there is a breadcrumb trail: Mitigator Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace. The main content area is divided into four tabs: Rogue Detection, Scan Groups, Friendly APs, and AP Maintenance. The AP Maintenance tab is active, showing a table of Wireless APs. The table has two columns: Local Controller and Wireless APs. The Local Controller column contains the text "Local Controller". The Wireless APs column contains a list of 16 APs, each with a checkbox and a unique ID. The APs are listed in a table format with two columns: Local Controller and Wireless APs. The Local Controller column contains the text "Local Controller". The Wireless APs column contains a list of 16 APs, each with a checkbox and a unique ID. The APs are listed in a table format with two columns: Local Controller and Wireless APs. The Local Controller column contains the text "Local Controller". The Wireless APs column contains a list of 16 APs, each with a checkbox and a unique ID. At the bottom of the table, there are three buttons: "Select All", "Deselect All", and "Delete marked APs".

Local Controller	Wireless APs
<input type="checkbox"/>	0500008043050356
<input type="checkbox"/>	2000006412051003
<input type="checkbox"/>	2000006412051027
<input type="checkbox"/>	2000006412051037
<input type="checkbox"/>	2000006412051043
<input type="checkbox"/>	2000006412051062
<input type="checkbox"/>	2000006412051064
<input type="checkbox"/>	2000006412051071
<input type="checkbox"/>	2000006412051093
<input type="checkbox"/>	2000006412051096
<input type="checkbox"/>	2000006492051023
<input type="checkbox"/>	2000006492051123
<input type="checkbox"/>	2000006492051124
<input type="checkbox"/>	2000006492051177
<input type="checkbox"/>	2000006492051181

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



Note: The selected APs are deleted from the Mitigator database, not from the Enterasys Wireless Controller database. You can delete the APs from the Enterasys 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.

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 top 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 - 192.168.3.45 No refresh Refresh every 30 seconds 

Data as of Jul 12, 2011 10:58:53 am

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 Enterasys 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.

Working with Reports and Displays

This chapter describes the various reports and displays available in the Enterasys Wireless Convergence Software system.

For information about...	Refer to page...
Available Reports and Displays	15-1
Viewing Reports and Displays	15-2
Viewing the Wireless AP Availability Display	15-3
Viewing Statistics for Wireless APs	15-4
Viewing Load Balance Group Statistics	15-8
Viewing the System Information and Manufacturing Information Displays	15-10
Viewing Displays for the Mobility Manager	15-12
Viewing Reports	15-14
Call Detail Records (CDRs)	15-17

Available Reports and Displays

The following displays are available in the Enterasys Wireless Convergence Software system:

- 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
- Mesh Statistics

- Active Wireless Load Groups
- Admission Control Statistics by Wireless AP
- Remotable VNS Information
- 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.

Viewing Reports and Displays

To View Reports and Displays:

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

enterasys
Secure Networks™ There's nothing more important than our customers.

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
- Mesh 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.

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

Lab-126-10 - Reports - Active Wireless APs No refresh Refresh every 30 sec Apply

Wireless AP	Serial	AP IP	Clients	Home	Mesh/WDS Children ¹	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	Radio 1 Mode Ch/Tx g Pwr	Radio 2 Mode Ch/Tx g Pwr
05000523000824	05000523000824	10.1.0.55	0	Local	0	3 d, 19:43:31	124785	408174	13653296	44750619	3 d, 19:55:40	off -	off - b/g 11/18dBm on
050008043050236	050008043050236	10.1.0.53	0	Local	0	3 d, 19:43:07	127624	398622	14506394	42438884	3 d, 19:42:18	off -	off - b/g/n 11/18dBm on
Summary	3 active APs		0										

1 Channel selection in progress
2 DNS Timeout
3 Number of active immediate Mesh/WDS child APs

Data as of Feb 23, 2011 12:14:40 pm

Refresh Export Close



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.

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 Enterasys 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 Enterasys Wireless Controller.
- The color in the upper pane of the box represents the state of the tunnel that is established to the current Enterasys Wireless Controller.



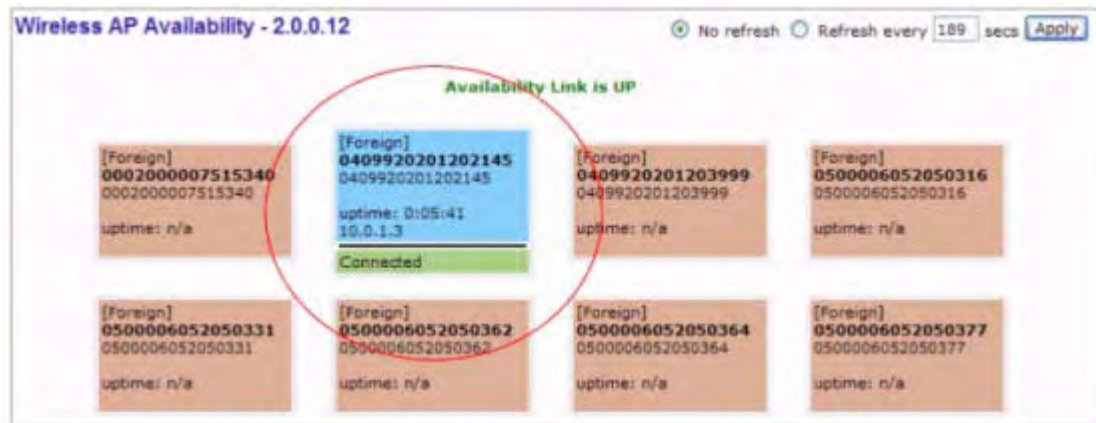
Note: The current Enterasys Wireless Controller is the one on which the Wireless AP Availability report is viewed.

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

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

- Controller1 and Controller2 are paired in session availability
- A Wireless AP has established an active tunnel to Controller1.
- The same Wireless AP has established a backup tunnel to Controller2.

If you open the Wireless AP Availability report on Controller2, the report will appear as follows:



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

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 top menu, click **Reports**. The **Reports & Displays** screen is displayed.

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

Lab126-10 - Reports - Wired Ethernet Statistics by Wireless APs No refresh Refresh every 30 secs

0500005230000824 **Status** Approved **IP Address** 10.1.0.53
MAC Address 00:0F:BB:04:E9:5C

Statistics	Sent	Received
Discarded Packets	0	0
Total Errors	0	0
Unicast Packets	11937	15742
Multicast Packets	619	54223
Broadcast Packets	27	3780
Total Packets	12583	73745
Total Bytes	2654835	8200206

- 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:

- From the top menu, click **Reports**. The **Reports & Displays** screen is displayed.
- Click the **Wireless Statistics by Wireless AP** display option. The **Wireless Statistics by Wireless APs** display opens in a new browser window.

EWC - Reports - Wireless Statistics by Wireless APs No refresh Refresh every 30 secs

0409920201201458 **AP Status:** Approved **AP IP Address:** 10.13.0.50 **Radio1** Radio2
0500008043050241

MAC Address 00:1A:E8:14:2A:21 **Mode** a
SSID Lab126-13-Int-CP **Channel** 153: 5765 MHz
Current Power Level 17 dBm

Associated Clients There is 1 active client on this radio
Active immediate WDS child APs There are no WDS children

Statistics	Sent	Received
Discarded Packets	0	0
Errors	1599	3921
Unicast Packets	48	117
Multicast Packets	0	241
Broadcast Packets	60	0
Total Successful Packets	108	358
Total Successful Bytes	20208	31469

Statistics	802.11 MIB Values
WEP ICV Error Count	0
WEP Excluded Count	0
Retry Count	4
Multiple Retry Count	1
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	1200

Data as of Apr 07, 2011 05:36:47 pm

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.

EWC - Reports - Associated Clients - AP 0500008043050241, Radio 802.11a/n

No refresh Refresh every 30 secs

Client		Received			Transmitted			Counts				
MAC Addr	RSS (dBm)	Rate (Mbps)	Frames	Errors	Rate (Mbps)	Frames	Errors	Auth.	Deauth.	Assoc.	Disassoc.	Reassoc.
00:13:CE:C7:4C:91	-55	54	373	0	50	48	0	3	0	3	0	0

Data as of Apr 07, 2011 05:37:40 pm

To View Active Clients by Wireless AP Statistics:

1. From the top menu, click **Reports**. The **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.

Lab126-10 - Reports - Active Clients by Wireless AP

0500005230000824 0500005230000824

0500005230000824

No refresh Refresh every 30 secs

AP	Client IP	Client MAC	RSS (dBm)	Auth. Prio.	Radio Protocol	RSS (dBm)	Time Conn.	Discard Filter	Topology	App(Rate/Bytes)	Packets Rec'd (Mac)	Bytes Rec'd (Mac)	U. Dropped Due To Rate	U. Dropped Due To Rate	U. Dropped Due To Rate	U. Last Refresh
No Client is connected to this Wireless AP.																

Active Users: 0
Auth. Users: 0
Non-Auth. Users: 0

Search Client By: user name

Data as of Jul 05, 2013 02:03:48 pm

- 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 Mesh VNS Wireless AP Statistics:

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

- Click the **Mesh Statistics** display option. The **Mesh Statistics** display opens in a new browser window.

C2400-9 - Reports - Mesh Statistics No refresh Refresh every 30 secs Apply

AP Name	SSID	Rx RSS	Hops	Rx/Tx Rate	Backhaul Channel	Parent Change	Rx Frames	Tx Frames	Rx/Tx Errors	Retry Percent
AP21_3610[MP]	n/a	n/a	0	n/a	n/a	n/a	n/a	n/a	n/a	n/a
- WP101_3610	mesh with space	-37	1	327/294	(36,+1):(5180,5200)	30	10710755	8382743	626/8	3
- GP03_3610-1	mesh with space	-42	1	323/267	(36,+1):(5180,5200)	31	4870778	1003714	265/2	7
AP23_3610[MP]	n/a	n/a	0	n/a	n/a	n/a	n/a	n/a	n/a	n/a
AP32_3610[MP]	n/a	n/a	0	n/a	n/a	n/a	n/a	n/a	n/a	n/a
- WP302_3610	mesh with space	-26	1	276/220	(36,+1):(5180,5200)	2	535090	180574	0/0	35
- WP303_3610	mesh with space	-16	2	343/200	(36,+1):(5180,5200)	4	442966	52001	3/0	15
- GP04_3610-1	mesh with space	-36	1	332/227	(36,+1):(5180,5200)	30	4108075	199740	183/1	21
- GP02_3610-1	mesh with space	-28	1	223/258	(36,+1):(5180,5200)	30	4173710	424241	342/0	12
- WP301_3610-1	mesh with space	-22	2	296/278	(36,+1):(5180,5200)	7	576600	112895	1/0	0
- GP05_3610-1	mesh with space	-26	2	205/243	(36,+1):(5180,5200)	28	6619357	2741269	283/5	0
AP21_3610	mesh with space	-26	1	231/288	(36,+1):(5180,5200)	29	6333309	2982527	137/4	0
- GP08_3610-1	mesh with space	-11	2	253/189	(36,+1):(5180,5200)	13	4855546	792943	134/0	0
- GP07_3610-1	mesh with space	-11	2	233/230	(36,+1):(5180,5200)	26	4271016	210279	219/9	1
AP22_3610	mesh with space	-22	1	218/191	(36,+1):(5180,5200)	32	5774752	2356880	168/6	6
- GP09_3610-1	mesh with space	-21	1	253/227	(36,+1):(5180,5200)	28	4851890	1215266	217/1	5
- GP06_3610-1	mesh with space	-14	2	256/251	(36,+1):(5180,5200)	19	5383498	2010208	265/3	0
- GP01_3610-1	mesh with space	-31	0	346/291	(149,+1):(5745,5765)	27	4275258	409123	1118/3	10

Data as of Apr 08, 2011 11:38:01 am Refresh Report Close



Note: The Rx RSS value on the **Mesh Statistics** display represents the received signal strength (in dBm).

To View Admission Control Statistics by Wireless AP:

- From the top menu, click **Reports**. The **Reports & Displays** screen is displayed.
- Click the **Admission Control Statistics by Wireless AP** display option. The **Admission Control Statistics by Wireless AP** display opens in a new browser window.

Lab125-10 - Reports - Admission Control Statistics by Wireless AP No refresh Refresh every 30 secs Apply

Users: 0500005230000824 0500005230000824

Client IP	Client MAC	Protocol	BSS MAC	SSID	AC	Direction	HDR [kps]	RTG [bytes]	SSA	Rate [kps]	Violations [kps]
							DL	UL	DL	UL	DL
No Client is connected to this Wireless AP											

Active Users: 0 Search Client by user name

Data as of Jul 13, 2011 02:42:41 pm Refresh Export Close

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)

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 top menu, click **Reports**. The **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. Reports display differently when reporting on client balance load groups and radio preference load groups.



About Radio Preference/Load Control Statistics

The statistics reported for each radio preference load balance group are:

- **Members** — The number of AP members

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

- **AP** — AP name
- **Band Preference**

- **Status** – The operational status: enabled or disabled
- **Probes Declined** – The number of probes declined
- **Auth/Assoc Requests Declined** – The number of authentications or associations declined
- **Load Control**
 - **Radio 1**
 - **Status** – The operational status: enabled or disable
 - **Rejected** – The number of clients declined at the first association attempt
 - **Radio 2**
 - **Status** – The operational status: enabled or disabled
 - **Rejected** – The number of clients declined at the first association attempt
 - **Returned** – The number of clients declined at the second association attempt

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.

About Client Balancing Statistics Reports

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
APXX_3643-RDR_Ping	1	0	Balanced	0	0	0
APXX_3643-RDR_Ping	2	3	Under-Loaded	0	0	0

Members: 2 Clients: 11 Average Load: 5.5

In a client balancing/load control statistics report, the statistics reported for each client balancing load balance group are:

- **Members** – 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.

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.

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 top menu, click **Reports**. The **Reports & Displays** screen is displayed.

- Click the **System Information** display option. The **System Information** display opens in a new browser window.

Lab126-10 - Reports - System Information No refresh Refresh every secs

System Information

System Up Time: 4:20

- CPU Utilization: 4.21

- Memory Usage:
Free: 76 %

- Disk Usage (1 Kbyte blocks)

Partition	Total Space	Used	Available	Use %
root	26873436	371996	26136320	2%
tmp	131072	488	130584	1%
home	2016016	32888	1880716	2%
cdr	2016044	32820	1880812	2%
logs	1510032	33044	1400280	3%
reports	1510032	32812	1400512	3%
trace	1510032	35508	1397816	3%

- System Temperature
System Temperature: 47 C
CPU Temperature: 46 C

- Fan Speed
System Fan: 3175 RPM

- EISA0 Interface:
Auto-negotiation: enabled
Auto-negotiation capability includes:
any speed and any duplex
Interface State: up, 1000Mbps full duplex

- EISA1 Interface:
Auto-negotiation: enabled
Auto-negotiation capability includes:
any speed and any duplex
Interface State: down

Data as of Jul 05, 2011 02:11:57 pm

To View Manufacturing Information:

- From the top menu, click **Reports**. The **Reports & Displays** screen is displayed.

- Click the **Manufacturing Information** display option. The **Manufacturing Information** display opens in a new browser window.

Lab-126-10 - Reports - Manufacturing Information

```
Manufacturing Information Version 1.0
Card Type: SME 2151
Part Number: S30810-Q2311-X100-03
Serial Number: K758064540004
Firmware Version: RT8
Software Version: 07.41.01.0119
Model: C2400 Enterprise
ADMIN MAC address: 08:00:06:85:91:ac
Card Type: NPE 2411
Part Number: S30810-Q2325-X200-3
Serial Number: SK758060830008
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: 08:00:06:81:c2:7d
MAC address 1: 08:00:06:81:c2:7e
MAC address 2: 08:00:06:81:c2:7f
MAC address 3: 08:00:06:81:c2:80
Card Type: MSE 2011
Part Number: Not Programmed
Serial Number: Not Programmed
Model Number: STI Flash 8.0.0
```

Viewing Displays for the Mobility Manager

When a Enterasys Wireless Controller has been configured as a mobility manager, two additional displays appear as options on the **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.

enterasys
Secure Networks™ There's nothing more important than our customers.

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

Mesh Statistics

Active Wireless Load Groups

Admission Control Statistics by Wireless AP

Remotable VNS Information

External Connections Statistics

System Information

Manufacturing Information

To View Mobility Manager Displays:

1. From the top menu, click **Reports**. The **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 Enterasys 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.

Viewing Reports

The following reports are available in the Enterasys Wireless 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)

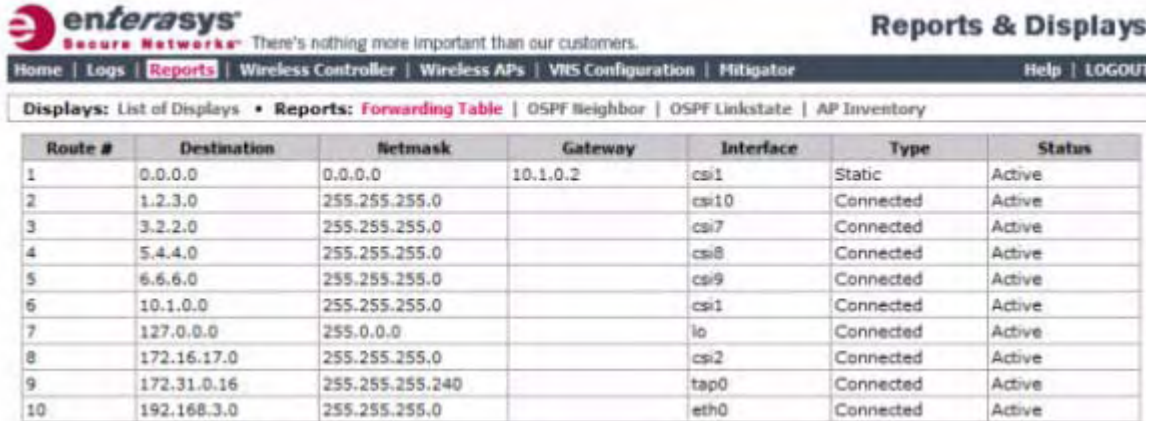
To View Reports:

1. From the top menu, click **Reports**. The **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:



The screenshot shows the Enterasys Reports & Displays interface. The top navigation bar includes Home, Logs, Reports, Wireless Controller, Wireless APs, VMS Configuration, Mitigator, Help, and LOGOUT. The main content area displays the Forwarding Table report with the following data:

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.1.0.2	csi1	Static	Active
2	1.2.3.0	255.255.255.0		csi10	Connected	Active
3	3.2.2.0	255.255.255.0		csi7	Connected	Active
4	5.4.4.0	255.255.255.0		csi8	Connected	Active
5	6.6.6.0	255.255.255.0		csi9	Connected	Active
6	10.1.0.0	255.255.255.0		csi1	Connected	Active
7	127.0.0.0	255.0.0.0		lo	Connected	Active
8	172.16.17.0	255.255.255.0		csi2	Connected	Active
9	172.31.0.16	255.255.255.240		tap0	Connected	Active
10	192.168.3.0	255.255.255.0		eth0	Connected	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-126-10 - Reports - Wireless AP Inventory

Wireless AP (Serial)	Port				HW				SW		Country	Antennas			
	Rdo	Ra	Rb	Rg	Rn	DP	BP	RT	FT	Req Ch	Ch / Tx	Aj	TxMn	TxMx	Dom
11n Channel Width				11n Guard Interval				11n Channel Bonding							
Failure Maintn.				Assn		IP Address				Netmask					
0002010712513643 (0002010712513643) Role: Access Point	esa-1				A&D Scalance W786-2HPW-External-2				07.41.01.0119		United States	left-1: No Antenna middle-1: N/A right-1: No Antenna left-2: No Antenna middle-2: N/A right-2: No Antenna			
1	on	-	-	off	5	100	2346	2346	auto	-	-	0 dB	18 dB	MyDomain	6 Mbp
2	-	on	off	off	5	100	2346	2346	auto	-	-	8 dB	18 dB	MyDomain	1 Mbp
enabled				DHCP		10.107.1.66				255.255.255.0					
050000523000824 (050000523000824) Role: Access Point	esa0				Wireless AP2610 Internal				07.41.01.0119		United States	-			
1	on	-	-	off	5	100	2346	2346	auto	-	-	0 dB	18 dB	MyDomain	6 Mbp
2	-	on	on	off	5	100	2346	2346	auto	11: 2462 MHz/16 dBm	-	8 dB	18 dB	MyDomain	1 Mbp

Table 15-1 lists the column names and abbreviations found in the **AP Inventory** report:

Table 15-1 AP Inventory Report Columns

Column Name	Description
Port	Ethernet port and associated IP address of the interface on the Enterasys Wireless Controller through which the Wireless AP communicates.
HW	Hardware version of the Wireless AP.
SW	Software version executing on the Wireless AP.
Country	Country in which the AP is deployed

Table 15-1 AP Inventory Report Columns (continued)

Column Name	Description
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.
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

Table 15-1 AP Inventory Report Columns (continued)

Column Name	Description
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 Enterasys 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.
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 Enterasys Wireless Controller is lost.

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.

Call Detail Records (CDRs)

You can configure the Enterasys 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 Enterasys Wireless Controller to generate CDRs, refer to [“Defining Accounting Methods for a WLAN Service”](#) on page 6-15.

CDRs are located in a CDR directory on the Enterasys 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 Enterasys Wireless Assistant (GUI) or CLI.

CDR File Naming Convention

CDRs are written to a file on the Enterasys 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**

CDR File Types

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

- **.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 Enterasys 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 Enterasys Wireless Controller to a remote server.



Note: The CDR directory on the Enterasys 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.

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.

Table 15-2 CDR Records and Their Description

CDR Records	Description
Acct-Session-ID	A unique CDR ID
User-Name	The name of the user, who was authenticated.

Table 15-2 CDR Records and Their Description (continued)

CDR Records	Description
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: <ul style="list-style-type: none"> • 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.
Enterasys-AP-Serial	The Wireless AP's serial number.
Enterasys-AP-Name	The Wireless AP's name.
Enterasys-VNS-Name	The VNS name on which the session took place.
Enterasys-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.

Table 15-2 CDR Records and Their Description (continued)

CDR Records	Description
Acct-Terminate-Cause	Indicates how the session was terminated. The field displays one of the following values: <ul style="list-style-type: none"> • 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 .

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 Enterasys Wireless Controller.
2. Copy the CDR files from the Enterasys 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 Enterasys Wireless Assistant (GUI) or CLI.

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

Backing Up and Copying CDR Files to a Remote Server

To Back Up and Copy the CDR Files to a Remote Server:

1. From the top menu, click **Wireless Controller**. The **Wireless Controller Configuration** screen is displayed.
2. In the left pane, click **Software Maintenance**. The **Software Maintenance** screen is displayed.

- Click the **Backup** tab.

The screenshot shows the 'Wireless Controller Configuration' interface. The 'Backup' tab is selected. The main content area is divided into sections: 'Available Backups' (empty), 'Upload Backup' (with fields for Protocol, Server, User ID, Password, Confirm, Directory, and Filename), 'Backup' (with a dropdown menu set to 'Config's, CDRs, Logs, Audit and Rogue' and a 'Backup Now' button), and 'Schedule Backups' (with status messages for next backup, schedule, upload location, and backup of, and a 'Schedule Backups...' button). A footer indicates 'Disk space left for Backup/Restore: 24546 MB'.

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

The screenshot shows a 'Software Maintenance' window. At the top, it says 'Please wait while performing backup of [cdrs] ...'. Below that, it displays the 'Result of backup:' as 'SUCCESS: Backup/Export complete: Lab126-10.05072011.142035'. A 'Close' button is located at the bottom center of the window.

- 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.

- 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**.

DRAFT

- **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.

Figure 15-1 Sample .dat File

```
-----  
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  
Calling-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
```

Performing System Administration

This chapter describes system administration processes, including:

For information about...	Refer to page...
Performing Wireless AP Client Management	16-1
Defining Enterasys Wireless Assistant Administrators and Login Groups	16-5

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 Enterasys Wireless Controller database. For more information, see the Enterasys Wireless Convergence Software *Maintenance Guide*.

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 15, Working with Reports and Displays](#).

To Disassociate a Wireless Device Client:

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

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

The screenshot shows the Enterasys Wireless APs management interface. The left sidebar contains a list of APs, with 'Client Management' highlighted. The main content area is divided into two tabs: 'Disassociate' (active) and 'Whitelist/Blacklist'. Under the 'Disassociate' tab, there are two sections: 'Select AP:' and 'Select Client(s) for 0500005230000824:'. The 'Select AP:' section shows a single entry: '0500005230000824 (0)'. The 'Select Client(s) for 0500005230000824:' section is empty and displays the message 'There are no active clients for this Wireless AP'. At the bottom of the interface, there is a search bar with 'MAC Addr.' and 'equals' dropdown menus, a 'Search' button, and 'Select All' and 'Deselect All' buttons. Below the search bar are three buttons: 'Add to Blacklist', 'Disassociate', and 'Show OUI'.

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

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

Blacklisting a Client

The **Whitelist/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:

- From the top menu, click **Wireless APs**. The **Wireless AP Configuration** screen is displayed.

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

The screenshot shows the Enterasys Wireless APs management interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VMS Configuration', 'Fidigator', 'Help', and 'LOGOUT'. The left-hand navigation pane lists various management options, with 'Client Management' highlighted in red. The main content area is titled 'Disassociate' and features two tabs: 'Disassociate' (active) and 'Whitelist/Blacklist'. Under the 'Disassociate' tab, there are two sections: 'Select AP:' showing '0500005230000824 (0)' and 'Select Client(s) for 0500005230000824:' showing 'There are no active clients for this Wireless AP'. At the bottom of the main area, there is a search bar with 'MAC Addr.' and 'equals' selected, and buttons for 'Search', 'Select All', 'Deselect All', 'Add to Blacklist', 'Disassociate', and 'Show OUI'.

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

- 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:

- From the top menu, click **Wireless APs**. The **Wireless AP Configuration** screen is displayed.
- In the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3. Click the **Whitelist/Blacklist** tab.

The screenshot shows the Enterasys Wireless APs configuration interface. The top navigation bar includes the Enterasys logo, the tagline "Secure Networks. There's nothing more important than our customers.", and the title "Wireless APs". The navigation menu includes Home, Logs, Reports, Wireless Controller, **Wireless APs**, VNS Configuration, Mitigator, Help, and LOGOUT. The left sidebar lists various management options, with "Client Management" highlighted in red. The main content area is titled "Whitelist/Blacklist" and features a "Disassociate" tab. The "MAC Addresses" section contains a large empty list box. To the right, there is a "MAC Address:" input field with an "Add" button. Below this are "Select All" and "Deselect All" buttons, followed by a "Remove Selected" button. Two radio buttons are present: "Allow MAC only if on the MAC address list" (unselected) and "Deny MAC address if it is on the list" (selected). At the bottom, there are "Save" and "Cancel" buttons, and a section for file operations with "Select file to import:", a "Browse..." button, and an "Import" button, along with "Export address list:" and an "Export" button.

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 top menu, click **Wireless APs**. The Wireless AP **Configuration** screen is displayed.
2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.
3. Click the **Whitelist/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 top menu, click **Wireless APs**. The Wireless AP **Configuration** screen is displayed.

2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.
3. Click the **Whitelist/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 top menu, click **Wireless APs**. The **Wireless AP Configuration** screen is displayed.
2. In the left pane, click **Client Management**. The **Disassociate** tab is displayed.
3. Click the **Whitelist/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.

Defining Enterasys Wireless Assistant Administrators and Login Groups

You can define the login user names and passwords for administrators that have access to the Enterasys 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 Enterasys Wireless Controller. Full administrators can manage all aspects of the Enterasys Wireless Controller, including GuestPortal user accounts.
- **Read-only administrators** — Users assigned to this login group have read-only access rights on the Enterasys 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 Enterasys Wireless Controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the Enterasys Wireless Assistant.



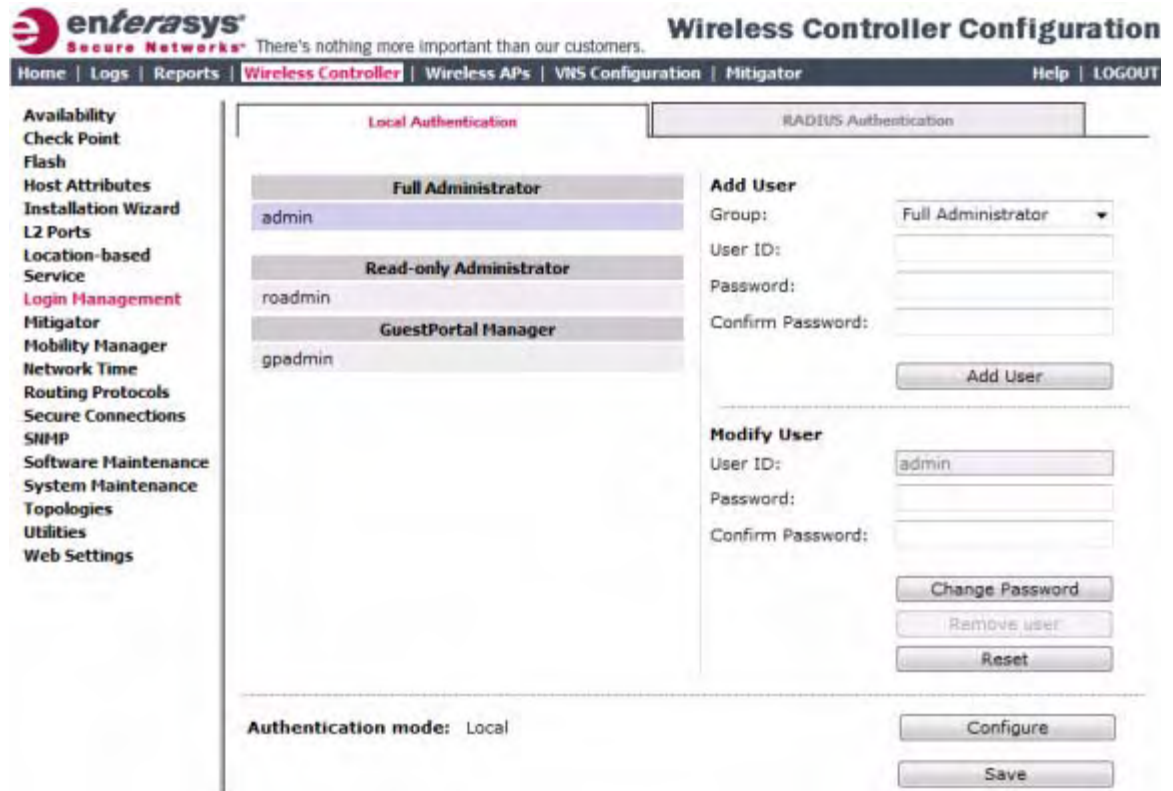
Note: When adding or modifying a user, note the following password character constraints:

- Allowed characters include A-Z a-z 0-9 ~!@#\$%^&*()_+|=\\{}];<>?.,.
- Characters not allowed include / ` ' " : and space is not valid.

To Add a Enterasys Wireless Controller Administrator to a Login Group:

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

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



- 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 Enterasys 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 Enterasys 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 Enterasys Wireless Controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the Enterasys Wireless Assistant. For more information, see [“Working with GuestPortal Administration”](#) on page 18-1.
- 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.
- In the **Password** box, type the password for the new user.
- In the **Confirm Password**, re-type the password.
- Click **Add User**. The new user is added to the appropriate login group list.

To Modify a Enterasys Wireless Controller Administrator’s Password:

- From the top menu, click **Wireless Controller**. The **Wireless Controller Configuration** screen is displayed.
- 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 Enterasys Wireless Controller Administrator:

1. From the top menu, click **Wireless Controller**. 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.

Logs, Traces, Audits and DHCP Messages

This chapter describes Enterasys Wireless Controller logs, traces, audits, and DHCP messages, including:

For information about...	Refer to page...
Enterasys Wireless Controller Messages	17-1
Working with Logs	17-1
Viewing Wireless AP Traces	17-8
Viewing Audit Messages	17-9
Viewing the DHCP Messages	17-10
Viewing Software Upgrade Messages	17-12
Viewing Configuration Restore/Import Messages	17-13

Enterasys Wireless Controller Messages

The Enterasys Wireless Controller generates four types of messages:

- **Logs (including alarms)** – Messages that are triggered by events
- **Traces** – Messages that display activity by component, for system debugging, troubleshooting, and internal monitoring of software



Caution: In order for the **Debug Info** option on the **Wireless AP Traces** screen to return trace messages, this option must be enabled while Wireless AP debug commands are running. To do so, you need to run a Wireless AP CLI command to turn on a specific Wireless AP debug. Once the CLI command is run, select the **Debug Info** option, and then click **Retrieve Traces**. For more information, see the Enterasys Wireless Controller *Convergence Software CLI Reference Guide*.

Because Wireless AP debugging can affect the normal operation of Wireless AP service, enabling debugging is not recommended unless specific instructions are provided.

- **Audits** – Messages that record administrative changes made to the system
- **DHCP** – Messages that record DHCP service events

Working with Logs

The log messages contain the time of event, severity, source component, and any details generated by the source component. Log messages are divided into three groups:

- Controller logs

- Wireless AP logs
- Login logs

Log Severity Levels

Log messages are classified at four levels of severity:

- Information (the activity of normal operation)
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with. The following are examples of events on the Enterasys Wireless Controller that generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the Enterasys Wireless Controller
- Software upgrade failure on the Wireless AP
- Detection of rogue access point activity without valid ID
- Availability configuration not identical on the primary and secondary Enterasys Wireless Controller

If SNMP is enabled on the Enterasys Wireless Controller, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions.



Note: The log statements **Low water mark level was reached** and **Incoming message dropped, because of the rate limiting mechanism** indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way.

Viewing the Enterasys Wireless Controller Logs

To View Enterasys Wireless Controller Logs:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.

- Click the **HWC: Events** tab. The Enterasys Wireless Controller log screen is displayed and the events are displayed in chronological order.

The screenshot shows the 'Logs & Traces' interface for the Enterasys Wireless Controller. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VMS Configuration', and 'Mitigator'. The 'Logs' tab is active, showing 'HWC: Events' and 'Severity: Critical'. A table of log messages is displayed with the following content:

Timestamp	Type	Component	Log Message
02/23/11 10:47:31	Critical	RU Manager	Cannot establish an Availability Link: Incompatible configuration. AC role Secondary is configured the same as availability peer.

At the bottom of the screen, there is a status bar indicating '1 critical log messages found' and 'Total pages: 1'. Navigation controls include a 'Go' button with a page number '1' and buttons for 'Tech Support', 'Export', and 'Refresh'.

- To sort the events by **Timestamp**, **Type**, or **Component**, click the appropriate column heading.
- To filter the events by severity, **Critical**, **Major**, **Minor**, **Info**, and **All**, click the appropriate log severity.
- To refresh the Enterasys Wireless Controller log screen, click **Refresh**.
- To export the Enterasys Wireless Controller log screen, click **Export**. The **File Download** dialog is displayed.
- Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.



Note: The component 'Langley' is the term for the inter-process messaging infrastructure on the Enterasys Wireless Controller.

Clearing Enterasys Wireless Controller Logs

To Clear Enterasys Wireless Controller Logs:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
- Click the **HWC: Events** tab. The Enterasys Wireless Controller log screen is displayed and the events are displayed in chronological order.
- To clear the logs, click **Clear Log Messages**.

- To confirm the deletion of the Enterasys Wireless Controller log messages, click **Ok**. The Enterasys Wireless Controller log messages are deleted.

Viewing Wireless AP Logs

To View Wireless AP Logs:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
- Click the **AP: Logs** tab. The Wireless AP log screen is displayed and the events are displayed in chronological order.

The screenshot shows the Enterasys Wireless Controller interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'WMS Configuration', and 'Mitigator'. The 'Logs & Traces' section is active, with 'AP: Logs' selected. Below the navigation, there are filters for severity: 'Critical', 'Major', 'Minor', 'Information', and 'All'. A 'Clear All Log Messages' button is also present. The main content area displays a table with the following columns: 'Wireless AP', 'HWC time', 'Sev', and 'AP-time/up-time : Log Messages'. The table contains one entry for the AP serial '0002010712513643' with the message: 'There are no critical log messages found for Wireless AP serial 0002010712513643.' At the bottom of the table, it indicates '0 AP critical log messages found'. There are 'Export' and 'Refresh' buttons at the bottom right of the table area.

- In the **Active Wireless AP** list, click a Wireless AP to view the log events for that particular Wireless AP.
- To sort the events by **Timestamp or Severity**, click the appropriate column heading.
- To filter the events by severity, **Critical, Major, Minor, Information**, and **All**, click the appropriate log severity.
- To refresh the Enterasys Wireless Controller log screen, click **Refresh**.
- To export the Enterasys Wireless Controller logs, click **Export**. The **File Download** dialog is displayed.
- Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing Login Logs

To View Administrator Login Logs:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
2. Click the **Login** tab. The Login screen is displayed and the login events are displayed in chronological order.

The screenshot shows the Enterasys 'Logs & Traces' interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VNS Configuration', 'Mitigator', 'Help', and 'LOGOUT'. Below this, there are tabs for 'HWC: Events', 'Restore/Import', 'S/W Upgrade', 'AP: Logs', 'Traces', 'Audit: UI', 'Services: DHCP', 'NTP', and 'Login'. The 'Administrator' tab is selected, and the 'GuestPortal' sub-tab is also visible. The main content area displays a table of login events with columns for 'Timestamp' and 'Auth Message'. The messages indicate session openings and closings for the user 'admin' by 'gui_s_mgr' from the IP 'Lab-126-10.chantrynetworks.com' using 'pam_unix' authentication. A 'Refresh' button is located at the bottom right of the table.

Timestamp	Auth Message
02/24/11 15:11:45	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/24/11 11:18:45	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/24/11 09:53:56	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/23/11 17:46:39	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/23/11 15:37:57	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/23/11 13:19:34	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/23/11 11:23:46	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/23/11 10:43:29	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/23/11 09:30:15	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/22/11 15:49:23	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/22/11 15:32:17	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/22/11 15:27:30	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/22/11 14:39:38	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/22/11 11:53:49	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/22/11 11:52:49	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/22/11 10:40:27	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/22/11 10:33:38	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/22/11 10:31:19	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin
02/22/11 10:27:41	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
02/18/11 18:11:21	Lab-126-10.chantrynetworks.com gui_s_mgr: (pam_unix) session closed for user admin

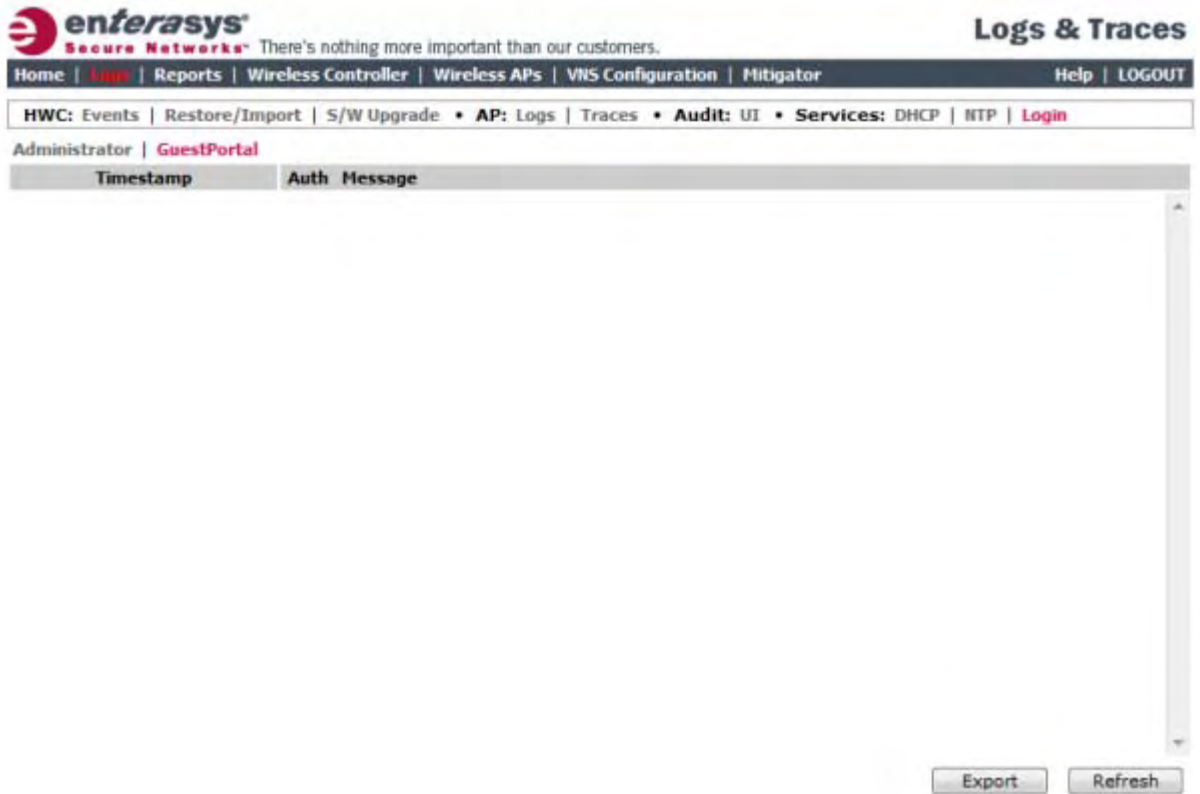
3. To refresh the **Login** screen, click **Refresh**.

Working with GuestPortal Login Logs

To View GuestPortal Login Logs:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
2. Click the **Login** tab. The Login screen is displayed and the login events are displayed in chronological order.

3. Click **GuestPortal**. The GuestPortal login events are displayed in chronological order.



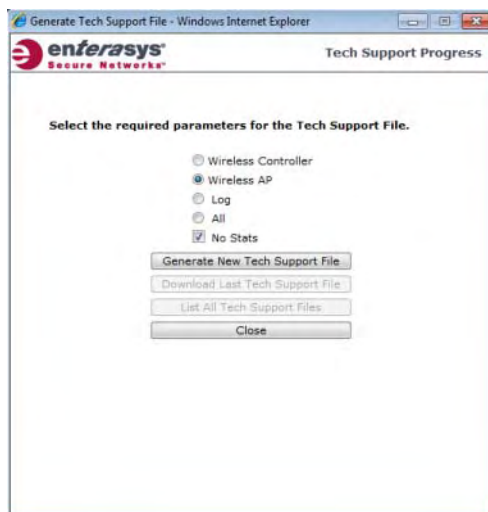
4. To export the GuestPortal log information, click **Export**. The **File Download** dialog is displayed.
5. Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Working with a Tech Support File

To Generate a Tech Support File:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
2. Ensure that the **HWC:Events** tab is selected.

- Click the **Tech Support** button at the bottom of the page. The **Generate Tech Support File** screen is displayed.



- Select the parameters for the tech support file:
 - Wireless Controller
 - Wireless AP
 - Logs
 - All
 - **No Stats** – If Wireless AP is selected, select this checkbox to include or exclude Wireless AP statistics in the tech support file.
- Click **Generate New Tech Support File**. A warning message is displayed informing you that this operation may temporarily affect system performance.
- Click **OK** to continue. The tech support file generation status is displayed.
- When the file generation has completed, click **Close**.

To Download the Last Generated Tech Support File:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
- Ensure that the **HWC:Events** tab is selected.
- Click the **Tech Support** button at the bottom of the page. The **Generate Tech Support File** screen is displayed.
- Click **Download Last Tech Support File**. The **File Download** dialog is displayed.
- Click **Save**. The **Save as** window is displayed.
- Navigate to the location you want to save the generated tech support file, and then click **Save**.

To Delete a Tech Support File:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
- Ensure that the **HWC:Events** tab is selected.
- Click the **Tech Support** button at the bottom of the page. The **Generate Tech Support File** screen is displayed.

4. Click **List All Tech Support Files**.
5. In the drop-down list, click the tech support file you want to delete. The tech support file is deleted.
6. Click **Close**.

Viewing Wireless AP Traces

To View Wireless AP Traces:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
2. Click the **AP: Traces** tab. The Wireless AP trace screen is displayed.

The screenshot shows the Enterasys 'Logs & Traces' interface. At the top, there is a navigation bar with 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'WMS Configuration', and 'Mitigator'. Below this is a breadcrumb trail: 'HWC: Events | Restore/Import | S/W Upgrade | AP: Logs | Traces | Audit: UI | Services: DHCP | NTP | Login'. The main content area is divided into two tabs: 'Wireless AP' and 'Tracing'. Under the 'Tracing' tab, there are three radio button options: 'Configurations' (selected), 'Debug Info', and 'Reports'. There are 'Start Tracing' and 'Retrieve Traces' buttons. Below these is a 'Trace Log Output' section with a scrollable area containing instructions: 'Click Start/Stop Tracing for collection of traces for this AP. Click Retrieve Traces to view available traces in this area.' At the bottom right, there are 'Export' and 'Refresh' buttons.



Caution: In order for the **Debug Info** option on the **Wireless AP Traces** screen to return trace messages, this option must be enabled while Wireless AP debug commands are running. To do so, you need to run a Wireless AP CLI command to turn on a specific Wireless AP debug. Once the CLI command is run, select the **Debug Info** option, and then click **Retrieve Traces**. For more information, see the Enterasys Wireless Controller *Convergence Software CLI Reference Guide*.

Because Wireless AP debugging can affect the normal operation of Wireless AP service, enabling debugging is not recommended unless specific instructions are provided.

3. In the **Active Wireless AP** list, click the Wireless AP whose trace messages you want to view.
4. In the **Collect traces for** section, do the following:
 - a. **Configurations** – Select to collect trace configuration information.
 - **Start/Stop Tracing** – Click to start or stop the collection of traces.

- **Retrieve Traces** – Click to view the available configuration traces in the **Trace Log Output** section.
 - b. **Debug info** – Select to collect trace debug information.
 - **Start/Stop Tracing** – Click to start or stop the collection of traces.
 - **Retrieve Traces** – Click to view the available debug traces in the **Trace Log Output** section.
 - c. **Reports** – Select to view available crash files.
 - **Retrieve Traces** – Click to view available crash files in the **Trace Log Output** section.
 - **Delete all crash reports** – Click to delete all crash reports.
5. To refresh the Enterasys Wireless Controller trace screen, click **Refresh**.
 6. To export and view the Wireless AP trace screen in HTML format, click **Export**.

Viewing the Wireless 802.11n AP Traces

Wireless 802.11n AP traces are combined into a single .tar.gz file and can only be viewed by saving the .tar.gz file to a directory on your computer.

To View Wireless 802.11n AP Traces:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
2. Click the **AP Traces** tab. The Wireless AP trace screen is displayed.
3. In the **Active Wireless AP** list, click the Wireless 802.11n AP whose trace messages you want to view.
4. Click **Retrieve Traces**. The **File Download** dialog appears.
5. Click **Save** and navigate to the location on your computer that you want to save the Wireless 802.11n AP trace report. The file is saved as a .tar.gz file.
6. To view the file, unzip the .tar.gz file.

Viewing Audit Messages

To View Audit Messages:

1. From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.

- Click the **Audit: UI** tab. The audit screen is displayed and the events are displayed in chronological order.

enterasys
Secure Networks™ There's nothing more important than our customers.

Logs & Traces

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

HWC: Events | Restore/Import | S/W Upgrade • AP: Logs | Traces • **Audit: UI** • Services: DHCP | NTP | Login

Timestamp	User	Section	Page	Audit Message
02/24/11 15:56:08	admin	Sys Mgmt	Flash	FAIL: Flash memory not present. Could not mount
02/22/11 10:31:14	admin	n/a	n/a	Possible session hijack detected from client IP 134.141.94.156. Original session is from 134.141.97.42
02/16/11 14:19:00	admin	Sys Mgmt	Wizard	Mobility Port changed from [undefined] to []
02/16/11 14:19:00	admin	Sys Mgmt	Wizard	Mobility Role changed from [Agent] to [Agent]
02/16/11 14:19:00	admin	Sys Mgmt	Wizard	Mobility has been disabled.
02/08/11 14:41:12	admin	VNS Cfg	Common	Set radius servers for WLAN Service 'Lab126-10-Int-CP'
02/08/11 14:41:12	admin	VNS Cfg	Common	Set Captive Portal type for WLAN Service 'Lab126-10-Int-CP' to Internal Captive Portal
02/07/11 15:30:41	admin	ap	load-group	Created client load group [test]
02/07/11 11:50:48	admin	vns	wlan	WLANS [tst_wlan] created with mode mesh SSID <1112>
02/01/11 10:41:11	admin	Sys Mgmt	SW Maint.	Maintenance task: HMC upgrade to image ftp
02/01/11 10:41:10	admin	CLI_syste m_managem ent	backup	SUCCESS to complete backup/export: backup/export file: sysupgrade_bak.zip.
02/01/11 10:40:49	admin	Sys Mgmt	Schedule	Upgrade Now has been selected.
01/31/11 14:19:15	admin	Sys Mgmt	OSPF	Link cost changed from [11] to [10] for esai
01/31/11 14:19:08	admin	Sys Mgmt	OSPF	Link cost changed from [10] to [11] for esai
01/31/11 11:51:46	admin	Sys Mgmt	MG	Mitigator Analysis Engine disabled
01/31/11 11:07:05	admin	Sys Mgmt	MG	Mitigator Analysis Engine enabled
01/31/11 11:03:43	admin	Sys Mgmt	MG	Mitigator Analysis Engine disabled
01/31/11 11:02:51	admin	Sys Mgmt	MG	Mitigator Analysis Engine enabled
01/07/11 17:13:39	admin	Sys Mgmt	SW Maint.	Maintenance task: HMC upgrade to image ftp
01/07/11 17:13:38	admin	CLI_syste m_managem ent	backup	SUCCESS to complete backup/export: backup/export file: sysupgrade_bak.zip.
01/07/11 17:13:18	admin	Sys Mgmt	Schedule	Upgrade Now has been selected.

640 audit messages found
Total pages: 1

Export Refresh

- To sort the events by **Timestamp**, **User**, **Section**, or **Page**, click the appropriate column heading.
- To refresh the audit screen, click **Refresh**.
- To export the audit screen, click **Export**. The **File Download** dialog is displayed.
- Do one of the following:
 - To open the audit file, click **Open**.
 - To save the audit file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing the DHCP Messages

To View DHCP Messages:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.

- Click the **Service: DHCP** tab. The DHCP message screen is displayed and the events are displayed in chronological order.

The screenshot displays the Enterasys 'Logs & Traces' interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Wireless Controller', 'Wireless APs', 'VMS Configuration', and 'Mitigator'. Below this, a breadcrumb trail shows 'HWC: Events | Restore/Import | S/W Upgrade • AP: Logs | Traces • Audit: UI • Services: DHCP | NTP | Login'. The main content area is a table with two columns: 'Timestamp' and 'DHCP Message'. The table contains a list of DHCP-related events, such as 'Wrote 1 leases to leases file.', 'DHCPOFFER on 172.16.161.253 to 00:21:2f:2e:fb:0b (enterasy-hao) via esa5', 'DHCPCREQUEST for 172.16.161.254 (172.16.161.1) from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5', and 'DHCPCPACK on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5'. A 'Refresh' button is located at the bottom right of the message list.

Timestamp	DHCP Message
02/19/11 16:30:34	dhcpcd: Wrote 1 leases to leases file.
02/19/11 16:29:39	dhcpcd: Wrote 1 leases to leases file.
02/14/11 12:47:11	dhcpcd: DHCPOFFER on 172.16.161.253 to 00:21:2f:2e:fb:0b (enterasy-hao) via esa5
02/14/11 12:47:10	dhcpcd: DHCPCDISCOVER from 00:21:2f:2e:fb:0b via esa5
02/05/11 00:35:52	dhcpcd: Wrote 1 leases to leases file.
02/04/11 14:35:52	dhcpcd: DHCPOFFER on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 14:35:52	dhcpcd: Wrote 1 leases to leases file.
02/04/11 14:35:52	dhcpcd: DHCPCREQUEST for 172.16.161.254 (172.16.161.1) from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 14:35:52	dhcpcd: DHCPCPACK on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 14:35:51	dhcpcd: DHCPCDISCOVER from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 14:35:16	dhcpcd: DHCPCREQUEST for 134.141.120.153 from 00:0f:b5:28:42:5a via esa5: unknown lease 13
02/04/11 12:48:05	dhcpcd: DHCPCREQUEST for 172.16.161.254 from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 12:48:05	dhcpcd: DHCPCPACK on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 12:33:25	dhcpcd: DHCPOFFER on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 12:33:25	dhcpcd: Wrote 1 leases to leases file.
02/04/11 12:33:25	dhcpcd: DHCPCREQUEST for 172.16.161.254 (172.16.161.1) from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 12:33:25	dhcpcd: DHCPCPACK on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/04/11 12:33:24	dhcpcd: DHCPCDISCOVER from 00:0f:b5:28:42:5a via esa5
02/04/11 12:32:45	dhcpcd: DHCPCREQUEST for 134.141.120.153 from 00:0f:b5:28:42:5a via esa5: unknown lease 13
02/04/11 09:19:37	dhcpcd: Wrote 1 leases to leases file.
02/03/11 23:19:37	dhcpcd: DHCPOFFER on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/03/11 23:19:37	dhcpcd: Wrote 1 leases to leases file.
02/03/11 23:19:37	dhcpcd: DHCPCREQUEST for 172.16.161.254 (172.16.161.1) from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/03/11 23:19:37	dhcpcd: DHCPCPACK on 172.16.161.254 to 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/03/11 23:19:36	dhcpcd: DHCPCDISCOVER from 00:0f:b5:28:42:5a (EngineeringLab2) via esa5
02/03/11 23:19:35	dhcpcd: DHCPCREQUEST for 172.16.161.254 from 00:0f:b5:28:42:5a via esa5: unknown network

- To sort the events by **timestamp**, click **Timestamp**.
- To refresh the DHCP message screen, click **Refresh**.

Viewing the NTP Messages

To View NTP Messages:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.

- Click the **Service: NTP** tab. The NTP message screen is displayed and the events are displayed in chronological order.

The screenshot shows the Enterasys 'Logs & Traces' interface. The breadcrumb navigation includes: Home | Logs | Reports | Wireless Controller | Wireless APs | VMS Configuration | Mitigator | Help | LOGOUT. The active menu is 'HWC: Events | Restore/Import | S/W Upgrade • AP: Logs | Traces • Audit: UI • Services: DHCP | NTP | Login'. The main content area displays a table of NTP messages with two columns: 'Timestamp' and 'NTP Message'. The messages are sorted by timestamp and show the NTP daemon's startup sequence, including kernel sync status, precision settings, and listening status for various interfaces (csi0 through csi25). A 'Refresh' button is located at the bottom right of the message list.

Timestamp	NTP Message
09/07/11 03:32:26	ntpd[7057]: synchronized to LOCAL(0), stratum 10
09/07/11 03:32:26	ntpd[7057]: kernel time sync status change 0001
09/07/11 03:29:11	ntpd[7056]: ntpd 4.2.4p4@1.1520-o Mon Aug 9 22:10:49 UTC 2010 (1)
09/07/11 03:29:11	ntpd[7057]: precision = 1.000 usec
09/07/11 03:29:11	ntpd[7057]: ntp_io: estimated max descriptors: 1024, initial socket boundary: 16
09/07/11 03:29:11	ntpd[7057]: Listening on interface #0 wildcard, 0.0.0.0#123 Disabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #1 lo, 127.0.0.1#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #2 eth0, 192.168.3.10#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #3 csi1, 10.1.0.1#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #4 csi2, 172.16.17.1#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #5 csi7, 3.2.2.1#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #6 csi8, 5.4.4.8#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #7 csi9, 6.6.6.6#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #8 csi10, 1.2.3.4#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #9 csi11, 5.5.5.5#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #10 csi13, 3.3.3.8#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #11 csi14, 6.6.6.6#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #12 csi15, 7.8.8.8#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #13 csi16, 78.8.8.8#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #14 csi17, 8.2.2.5#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #18 csi18, 7.5.6.5#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #16 csi19, 6.3.3.3#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #17 csi20, 5.8.8.8#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #18 csi21, 9.7.6.8#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #19 csi23, 10.2.2.2#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #20 csi24, 28.2.2.2#123 Enabled
09/07/11 03:29:11	ntpd[7057]: Listening on interface #21 csi25, 32.2.2.2#123 Enabled

- To sort the events by **timestamp**, click **Timestamp**.
- To refresh the NTP message screen, click **Refresh**.

Viewing Software Upgrade Messages

The **S/W Upgrade** tab displays the most recent upgrade actions, either success or failure, and the operating system patch history. Some examples of the upgrade actions that can be displayed are:

- FTP failure during backup of system image
- Configuration reset failure
- Configuration export failure
- Configuration import details

To View Software Upgrade Messages:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.

- Click the **S/W Upgrade** tab. The software upgrade message screen is displayed.

enterasys
Secure Networks™ There's nothing more important than our customers.

Home | **Logs** | Reports | Wireless Controller | Wireless APs | VMS Configuration | Mitigator Help | LOGOUT

HWC: Events | Restore/Import | **S/W Upgrade** • AP: Logs | Traces • Audit: UI • Services: DHCP | NTP | Login

History | Detail

Date	Type	Version
Tue Feb 1 10:43:33 EST 2011	Upgraded	07.41.01.0119
Fri Jan 7 17:15:37 EST 2011	Upgraded	07.41.01.0096
Tue Jan 4 12:36:58 EST 2011	Upgraded	07.41.01.0090T
Tue Dec 7 10:30:15 EST 2010	Upgraded	07.41.01.0062T
Tue Nov 30 14:27:43 EST 2010	Upgraded	07.41.01.0052T
Tue Nov 23 09:40:24 EST 2010	Upgraded	07.41.01.0046T
Fri Nov 19 15:50:38 EST 2010	Downgraded	07.41.01.0042T
Fri Nov 19 14:09:06 EST 2010	Upgraded	07.41.01.0043F
Thu Nov 18 16:52:58 EST 2010	Upgraded	07.41.01.0042F
Tue Nov 2 17:15:43 EDT 2010	Upgraded	07.41.01.0025T
Wed Oct 20 13:12:43 EDT 2010	Upgraded	07.41.01.0011T
Tue Oct 19 17:50:45 EDT 2010	Upgraded	07.41.01.0010T
Fri Sep 17 14:31:17 EDT 2010	Upgraded	07.31.01.0127
Mon Sep 13 16:51:33 EDT 2010	Upgraded	07.31.01.0120
Fri Sep 10 10:15:55 EDT 2010	Upgraded	07.31.01.0118T
Wed Sep 8 15:07:06 EDT 2010	Upgraded	07.31.01.0115
Thu Aug 19 15:12:31 EDT 2010	Upgraded	07.31.01.0103
Thu Jul 29 11:27:38 EDT 2010	Upgraded	07.31.01.0085
Tue Jul 20 17:37:12 EDT 2010	Upgraded	07.31.01.0074T
Fri Jul 9 14:14:55 EDT 2010	Upgraded	07.31.01.0065T
Mon Jun 7 14:23:43 EDT 2010	Upgraded	07.21.01.0116
Wed May 26 16:50:40 EDT 2010	Upgraded	07.21.01.0105T
Thu May 20 14:33:10 EDT 2010	Installed	07.21.01.0098
Thu May 20 18:20:19 EDT 2010	Upgraded	V6R1.10507.0
Mon Jul 27 18:28:07 EDT 2009	Installed	V6R1.10029.0
Mon Jul 27 18:27:27 EDT 2009	Installed	05-6_1_8-1

26 records found

Export Refresh

- Do the following:
 - To view software upgrade messages, click **Detail**.
 - To view the operating system history, click **History**.
- To refresh the screen, click **Refresh**.
- To export the software upgrade messages or operating system history, click **Export**. The **File Download** dialog is displayed.
- Do one of the following:
 - To open the file, click **Open**.
 - To save the file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing Configuration Restore/Import Messages

The **Restore/Import** tab displays the most recent configuration restore/import results.

To View Restore/import Messages:

- From the top menu, click **Logs**. The **Logs & Traces** screen is displayed.
- Click the **Restore/Import** tab. The restore/import message screen is displayed.
- To refresh the restore/import message screen, click **Refresh**.
- To export the restore/import message screen, click **Export**. The **File Download** dialog is displayed.

5. Do one of the following:
 - To open the file, click **Open**.
 - To save the file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Working with GuestPortal Administration

This chapter describes GuestPortal administration, including:

For information about...	Refer to page...
About GuestPortals	18-1
Adding New Guest Accounts	18-2
Enabling or Disabling Guest Accounts	18-4
Editing Guest Accounts	18-5
Removing Guest Accounts	18-6
Importing and Exporting a Guest File	18-7
Viewing and Printing a GuestPortal Account Ticket	18-9
Working with the GuestPortal Ticket Page	18-11
Configuring Web Session Timeouts	18-12

About GuestPortals

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 [“Creating a GuestPortal VNS”](#) on page 7-39.

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 Enterasys Wireless Assistant. For more information, see [“Defining Enterasys Wireless Assistant Administrators and Login Groups”](#) on page 16-5.

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

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 Enterasys Wireless Controller.
 - If you have full administrator rights:
 - (1) From the top menu, click **VNS 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.
 - (4) Make sure the Mode is set to GuestPortal and then click **Configure**. The Configuration page displays.
 - (5) 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
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

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

3. To enable the new guest account, select the **Enabled** checkbox. For more information, see [“Enabling or Disabling Guest Accounts”](#) on page 18-4.
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 specifies no limit to the account lifetime. Only a user with administrative privileges can change the value of 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 specifies no limit to the 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**.

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 Enterasys Wireless Controller.
 - If you have full administrator rights:
 - (1) From the top menu, click **VNS 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 **Manage Guest Users**.

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

The screenshot shows the Enterasys Virtual Network Configuration interface. At the top, there is a navigation bar with the Enterasys logo and the text "Secure Networks. There's nothing more important than our customers." The navigation bar includes links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. There are also links for Help and LOGOUT. Below the navigation bar, there is a search box with a "Search" button and a "Print Ticket for Selected Account" button. The main content area features a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data:

User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/> mark	Guest-mark	0	30	2010-08-10 15:40:00		<input checked="" type="checkbox"/>
<input type="checkbox"/> mark	mark	1	30	2010-08-04 13:51:00		<input checked="" type="checkbox"/>

Below the table, there are three main sections of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts.
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts.
- File Management:** Import Guest File, Export Guest File.

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.

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 Enterasys Wireless Controller.
 - If you have full administrator rights:
 - (1) From the top menu, click **VNS 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 **Manage Guest Users**.

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

The screenshot shows the Enterasys Virtual Network Configuration interface. At the top, there is a navigation bar with links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. Below the navigation bar is a search box for User Name and a button labeled Search. To the right of the search box is a button labeled Print Ticket for Selected Account. Below the search box is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data. Below the table are three groups of buttons: Account Management (Add Guest Account, Edit Selected Accounts, Remove Selected Accounts), Account Enable/Disable (Enable Selected Accounts, Disable Selected Accounts), and File Management (Import Guest File, Export Guest File).

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

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 [“Adding New Guest Accounts”](#) on page 18-2.
5. To save your changes, click **OK**. A confirmation message is displayed in the **GuestPortal Guest Administration** screen footer.

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 Enterasys Wireless Controller.
 - If you have full administrator rights:
 - (1) From the top menu, click **VNS 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 **Manage Guest Users**.

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

The screenshot shows the Enterasys Virtual Network Configuration interface. At the top, there is a navigation bar with links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), and Mitigator. Below the navigation bar is a search box labeled "Search" with a "User Name:" input field and a "Search" button. To the right of the search box is a "Print Ticket for Selected Account" button. Below the search box is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data:

User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/> mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/> mark	mark	1	30	2010-08-04 13:51:00		✓

Below the table are three groups of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts
- File Management:** Import Guest File, Export Guest File

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.

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 Enterasys Wireless Controller.

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

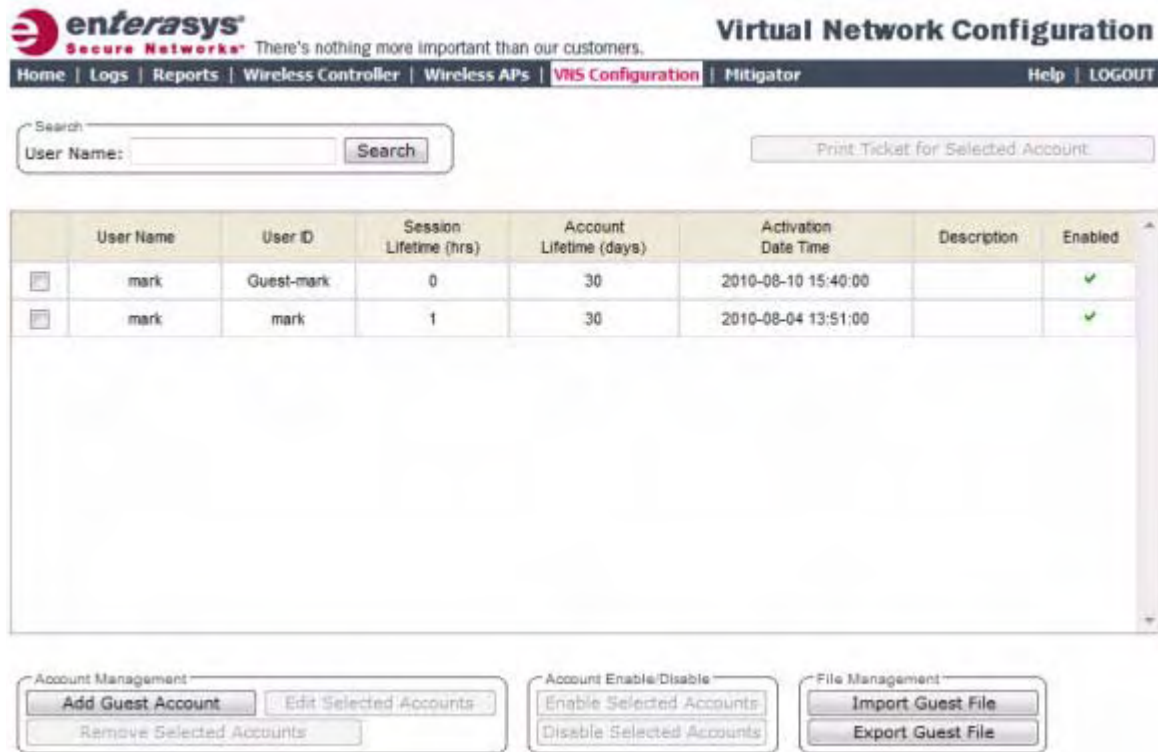
Table 18-1 Guest Account Import and Export .csv File Values

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 Enterasys Wireless Controller in an availability pair, yes (1) no (0)

To Export a Guest File

1. Do one of the following:
 - If you have GuestPortal Manager rights, log onto the Enterasys Wireless Controller.
 - If you have full administrator rights:
 - (1) From the top menu, click **VNS 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 **Manage Guest Users**.

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



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 Enterasys Wireless Controller.
 - If you have full administrator rights:
 - (1) From the top menu, click **VNS 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 **Manage Guest Users**.

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

The screenshot shows the Enterasys Virtual Network Configuration interface. At the top, there is a navigation bar with links for Home, Logs, Reports, Wireless Controller, Wireless APs, **VMS Configuration**, Mitigator, Help, and LOGOUT. Below the navigation bar is a search box labeled "Search" with a "User Name:" field and a "Search" button. To the right of the search box is a button labeled "Print Ticket for Selected Account".

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

Below the table are three groups of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts
- File Management:** Import Guest File, Export Guest File

- In the **File Management** section, click **Import Guest File**. The **Import Guest File** dialog is displayed.
- Click **Browse** to navigate to the location of the .csv guest file that you want to import, and then click **Open**.
- Click **Import**. The file is imported and a confirmation message is displayed in the **Import Guest File** dialog.
- Click **Close**.

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 Enterasys 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 Enterasys Wireless Controller. To upload a custom GuestPortal ticket template you need full administrator access rights on the Enterasys Wireless Controller. The filename of a custom GuestPortal ticket template must be .html. For more information, see [“Working with the GuestPortal Ticket Page”](#) on page 18-11.

To View Print a GuestPortal Account Ticket:

- Do one of the following:
 - If you have GuestPortal Manager rights, log onto the Enterasys Wireless Controller.

- If you have full administrator rights:
 - (1) From the top menu, click **VNS 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 **Manage Guest Users**.

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

The screenshot shows the Enterasys Virtual Network Configuration interface. At the top, there is a navigation bar with the Enterasys logo and the text "Secure Networks" and "There's nothing more important than our customers." The navigation bar includes links for Home, Logs, Reports, Wireless Controller, Wireless APs, VNS Configuration (highlighted), Mitigator, Help, and LOGOUT. Below the navigation bar is a search box with the label "Search" and a "Search" button. To the right of the search box is a button labeled "Print Ticket for Selected Account".

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

Below the table are three groups of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts
- File Management:** Import Guest File, Export Guest File

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.

PRINT

GuestPortal

Guest Name: test0001
User ID: test0001
Password: abc01234
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 C, Default GuestPortal Source Code](#).

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 Enterasys 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 Enterasys 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 C, Default GuestPortal Source Code](#).

Activating a GuestPortal Ticket Page

To Activate a GuestPortal Ticket Page:

1. From the top menu, click **VNS 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 Enterasys Wireless Controller.

Uploading a Custom GuestPortal Ticket Page

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 Enterasys 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 Enterasys Wireless Controller.

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

Deleting a Custom GuestPortal Ticket Page

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**.

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 top menu, click **Wireless Controller**. The **Wireless Controller Configuration** screen is displayed.

- In the left pane, click **Web Settings**. The **Wireless Controller Web Management Settings** screen is displayed.

- 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.
- 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.
- 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.
- 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.



Glossary

For information about...	Refer to page...
Networking Terms and Abbreviations	A-1
Wireless Controller Terms and Abbreviations	A-15

Networking Terms and Abbreviations

Table A-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	<p>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.</p> <p>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.</p>
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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. <i>See also</i> IBSS.
Captive Portal	A browser-based authentication mechanism that forces unauthenticated users to a Web page. Sometimes called a 'reverse firewall'.
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
DHCP	<p>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.</p> <p>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.)</p> <p>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)</p>
Directory Agent (DA)	<p>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.</p> <p>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.</p> <p>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.</p> <p>(SLP version 2, RFC2608, updating RFC2165)</p>
Diversity antenna and receiver	<p>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.</p>
DNS	Domain Name Server
DSSS	<p>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)</p>
DTIM	DTIM delivery traffic indication message (in 802.11 standard)
Dynamic WEP	<p>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.</p>

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
EAP-TLS EAP-TTLS	<p>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.</p> <p>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.</p> <p>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.</p> <p>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)</p>
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	<p>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.</p> <p>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.</p> <p>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.</p>
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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.
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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.
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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).
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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.
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: <ul style="list-style-type: none">• 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".

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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.
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

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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.
SLP	<p>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.</p> <p>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.</p> <p>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.</p> <p>(SLP version 2, RFC2608, updating RFC2165)</p>
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)	<p>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:</p> <ul style="list-style-type: none">• 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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
SSID	<p>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.</p> <p>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.</p> <p>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.</p>
SSL	<p>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.</p> <p>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.</p>
Subnet mask	(See netmask)
Subnets	<p>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.</p>
SVP	<p>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.</p>
Switch	<p>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.</p>
syslog	<p>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)</p>
TCP / IP	<p>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.</p> <p>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.</p>

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
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)
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."

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
VNS	Virtual Network Services (VNS). A Enterasys 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.
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.

Table A-1 Networking Terms and Abbreviations (continued)

Term	Explanation
WPA-PSK	<p data-bbox="474 241 1450 359">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.</p> <p data-bbox="474 367 1450 478">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.</p>

Wireless Controller Terms and Abbreviations

Table A-2 Wireless Controller Terms and Abbreviations

Term	Explanation
CTP	<p>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 Enterasys 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.</p>
DRM (dynamic radio/RF management)	<p>Dynamic Radio Management (DRM) functionality of the Enterasys Wireless Controller is used to help establish the optimum radio configuration for your Wireless APs. DRM is enabled by default. The Enterasys Wireless Controller's DRM:</p> <ul style="list-style-type: none"> • 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. <p>The DRM feature is comprised of two functions:</p> <ul style="list-style-type: none"> • 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.
Enterasys Wireless Controller	<p>The Enterasys 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.</p>
Langley	<p>Langley is a Enterasys Wireless Convergence Software term for the inter-process messaging infrastructure on the Enterasys Wireless Controller.</p>
Mitigator	<p>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 Enterasys Wireless Controller that receives and manages the RF scan messages sent by the Wireless AP, (3) an Analysis Engine on the Enterasys Wireless Controller that processes the scan data.</p>
Mobility manager (and mobility agent)	<p>The technique by which multiple Enterasys 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 Enterasys Wireless Controllers, to provide mobility to the wireless device user. One Enterasys Wireless Controller on the network must be designated as the mobility manager. All other Enterasys 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.</p>

Table A-2 Wireless Controller Terms and Abbreviations (continued)

Term	Explanation
Data Collector	The Data Collector is an application on the Enterasys 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 Enterasys's means of mapping wireless networks to the topology of an existing wired network. When you set up Virtual Network Services (VNS) on the Enterasys Wireless Controller, you are defining subnets for groups of wireless users. This VNS definition creates a virtual IP subnet where the Enterasys 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 Enterasys Wireless Controller, one or more Wireless APs (by radio) are associated with it. A range of IP addresses is set aside for the Enterasys 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 Enterasys 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.

Regulatory Information



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

This appendix provides regulatory information for the Enterasys Wireless Controller C25/C20/C4110/C5110 and the Enterasys Wireless AP models.

For information about...	Refer to page...
Enterasys Wireless Controller C25/C20/C4110/C5110	B-2
Wireless APs 26XX, 36XX, and 37XX	B-3



Note: Throughout this appendix, the term 'Wireless AP' refers to AP models (AP26XX series, AP36XX series, and AP37XX 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 Enterasys Wireless Outdoor AP, models AP 2650/2660, see the Enterasys Wireless *Outdoor AP Installation Guide*. For technical specifications and certification information for the Enterasys Wireless Outdoor AP3660, see the Enterasys Wireless *Outdoor AP3660 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 Enterasys Wireless Controller or the Wireless APs which are not expressly approved by Enterasys could void the user's authority to operate the equipment.

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



Note: The Enterasys 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.

Enterasys Wireless Controller C25/C20/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

Rack Mounting Your System

Refer to the following guidelines when setting up your Enterasys 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 (T_{ma}) 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).

Wireless APs 26XX, 36XX, and 37XX

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.

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.

Table B-1 Wireless AP Wi-Fi Certification ID

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



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

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.

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.

United States

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.

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 Enterasys certified antennas. Any changes or modification to the product not expressly approved by Enterasys 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.

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. For all external antennas, the minimum separation distance should be 25 cm. However, 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 42cm.

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 [AP2620 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.

For all external antennas, the minimum separation distance should be 25 cm. However, 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 42cm.

Canada

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 numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée 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.

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)

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 [AP2620 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.

For all external antennas, the minimum separation distance should be 25 cm. However, 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 42cm.

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 Enterasys.

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).



Declaration of Conformity in Languages of the European Community

English	Hereby, Enterasys, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Enterasys 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 Enterasys 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 Enterasys 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 Enterasys 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, Enterasys 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 Enterasys 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 Enterasys erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Enterasys 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 Enterasys ΔΗΛΩΝΕΙ ΟΤΙ Radio LAN device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Icelandic	Enterasys lýsir her með yfir að thessi bunadur, Radio LAN device, uppfyllir allar grunnkröfur, sem gerðar eru í R&TTE tilskipun ESB nr 1999/5/EC.
Italian	Con la presente Enterasys 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 Enterasys 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	Enterasys declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, Enterasys, jiddikjara li dan Radio LAN device jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.

New Member States Requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab Enterasys seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungary	Alulírott, Enterasys nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.

DRAFT

Slovak	Enterasys týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	Enterasys tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."
Slovenian	Šiuo Enterasys deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo Enterasys deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem
Lithuanian	Enterasys deklaruoja, kad Radio LAN device atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Polish	Niniejszym, Enterasys, deklaruję, że Radio LAN device spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

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

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 [AP2620 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.

For all external antennas, the minimum separation distance should be 25 cm. However, 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 42cm.

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 Enterasys 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 Enterasys 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 Enterasys.
- 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.

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 B-2](#). Some restrictions apply in Belgium, France, Greece, and Italy.

Table B-2 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)
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

Table B-2 European Spectrum Usage Rules (continued)

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)
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
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



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

Certifications of Other Countries

The Wireless APs have been certified for use in various other countries. When the Wireless AP is connected to the Enterasys 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 [AP2620 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)

AP2620 Approved External Antennas

The AP2620 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 optional antennas listed in [Table B-3](#) have been tested and approved for use with the external antenna models.

This device has been designed to operate with the optional antennas listed below, and having a maximum gain of 18 dB. Antennas not included in this list or having a gain greater than 18 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication.

Table B-3 List of FCC/IC/ETSI Approved Antennas — AP2620

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-2S14090	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

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.

For all external antennas, the minimum separation distance should be 25 cm. However, 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 42cm.

AP3620 Approved External Antennas

The AP3620 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 optional antennas listed in [Table B-4](#) have been tested and approved for use with the external antenna models.

This device has been designed to operate with the optional antennas listed below, and having a maximum gain of 23 dB. Antennas not included in this list or having a gain greater than 23 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication.

Table B-4 List of FCC/IC/ETSI Approved Antennas — AP3620

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

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.

For all external antennas, the minimum separation distance should be 25 cm. However, 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 42cm.

Certified 3rd Party Antennas

Table B-5 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.

Table B-5 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	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
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

Table B-5 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	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



Default GuestPortal Source Code

For information about...	Refer to page...
Ticket Page	C-1
GuestPortal Sample Header Page	C-4
GuestPortal Sample Footer Page	C-5

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!

Placeholders Used in the Default GuestPortal Ticket Page

Table C-1 Default GuestPortal Ticket Page Template Placeholders

Placeholder tag	Description
!GuestName	Guest Name
!GuestComment	Guest Comment
!TimeOfDayStart	Time-of-day start
!TimeOfDayDuration	Time-of-day session duration
!SessionLifeTime	Maximum session time

DRAFT

Table C-1 Default GuestPortal Ticket Page Template Placeholders (continued)

Placeholder tag	Description
!UserID	User ID for the guest
!Password	Password for the guest
!SSID	SSID to connect to
!AccountActivationTime	Account available time
!AccountLifeTime	Account life time

Default GuestPortal Ticket Page Source Code



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

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>

```

```

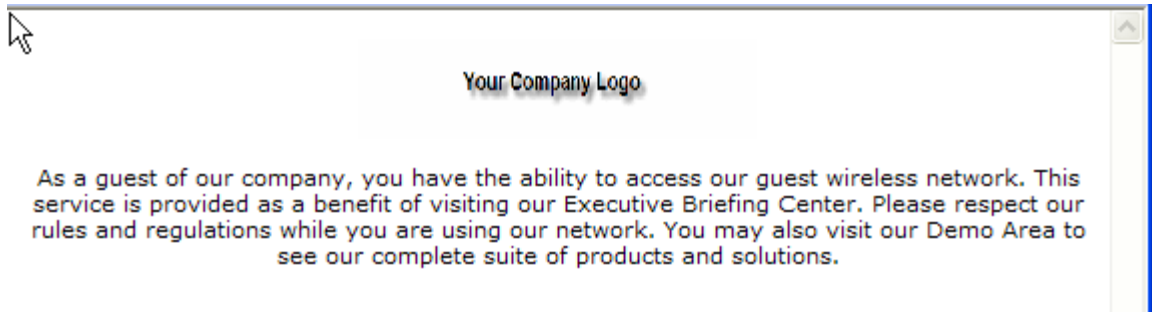
<div style="width:790px;margin:10px auto;text-align:left">
    <b>Instructions:</b>
    <hr width=790 size=2 noshade>
    <div style="padding-left:30px;">
        <ul>
            <li>Enable your wireless device to connect to the '!SSID' SSID.
            <li>Once connected, launch your Internet browser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

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

GuestPortal Sample Header Page



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">
    </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>
```

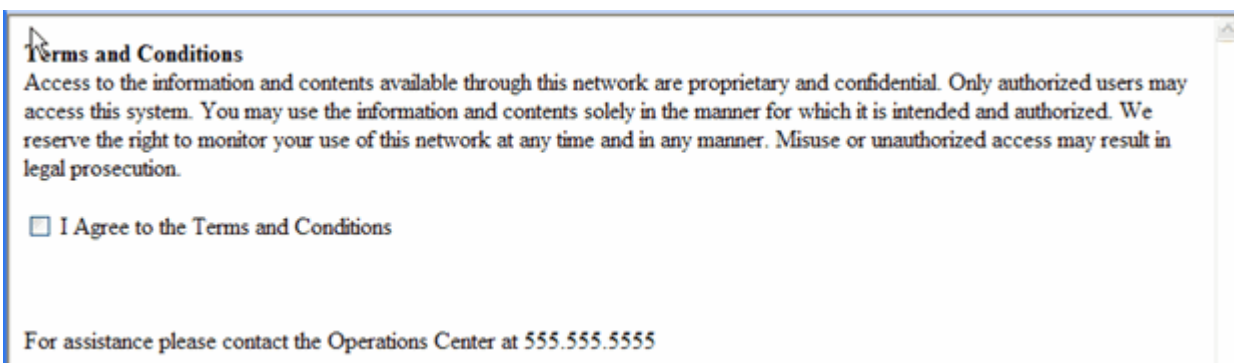
```

<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">
  </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>

```

GuestPortal Sample Footer Page



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>
```