



Configuration Guide

NetVanta 160 Series Wireless Configuration Guide

This configuration guide provides an overview of wireless technology, the elements of wireless local area networks (WLANs), methods for configuring ADTRAN Operating System (AOS) NetVanta 160 Series access points (APs), radios, and virtual access points (VAPs), as well as WLAN topography overviews. For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide* available online at the ADTRAN support community (<https://supportforums.adtran.com>).

This guide consists of the following sections:

- *Introduction to Wireless Technology on page 2*
- *Hardware and Software Requirements and Limitations on page 6*
- *Configuring the AOS AP on page 7*
- *Configuring the AOS AP Radios on page 21*
- *Configuring AOS AP Virtual Access Points on page 24*
- *WLAN Topographies on page 33*
- *Troubleshooting on page 36*
- *CLI Configuration Example on page 40*
- *Appendix A: Supported Country-Region Radio Channels on page 41*
- *Appendix B. Creating MAC ACLs Using the GUI and CLI on page 49*

Introduction to Wireless Technology

WLANs are becoming the new standard in small- and medium-sized business models. By using wireless technology, users can become more productive while decreasing the cost of connectivity for the business. WLANs provide an excellent alternative for growing businesses to the costly procedure of extending wired local area networks (LANs).

WLANs replace Layer 1 transmission media, such as CAT 5 cabling, with radio transmissions that enable wireless user connectivity and the extension of a wired network.

ADTRAN WLAN Components

There are many ways to incorporate WLANs into existing LANs. ADTRAN creates WLANs by adding one or more AOS APs to an access controller (AC). In an ADTRAN WLAN network architecture, there are four primary components: an AC, APs, radios, and VAPs.

The AC is usually a router or a switch that controls and configures the behavior of the AP. Each AOS AC can control between 8 and 24 AOS APs (either NetVanta 160 Series standalone APs or embedded APs such as the NetVanta 1335 Wi-Fi) and communicates with them using ADTRAN Wireless Control Protocol (AWCP) during configuration and status querying.

The AP is connected to the AC through the Layer 2 broadcast domain and provides wireless access for mobile users. The AP is configured by the AC and determines how users will connect to the network. The NetVanta 160 and 161 APs contain internal 802.11a and 802.11b/g radios that can operate in 802.11a, 802.11a/n, 802.11b/g, 802.11b/g/n, or 802.11g/n modes. The NetVanta 161 AP can accommodate up to six antennas for maximum network usability.

VAPs are logical entities that exist within the physical AP, yet appear to wireless clients as independent APs. Each AOS AP supports up to eight VAPs per radio, and each VAP is identified by a service set identifier (SSID).

Basic WLAN Structure

The basic structure of the WLAN is as follows: An AC resides on a wired network with Telnet and/or Web access enabled for configuration, and a desired number of APs (up to 24) are wired to the AC. The APs may be wired directly to the AC, or they may be connected to a switchport somewhere in the attached network. The APs receive and transmit data to wireless clients, allowing client access in a range of locations.

When arranging the WLAN components, there are a number of criteria to keep in mind.

1. The AOS APs will only operate in thin access point mode. This means the AOS AP must be hardwired to an AOS AC, router, or switch somewhere on the network, so consideration must be given to the distance and placement of the AOS AP in relation to the AC for the most coverage area for wireless clients.
2. Obstructions and metal surfaces can create disturbances and interference in the wireless signals, so consideration must be given to the area surrounding the AP.
3. Overlapping cells and channel reuse will occur when too many APs are placed too close together. This overlap will result in signal degradation. To maximize user throughput, APs should be placed such that overlapping of cells on the same channel does not occur.

WLAN Standards

Wireless technology uses standards of IEEE 802.11, namely 802.11b, 802.11g, 802.11a, and 802.11n for communication. Both the NetVanta 160 and 161 APs have two radios: one for receiving and transmitting on 2.4 GHz and one for 5 GHz transmissions. The 2.4 GHz radio supports 802.11b/g/n standards, and the 5 GHz radio supports 802.11a/n standards. The decision of which radio and standard to use should be based on a particular network's needs. The standards are described in the following sections.

802.11b

802.11b is the earliest version of the 802.11 standard. In North America, 802.11b supports channels 1 through 11, which can be divided into three non-overlapping, non-interfering channel sets (channels 1, 6, and 11). This allows three 802.11b APs to operate in close proximity without interference.

802.11b supports rate shifting bandwidths of 1, 2, 5.5, and 11 Mbps operating on the 2.4 GHz frequency.

The 802.11b signal range reaches approximately 100 meters in an unobstructed area and approximately 60 meters in an office environment.

Points to remember when considering the use of 802.11b are that (1) the frequency it uses is potentially crowded by the use of other APs, cordless phones, and microwaves; (2) its speed capabilities are the lowest of the WLAN implementations; and (3) it does not allow for more than three non-overlapping channel assignments, thus restricting the number of users, as well as the data rate available.

802.11g

802.11g works on the same band as the 802.11b (2.4 GHz), but it operates at the higher data rate of 54 Mbps. 802.11g hardware is operable with 802.11b hardware; however, the presence of 802.11b participants in an 802.11g network significantly reduces the speed of the network.

The 802.11g signal range is approximately 100 meters in unobstructed areas and approximately 75 meters in an office environment.

One advantage to using 802.11g is that it has a higher data rate than the 802.11b, which provides more bandwidth per user. Something to keep in mind with the 802.11g is that, like the 802.11b, its frequency can be crowded by the interference of other APs, cordless phones, and microwaves.

802.11a

The 802.11a standard operates in the 5 GHz band, and provides 12 non-overlapping channels which are separated into three ranges. The lowest range is 5.15 to 5.25 GHz, which allows four non-overlapping channels; the middle range is 5.25 to 5.35 GHz, which also allows for four non-overlapping channels; and the highest range is 5.725 to 5.825 GHz, which is used for outside point-to-point or point-to-multipoint applications. Each range has its own regulated power and antenna requirements.

The 802.11a standard is inoperable with either 802.11b or 802.11g. The 802.11a uses a higher band frequency than the 802.11b/g, so there is less interference to contend with. The 802.11a also provides more total bandwidth, which allows more bandwidth per user.

The 802.11a signal range is approximately 50 meters in an unobstructed area, and approximately 25 meters in an office environment.

Points to remember when considering the use of 802.11a include the fact that the higher frequency is more easily absorbed by less dense objects, such as walls and ceiling tiles. Also, for larger coverage areas the power input to the mobile device's radio must be higher, resulting in reduced battery life and mobility

connection time for the mobile user. The number of clients using A cards is also less than with B/G cards, an important factor in determining your network's needs.

802.11n

The 802.11n standard is the newest widely adopted standard in the 802.11 family. The 802.11n builds on the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and 40 MHz channels to the physical layer, as well as adding frame aggregation to the medium access control (MAC) layer. The 40 MHz channels double the channel width from the 20 MHz of previous 802.11 channels and provide twice the data rate available over previous channels. These 40 MHz 802.11n channels can be enabled in 5 GHz mode, or in the lower 2.4 GHz modes of the 802.11b/g channels as long as it will not interfere with any other 802.11 devices (802.11b/g radios or Bluetooth devices).

802.11n devices should generally operate in 5 GHz mode because there are fewer overlapping radio channels and less interference than in the 2.4 GHz mode. When creating a network with 802.11b/g/n radios and devices, configuring the 2.4 GHz radio to operate and legacy 802.11b/g mode and the 5 GHz radio to operate in 802.11a/n mode provides the most optimal 802.11 radio configuration for both legacy and new devices.

Comparing 802.11b/g/a/n

The following chart compares the major characteristics of all four standards.

Table 1. WLAN Standards Characteristics

Characteristic	802.11b	802.11g	802.11a	802.11n
Frequency Band	2.4 GHz	2.4 GHz	5.8 GHz	2.4 GHz or 5 GHz
Modulation	Direct-sequence spread spectrum (DSSS)	DSSS/Orthogonal frequency-division multiplexing (OFDM)	OFDM	OFDM
Data Rates	1, 2, 5.5, 11 Mbps	DSSS - 1, 2, 5.5, 11 Mbps OFDM - 6, 9, 12, 15, 24, 36, 48, 54 Mbps	6, 9, 12, 15, 24, 36, 48, 54 Mbps	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 Mbps for 20 MHz 15, 30, 45, 60, 90, 120, 135, 150 Mbps for 40 MHz
Max Data Rate	11 Mbps	54 Mbps	54 Mbps	150 Mbps (20 MHz) 300 Mbps (40 MHz)

Table 1. WLAN Standards Characteristics (Continued)

Characteristic	802.11b	802.11g	802.11a	802.11n
Effective Data Throughput	5 Mbps	32 Mbps	32 Mbps	90 Mbps per stream on a 20 MHz channel, 200 Mbps on 40 MHz channel
Advertised Range	100 m	100 m	75 m	N/A
Office Range	60 m	75 m	25 m	N/A
Non-overlapping Channels	3	3	8	23
Interfering Services	Cordless Phones, Microwaves, Bluetooth Devices	Cordless Phones, Microwaves, Bluetooth Devices	HyperLAN Devices, Maritime, Satellite and RADAR Systems	Cordless Phones, Microwaves, Bluetooth Devices, HyperLAN Devices, Maritime, Satellite and RADAR Systems (depending on GHz used)
Availability	Worldwide	Worldwide	Limited	Limited

WLAN Security

Wireless security is an important factor in the configuration of a WLAN. An AOS AP supports the 802.11 wired equivalent privacy (WEP), 802.1x, Wi-Fi protected access (WPA), and WPA2 security modes. An understanding of the security parameters necessary for a particular network is required before configuring the WLAN. Review the following short descriptions of security commands.

Personal Modes: Preshared Keys (PSK)

- The **WEP: OPEN** security parameter allows clients to connect using WEP keys, based on the 802.11 standards. In this security mode, open authentication with static WEP keys is used.
- The **WEP: SHARED** security parameter allows clients to connect using WEP keys, based on the 802.11 standards. In this security mode, shared authentication with encrypted static keys is used.



*Although **WEP: SHARED** uses encrypted keys, plain-text challenge requests present security risks that must be taken into account when determining the correct network security parameters.*

- The **WPA: TKIP** parameter allows clients to connect using WPA personal and preshared keys, without requiring a Remote Authentication Dial-In User Service (RADIUS) authentication server. Temporal Key Integrity Protocol (TKIP) specifies the algorithms used for rotating keys.



Based on 802.11n standards, using TKIP for encryption forces the radio to function at legacy rates, even if it is configured for 802.11n mode.

- The **WPA/WPA2: TKIP/AES-CCMP** parameter allows clients to connect through either WPA or WPA2 personal to associate with each other, also without requiring a RADIUS authentication server. TKIP specifies the algorithms used for rotating keys in conjunction with Advanced Encryption Standard and Counter Mode CBC MAC Protocol (AES-CCMP), which specifies the algorithms used for WPA2.

Enterprise Modes (Radius/802.1x)

- The **WPA: TKIP: EAP** parameter allows clients to connect using WPA enterprise and 802.1x authentication. A RADIUS authentication server is required. TKIP specifies the algorithms used for rotating keys, while Extensible Authentication Protocol (EAP) provides a universal authentication framework in the wireless network.
- The **WPA2: AES-CCMP: EAP** parameter allows clients to connect using WPA2 enterprise along with 802.1x authentication. A RADIUS authentication server is required. This parameter combines the use of AES-CCMP algorithms with the EAP universal wireless authentication framework.
- The **WPA/WPA2: TKIP AES-CCMP: EAP** parameter allows clients to connect using either WPA or WPA2 enterprise with 802.1x authentication. A RADIUS authentication server is required. By using this parameter, both WPA and WPA2 protocols are supported with a combination of TKIP, WPA2 algorithms (AES-CCMP), and the use of EAP universal wireless authentication framework.



For RADIUS authentication to function, the AP must be assigned an IP address and gateway. Refer to [Step 5: RADIUS Server on page 15](#) of this guide for more information.

For more detailed information regarding security options, refer to the *NetVanta 160 Wireless Interface Command Sets* in the *AOS Command Reference Guide* available online at <https://supportforums.adtran.com>.

Hardware and Software Requirements and Limitations

The NetVanta 160 Series WLAN features were introduced in AOS R10.4.0. Support for WLAN, WEP key generation, and the number of supported access points (APs) are available on AOS products as outlined in the *AOS Feature Matrix* available online at <https://supportforums.adtran.com>.

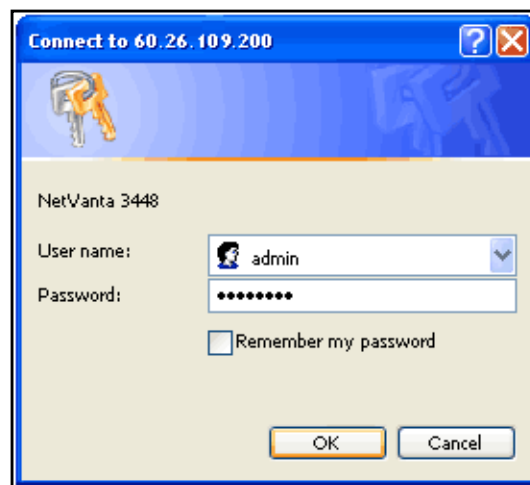
Configuring the AOS AP

There are two ways to begin configuring an AOS AP: (1) the Web-based graphical user interface (GUI) and (2) the command line interface (CLI). The remainder of this configuration guide pertains particularly to the GUI; for descriptions of CLI functions, refer to the *AOS Command Reference Guide*.

Accessing the GUI

You can access the GUI from any Web browser by following these steps:

1. Connect the AC to your PC using the switchports labeled **0/1** to **0/n** or the **ETH 0/1** or **ETH 0/2** ports on either the back or the front of the unit depending on the product. Also, connect the AOS AP to the AC either by using the **ETH 0/1** or **ETH 0/2** ports on the back of the unit or by connecting the AP to a switchport somewhere in the attached network. As long as the controller and AP are connected by the same broadcast domain, control can be established.
2. Set your PC to a fixed IP address of 10.10.10.2. If you cannot change the PC's IP address, you will need to change the AC's IP address using the CLI. (Refer to the quick start guide shipped with your ADTRAN controlling unit for instructions).
3. Enter the AC's IP address in your browser address line in the following form: **http://<ip address>**, for example: **http://60.26.109.200**.
4. At the prompt, enter your user name and password (the default settings are **admin** and **password**).



5. The initial GUI menu appears.

Accessing the Configuration Wizard

Once connected to the GUI, expand the **Data** tab on the left side of the menu if not expanded already. Navigate to **Data > Wireless > AC/AP Discovery** to gain access to the configurations of the AC and APs.

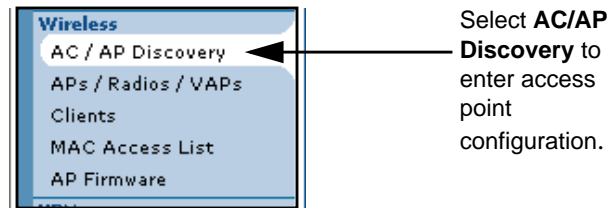
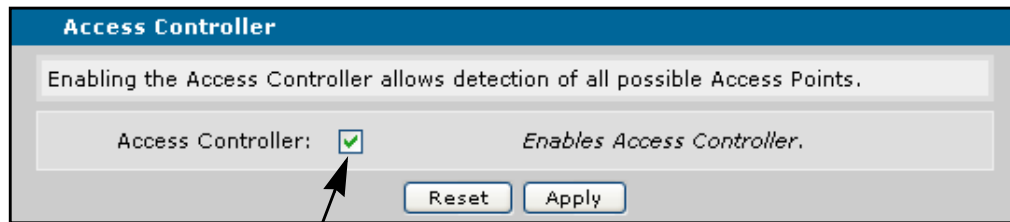


Figure 1. Wireless Menu

The AC must be enabled to automatically detect APs. To enable the AC, check the box by **Access Controller** at the top of the menu and select **Apply**.



Select **Access Controller** to enable the AC.

Figure 2. Access Controller Menu



APs can be manually added to the AC. The wizard is only for the configuration of APs that are automatically detected.

Once the AC is enabled, it will search for nearby APs. When APs are detected by the AC, they will appear at the bottom in the **Dynamically Discovered Access Points** portion of the menu (see [Figure 3](#)). The

Wizard button will appear to the right of the discovered AP, verifying that the AC has detected an AP and it can now be added to the controller. Select the **Wizard** button to begin configuring the AP.

Dynamically Discovered Access Points

The list below contains all of the access points (APs) detected by the access controller. For non-configured APs, click on the 'Wizard' button for configuration. After the AP is setup, the 'Wizard' button will be hidden. To modify an existing AP, or to add a new AP, go to the [APs/Radios/Vaps](#) page.

Name	MAC Address	Status	Control Status
Adtran1DF93B	00:A0:C8:1D:F9:3B	Session	Controlled by this AC
Adtran1F6F1B	00:A0:C8:1F:6F:1B	Available	N/A

Refresh in 3 seconds...

Figure 3. Dynamically Discovered Access Points Menu



*APs that appear in the **Dynamically Discovered Access Points** menu will not be controlled by the AC until each is added manually.*

Using the Configuration Wizard

Once the **Wizard** button has been selected, a new window will open to guide you through adding an AP to the controller. After the introduction menu, select **Next** to proceed to *Step 1: AP Information on page 10*.

Step 1: AP Information

The first step of the Wireless Wizard will ask for information regarding the AP's name, location, and the country in which it is operated.

The screenshot shows the 'Wireless Wizard: Step 1' configuration interface. On the left is a blue sidebar with a menu: 'Welcome', 'Configure AP' (highlighted), '802.11a Radio', '802.11b/g Radio', and 'Confirm'. The main content area has a title bar 'Wireless Wizard: Step 1' and a sub-header 'AP MAC: 00:A0:C8:1F:6F:1B'. Below this are three rows of input fields: 'AP Name' (text box, note: 'Enter a unique name to identify this access point.'), 'AP Location' (text box, note: 'Optional'), and 'AP Country-Region' (dropdown menu showing 'United States', note: 'Identify the country where the AP is being operated. You must enter a country.'). At the bottom are three buttons: '< Back', 'Next >', and 'Exit'.

Figure 4. Identifying the Access Point

Use a unique name to identify this particular AP. The AP location is optional and only serves to further identify this AP. The **AP Country-Region** drop-down menu specifies the country in which the AP will operate. Countries in which the AP is certified to operate, as well as those that are not certified, are displayed. If an uncertified country is selected, and the 802.11a radio is not allowed for that country, you will not be able to configure the 802.11a radio. [Appendix A: Supported Country-Region Radio Channels on page 41](#) outlines the 802.11b/g and 802.11a support for all countries available on the drop-down menu.

Once the required information has been entered, select **Next** to move to **Step 2**.

Step 2: Enabling 802.11a Radio

Step 2 provides the settings for enabling radio 802.11a. If an 802.11a radio is not necessary for your network, do not check the enable box; instead select **Next** at the bottom of the menu. Selecting **Next** will take you to the enabling menu for the 802.11b/g radio, in which case proceed with Step 2 through Step 5 for the 802.11b/g radio.

If you wish to use the 802.11a radio in your network, check the enable box and enter the required information (SSID value and broadcast mode).

The **SSID Value** is attached to the packet header. It consists of up to 32 case-sensitive characters and can include spaces. SSIDs serve to differentiate WLANs from one another and VAPs from one another. They are included in the beacon frames in plain text. To broadcast the SSID in the beacon, check the **Enable Broadcast Mode** checkbox. To prevent the SSID from being broadcast, do not enable the broadcast mode.

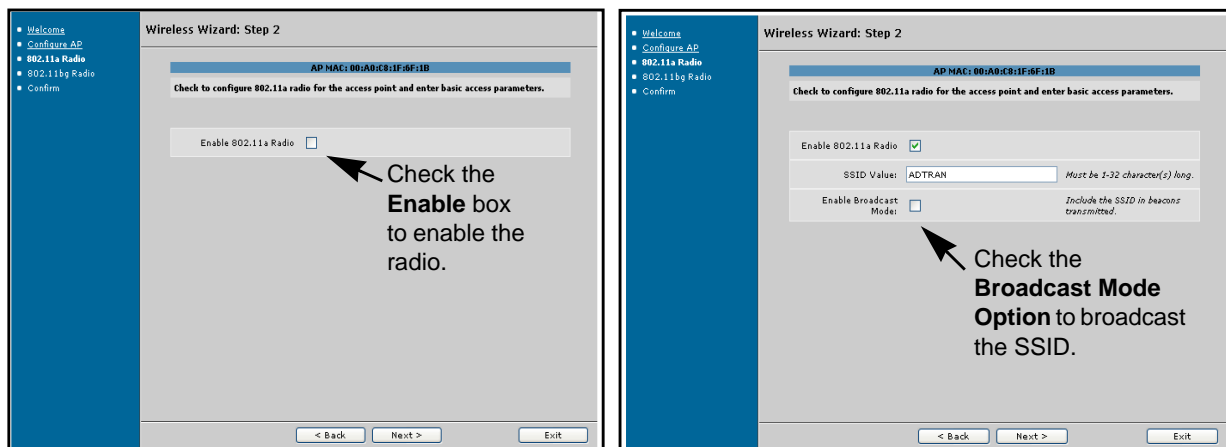


Figure 5. Enabling the 802.11a Radio

Once you have entered the required information, select **Next** at the bottom of the menu to proceed to Step 3.

Steps 3 through 5: Radio Security Configuration

In Step 3, the radio security mode is set by choosing from the drop-down menu. Choose the security mode that best fits your network.

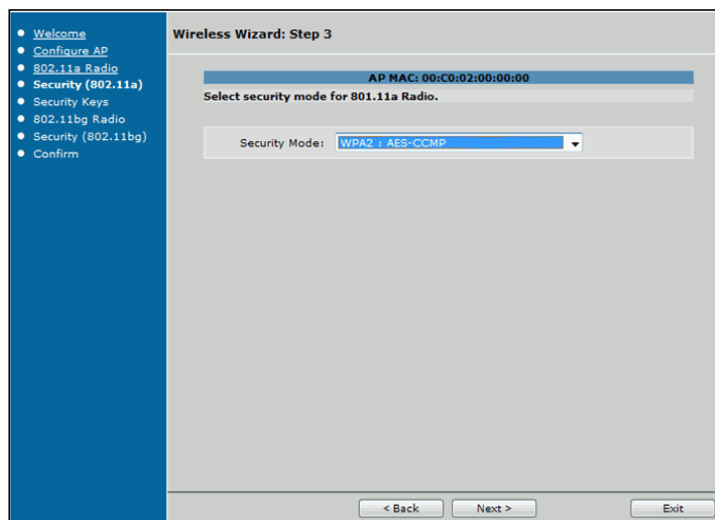


Figure 6. Security Mode Configuration Menu

NOTE *The default security mode is WPA2: AES-CCMP.*

Different security modes require different information for configuration. The three major types of information needed for security parameters are **Preshared Keys**, **WEP keys**, and **RADIUS Server** information. The following is a breakdown of each type of security option, and the steps needed for configuration.

Preshared Key Security Choices

- **WPA2: AES-CCMP**
- **WPA/WPA2: TKIP/AES-CCMP**
- **WPA: TKIP**

Selecting one of these security options in Step 3 will take you to *Step 4A: Preshared Keys on page 13* to enter the preshared key.

WEP Key Security Choices

- **WEP: SHARED**
- **WEP: OPEN**

Selecting one of these security options in Step 3 will take you to *Step 4B: WEP Keys on page 13* to enter the WEP key information.

RADIUS Server Security Choices

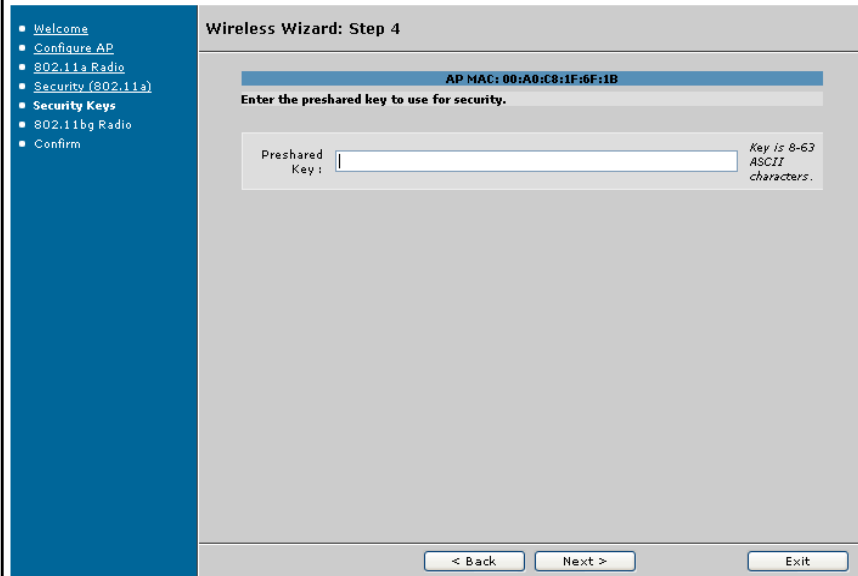
- **WPA/WPA2: TKIP/AES-CCMP: EAP**
- **WPA2: AES-CCMP: EAP**
- **WPA: TKIP: EAP**

Selecting one of these security options in Step 3 will take you to *Step 5: RADIUS Server on page 15* to enter the RADIUS information.

Once the appropriate security mode has been selected, select **Next** to proceed.

Step 4A: Preshared Keys

Certain security modes require the use of preshared keys for generation of a unicast session for each client. After entering the predetermined key name in the **Preshared Key** field, select **Next** to continue to *Steps 6 through 8: Configuring the 802.11b/g Radio on page 15*.



The screenshot shows the 'Wireless Wizard: Step 4' configuration window. On the left is a blue sidebar with a navigation menu containing: Welcome, Configure AP, 802.11a Radio, Security (802.11a), Security Keys, 802.11b/g Radio, and Confirm. The main area has a title bar 'Wireless Wizard: Step 4' and a sub-header 'AP MAC: 00:A0:C8:1F:6F:1B'. Below this is the instruction 'Enter the preshared key to use for security.' A text input field labeled 'Preshared Key:' is present, with a note to its right stating 'Key is 8-63 ASCII characters.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Exit'.

Figure 7. Preshared Key Configuration

Step 4B: WEP Keys

Certain security modes require the use of WEP keys. To use WEP keys, the key size in bits must be entered, along with up to four key names. It is important to remember that in WEP keys with the addition of a 24-bit initialization vector, the 40-bit key becomes 64 bits, the 104-bit key becomes 128 bits, and the 128-bit key becomes 152 bits on the client.



The WEP key generator can be used to generate all four keys from a passphrase. Refer to [WEP Key Generator on page 28](#) for more information.

Wireless Wizard: Step 4

AP MAC: 00:A0:C8:1F:6F:1B

WEP Keys

Choose the key size and enter the keys. Enter a passphrase and generate the keys using md5. **Please be sure to copy the keys and save them somewhere you have access.**

Note: 'Key 1' will be automatically set as the transmit key.

Key Size: 40 Key size in bits.

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

< Back Next > Exit

Figure 8. WEP Keys Configuration



The first key name entered is automatically set to be the transmit key. All four key names must be entered either manually or through the WEP key generator.

After the key information has been entered, select **Next** to continue to *Steps 6 through 8: Configuring the 802.11b/g Radio on page 15.*

Step 5: RADIUS Server

Some security modes require the use of a RADIUS server for authentication. Configure the RADIUS server by entering the IP address of the server along with the secret key for authentication. After this information has been entered, select **Next** to continue to Step 6.

Wireless Wizard: Step 5

AP MAC: 00:A0:C8:1F:6F:1B

Radius Server IP Address: . . . Enter an IP Address for the radius server.

Radius Server Shared Secret: Secret key for radius server authentication.

< Back Next > Exit

Figure 9. Radius Server Configuration



*An IP address for the AP must be set in the **IP Settings** tab (refer to [IP Settings on page 19](#)) for communication with the RADIUS server.*

Steps 6 through 8: Configuring the 802.11b/g Radio

Steps 6 through 8 are exactly the same as [Step 2: Enabling 802.11a Radio on page 10](#) through [Step 5: RADIUS Server on page 15](#)). The configuration process is repeated for the 802.11b/g radio. Once the configurations for the second radio are complete, selecting **Next** will continue on to a confirmation menu.

Confirmation

Once security settings have been configured for both radios, a confirmation menu appears, presenting an opportunity to review and validate information that has been entered. Verify the information and select **Finish** to complete the wizard.

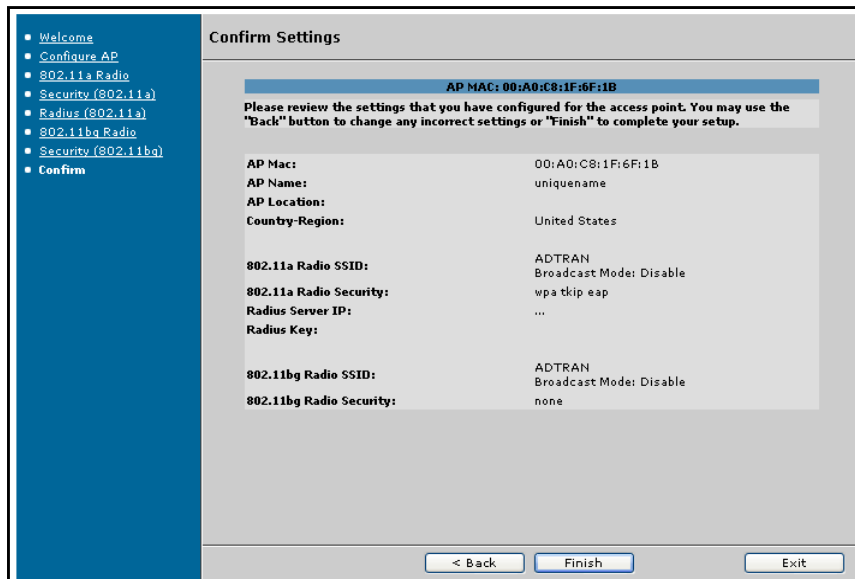


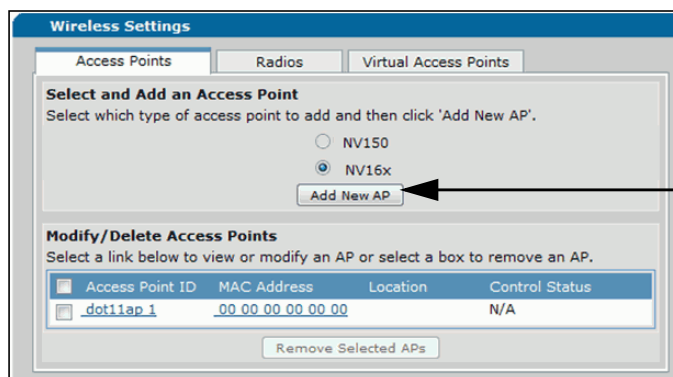
Figure 10. Confirm Settings Menu

The configured APs will appear in the main menu under **Dynamically Discovered Access Points** and will be under the control of the AC. The APs are now accessible for specific configurations.

NOTE *Once an AP is controlled by the AC, the wizard button option will no longer be available.*

Manually Adding an Access Point

APs can also be manually added to the AC. To add an AP, select **Data > Wireless > APs/Radios/VAPs** tab, select **NV 16x**, and then select the **Add New AP** button.



Select **Add New AP** to manually add an interface.

Figure 11. Access Points Tab Menu

After selecting the **Add New AP** button, the following configuration settings are available.

Figure 12. Access Point Configuration Menu

The MAC address of the AP can be obtained by looking at the label on the bottom of the unit. The unit’s MAC address will also show in the **Dynamically Discovered Access Points** menu when the AP is first discovered.

The Ethernet speed, duplex, and 802.1q settings are configured from the **Access Point Configuration** menu. A MAC address filter, as well as IP addresses and syslog forwarding settings, can also be applied to allow only specific clients to communicate with the AP. The MAC access control list (ACL), accessible from a hyperlink on the right of the menu, must be created before you can apply the MAC address filter to the AP.

NOTE For more information regarding the configuration of MAC ACLs, refer to [Appendix B. Creating MAC ACLs Using the GUI and CLI on page 49.](#)

NOTE Each AP ID is designated in the form **dot11ap <ap>**. The <ap> represents the interface number to which the AP is assigned.

Modifying AP Configuration

To modify or view a configured AP, select the link of the AP you wish to view or modify.

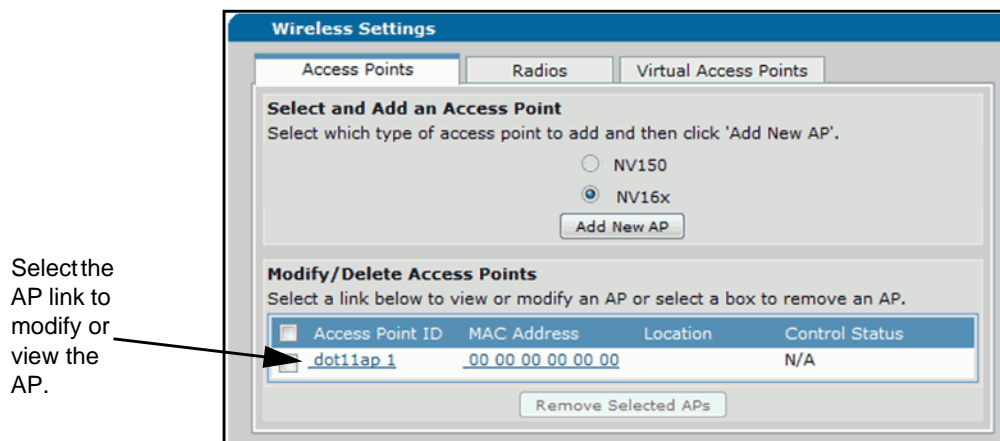


Figure 13. Modify/Delete Access Points Menu

General Parameters

Once you have selected the link, the **Access Point Configuration** menu (the same menu used to statically add an AP, see [Figure 12 on page 17](#)) will open. The menu displays information for a specific AP, including **Access Point Interface**, **Name**, **Location**, **MAC Address**, **Speed/Duplex** settings, **Country/Region**, and **MAC Access List**. From this menu, changes can be made to the preceding parameters.



Multiple ACs can be configured to control a single AP. After an AP reboot, the AP retains no knowledge of the previous AC and will be controlled by the first AC to complete the negotiation handshake. The controlling AC applies its configuration to a controlled AP. If control is passed to another AC, that AC's configuration for the AP will be applied, even if it is different than that of the previous controlling AC. If using multiple ACs to control an AP, it is important that the configuration settings be coordinated and applicable for the overall network design.

IP Settings

The optional IP settings for the AP can be configured from the **IP Settings** tab at the bottom of the **Access Point Configuration** menu. These settings are optional and only used if using a RADIUS server.

The screenshot shows the 'IP Settings' tab in a configuration window. It contains three rows of input fields, each with a numeric keypad and a help icon (question mark). The first row is 'Access Point IP address' with a tooltip: 'Enter the IP address for the Access Point's Ethernet Interface. (optional)'. The second row is 'Access Point IP Mask' with a tooltip: 'Enter the network mask for the Access Point.'. The third row is 'Access Point Default Gateway' with a tooltip: 'Enter the Default Gateway for the Access Point.'. At the bottom of the tab are 'Reset' and 'Apply' buttons.

Figure 14. IP Settings Tab Menu

From the **IP Settings** tab, the AOS AP can be assigned an IP address, IP mask, and default gateway.

NOTE You will not be able to configure the AP (Telnet, SSH, or HTTP/HTTPS) from its IP address. The IP information is used to communicate with a RADIUS authentication server when using 802.1x. It will also respond to Internet Control Message Protocol (ICMP) echo requests (ping) for connectivity testing.

NOTE The IP address must be in the correct subnet for the native virtual local area network (VLAN) to which the AP is connected (if the AP is connected to a VLAN-aware switch). Even if 802.1q encapsulation is enabled, and other VLANs are configured on the AP, the AP uses the configured IP address natively (without VLAN tags) only on its Ethernet interface.

Advanced Settings

Use the **Advanced** settings tab to release control of a specific AP, enable event history logs, and select the type of messages sent via the control protocol. To access the **Advanced** settings menu, select the **Advanced** tab at the bottom of the **Access Point Configuration** menu.

The screenshot shows the 'Advanced' tab in a configuration window. It contains four rows of settings. The first row is 'AP Standby' with an unchecked checkbox and tooltip: 'Release control of this Access Point.'. The second row is 'Syslog Forwarding' with an unchecked checkbox and tooltip: 'Enables the forwarding of messages via syslog.'. The third row is 'Syslog Forwarding Priority Level' with a dropdown menu set to 'Error' and tooltip: 'The level of messages sent to the syslog server, info showing the most.'. The fourth row is 'Syslog Receiver IP Address' with a text input field and tooltip: 'The IP address of the syslog server.'. At the bottom of the tab are 'Reset' and 'Apply' buttons.

Figure 15. Advanced Tab Menu

Check the **AP Standby** box to release control of the AP. By checking this box, the AC will no longer send responses to echoes from this particular AP.

Check the **Syslog Forwarding** box to enable the forwarding of messages using syslog.

Specify the **Syslog Forwarding Priority Level** from the drop-down menu. Choose the message type to be sent via the control protocol. Choices include: **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, and **Debug**.

Specify the IP address of the syslog server in the appropriate field.

VLAN Settings

The VLAN settings are used primarily in the creation of VAPs. The VLAN settings are located on the **VLAN** tab at the bottom of the **Access Point Configuration** menu. Configurations under the **VLAN** menu include enabling 802.1q encapsulation, setting a native VLAN ID, and setting the priority level for 802.1q communication.

The 802.1q encapsulation should be enabled in order to configure VAPs operating on different VLANs. The 802.1q protocol maps VAPs to specific VLANs within the network via trunking, thus dividing the network among specific groups of users.

Setting the native VLAN ID specifies the VLAN over which the AWCP, RADIUS, and syslog traffic will pass.

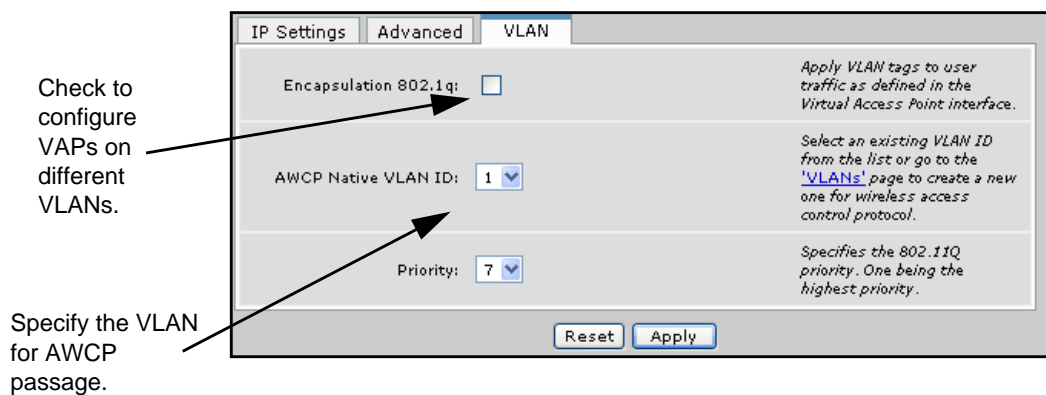


Figure 16. VLAN Tab Menu

For more information regarding VAPs, refer to *Configuring AOS AP Virtual Access Points on page 24* of this guide. For an example VAP/VLAN topography, refer to *Virtual Access Point Model on page 35* of this guide.

Applying the Settings

Any settings configured or changed on the NetVanta 160 Series must be applied twice: once to the AC controlling the AP and once to the AP itself.

When all parameters for the AP are configured, select the **Apply** button at the bottom of the **Access Point Configuration** menu to apply the settings to the AC.

To apply the settings, or any setting changes, to the AP itself, navigate to **Data > Wireless > AP/Radio/VAPs**. Select the AP in the **Outstanding NV16x Access Point Configurations** menu by

checking the box next to the appropriate AP. Next, select **Configure Selected APs** to apply the configuration to the AP. You must apply the configuration to the AP, or the AP will not be configured.

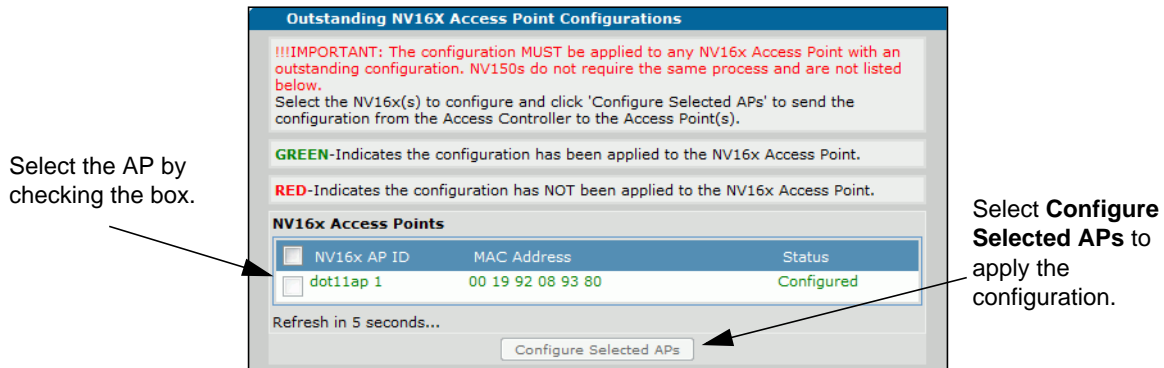


Figure 17. Applying the Configuration to the AP

NOTE *If the AP is listed in red font, some or all of the AC's configuration of the AP is pending, and has not yet been applied to the AP.*

Repeat the process for any additional APs you wish to configure or add.

Configuring the AOS AP Radios

When the AP is configured, both radios are detected and assigned an interface. Selecting **Data > Wireless > APs/Radios/VAPs > Radios** tab will show both radios associated with an AP.

The radio ID is based on the interface to which the AP is mapped (**dot11ap** <ap/radio>, where <ap> is the AP interface number and <radio> is the radio interface number). An asterisk beside the radio ID indicates that the radio is enabled. Each **Radio ID** is a hyperlink that accesses a configuration page for the radio's basic and advanced settings.

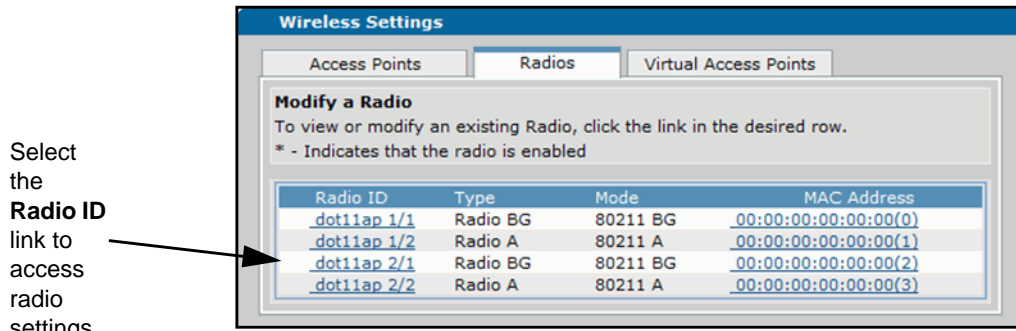


Figure 18. Radios Tab Menu

NOTE *The radios are automatically detected. You cannot manually add or delete radios.*

Basic Settings

Basic radio settings include enabling the radio; selecting the station role, radio channel, and rate. To enter the basic configuration menu, select the **Basic** tab.

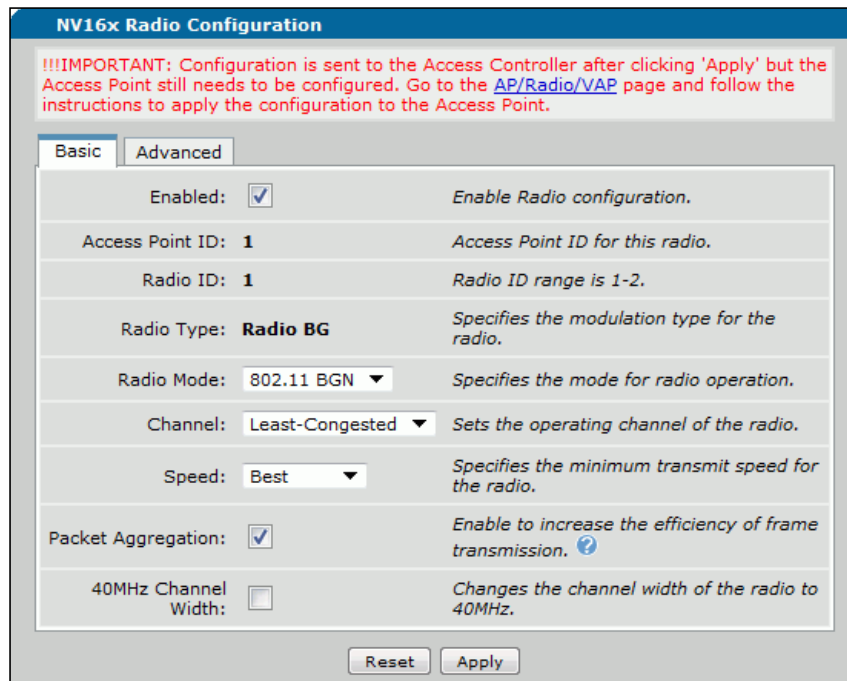


Figure 19. Radio Configuration Basic Tab Menu

Selecting Enabled

Enabling the radio will determine whether the radio is broadcasting.

Selecting the Radio Mode

The **Radio Mode** drop-down menu specifies in which mode the radio will be operating. **BG** Radios can operate in **BG** mode, **BGN** mode, or **GN** mode. **A** radios can operate in **A** or **AN** modes.

Selecting Radio Channel and Speed

Radio **Channel** selection sets the operating channel for the radio. The **Channel** can be set to zero to scan for the best channel. Other channel options vary by radio type, but also include a **Least Congested** option. The **Speed** selection is the minimum speed that the AP requires from a client in order to allow the client to connect to the network. The **Speed** selection can be set to **Best** for the best available speed or to a specific speed.

Selecting Packet Aggregation

Packet Aggregation, when enabled, increases the efficiency of frame transmission for data packets.

Enabling 40 MHz Channel Width

Enabling the 40 MHz channel width changes the width of the radio channel to 40 MHz.

Advanced Settings

The **Advanced** tab provides many options for radio configuration, including antenna settings and power options.

NV16x Radio Configuration

!!!IMPORTANT: Configuration is sent to the Access Controller after clicking 'Apply' but the Access Point still needs to be configured. Go to the [AP/Radio/VAP](#) page and follow the instructions to apply the configuration to the Access Point.

Basic | **Advanced**

Inactivity Timeout Max:	5	Sets the inactivity timeout for an association. Range is 1-99.
Fragment Threshold Length:	2346	Wireless link transmit packets beyond this length will be fragmented. Range 256-2346.
Beacon Period:	100	Period of time between beacons in 802.11 time units (TU). Range 20-1000.
RTS Threshold:	2346	Sets the length of the RTS Threshold. Range 256-2346.
Local Power Level:	Full	Sets the transmit power level.
Antenna:	MIMO 2x2	Sets transmit and receive antenna.

Reset Apply

Figure 20. Radio Configuration Advanced Tab

For optimal radio operation, most of the advanced setting defaults should remain unchanged. The default values are described in [Table 2](#):

Table 2. Radio Default Settings

Parameter	802.11b/g/n Radio Defaults	802.11a/n Radio Defaults
Inactivity Timeout Max	5	5
Fragment Threshold Length	2346	2346
Beacon Period	200	200
RTS Threshold	2346	2346
Local Power Level	Full	Full
Antenna	MIMO 2 x 2	MIMO 2 x 2

When radio configuration is complete, select the **Apply** button at the bottom of the menu to apply the settings to the AC. To apply the changes to the AP, follow the instructions in [Applying the Settings on page 20](#).

Configuring AOS AP Virtual Access Points

A VAP is a logical representation of a wireless network. VAPs are distinguished by an SSID and can be mapped to a VLAN. VLAN information can be shared across switches with Ethernet trunks. An AOS AP can terminate Ethernet trunks and associate a VAP with a VLAN. A common example of this is having two VAPs, one associated to a corporate VLAN and one associated to a guest VLAN.

To configure a VAP, select **Data > Wireless > APs/Radios/VAPs > Virtual Access Point** tab. Each radio will have a default VAP configured. The VAP name is based on the interface to which the AP and radio are mapped (**dot11ap** <ap/radio.vap>, where <ap> is the AP interface number, <radio> is the radio interface number, and <.vap> is the VAP interface number). To add a VAP, select the appropriate **AP, Radio** interface, and **VAP** interface numbers, and then select **Add/Modify**.

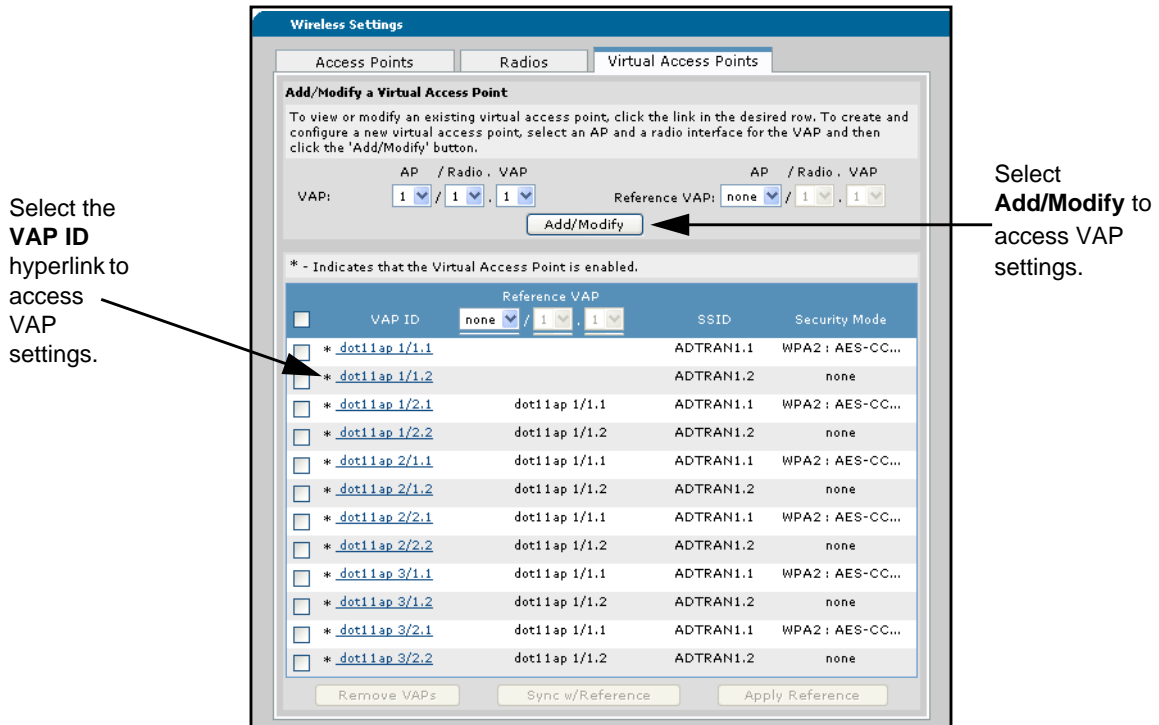


Figure 21. Add/Modify a Virtual Access Point Menu

Once a VAP has been added, it can be accessed either through the **Add/Modify** button or the **VAP ID** hyperlink.

Basic VAP Settings

The **Basic Settings** tab for the VAP is located in the **Virtual Access Point Configuration** menu, accessed by selecting the **VAP ID** hyperlink or **Add/Modify** button on the menu shown in *Figure 21 on page 25*. On the **Basic** settings tab (*Figure 22*), you can define the SSID, turn off SSID broadcast, enable interclient separation, and describe the VAP.

NV16x Virtual Access Point Configuration

!!!IMPORTANT: Configuration is sent to the Access Controller after clicking 'Apply' but the Access Point still needs to be configured. Go to the [AP/Radio/VAP](#) page and follow the instructions to apply the configuration to the Access Point.

Basic	Security
Enabled: <input checked="" type="checkbox"/>	Enables this Virtual Access Point.
VAP Interface: 1	VAP instance on the physical radio. Range 1-8.
Description: <input type="text"/>	Alphanumeric string to be used as a unique description for the VAP.
SSID Value: <input type="text" value="160bg-9380"/>	Service Set Id is a unique id to associate with the radio. Range 1-32 character(s).
SSID Broadcast Mode: <input checked="" type="checkbox"/>	Include the SSID in beacons transmitted.
VLAN ID: <input type="text" value="<Please Select a VLAN ID>"/>	Associate this VAP to a VLAN. To create a VLAN visit the 'VLANs' page. 802.1q must be enabled on the 'AP Configuration' page.
Interclient Separation: <input type="checkbox"/>	Prevents clients within this VAP from communicating directly with each other.

Reset Apply

Figure 22. VAP Basic Settings Tab Menu

If the **SSID Broadcast Mode** is not checked, the AP beacon will no longer broadcast the SSID. This provides a minimal amount of security and it is recommended.

Enabling **Interclient Separation** prevents clients within the VAP from communicating directly with each other.

When the basic settings are configured, select the **Apply** button to activate them on the AC. To apply the changes to the AP, refer to *Applying the Settings on page 20*.

VAP Security Settings

The VAP Security settings tab is located in the **Virtual Access Point Configuration** menu. Choose the security mode of your preference from the drop-down menu.

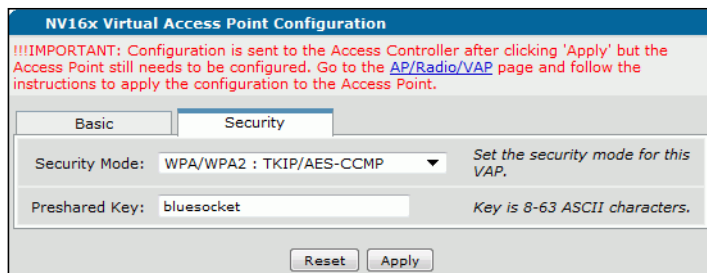


Figure 23. VAP Security Settings Tab Menu

NOTE *The AP and the client must have matching security settings. If using an authentication server, the server settings will have to match the client's as well. If using EAP, the client and authentication server (RADIUS) must use the same EAP types.*

Once the security setting is chosen from the drop-down menu, there will be an automatic prompt for the appropriate information for the particular security setting. The example in [Figure 24](#) uses a WPA setting (WPA: TKIP: EAP).

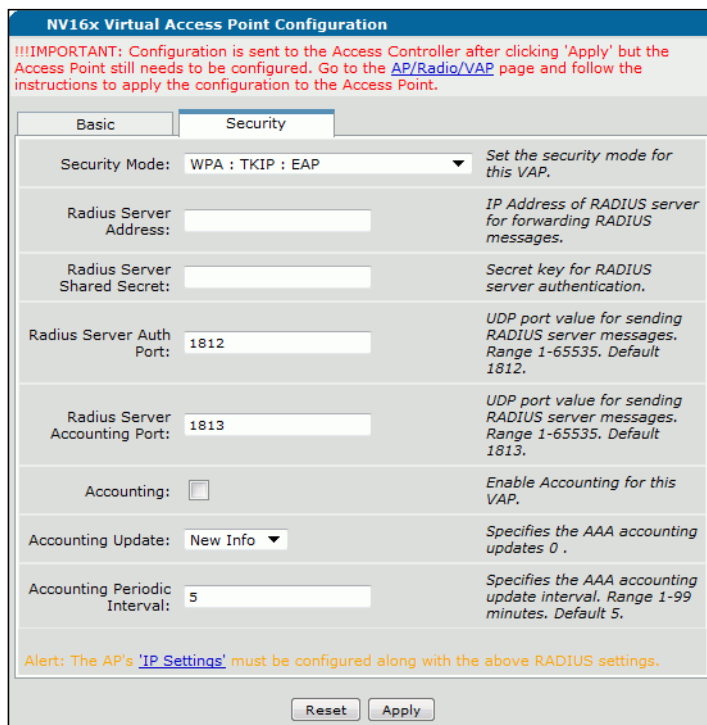


Figure 24. WPA: TKIP: EAP Security Settings Example

WEP Key Generator

All WEP security options include a WEP key generator feature. The feature operates by using a passphrase to generate WEP keys through a standard MD5 key generator. The feature allows for keys to be quickly produced if the passphrase is known. Most mobile clients have the ability to generate keys, and through this feature VAPs will also have the ability to produce these keys. To use the WEP key generator, follow these steps:

1. From the appropriate **VAP Security Settings** menu (any menu that requires a WEP key), enter the passphrase in the appropriate field.

The screenshot shows the 'Virtual Access Point Configuration' window with the 'Security Settings' tab active. The 'Security Mode' is 'WEP: SHARED'. The 'Key Size' is '40'. The 'Passphrase' field contains 'engineering'. A yellow box highlights the 'Generate Keys' button. Below the passphrase field are four rows for 'Key 1' through 'Key 4', each with a text input field and a radio button labeled 'Transmit Key'. The radio button for 'Key 1' is selected. At the bottom are 'Reset' and 'Apply' buttons.

Figure 25. WEP Key Generator Passphrase Menu

The passphrase is a phrase 1 to 32 characters in length. When the **Generate Keys** button is selected, the key generator will generate random values for each element (letter or number) in the passphrase, thus creating secure WEP keys.

2. Once the passphrase has been entered, select **Generate Keys**. Four keys are generated from the single passphrase.

This screenshot is similar to Figure 25 but shows the results of clicking 'Generate Keys'. The 'Passphrase' field now contains 'engineering'. The 'Key 1' field contains '0A5F41E648', 'Key 2' contains '9DDF46B9DB', 'Key 3' contains 'B16CB3E9DA', and 'Key 4' contains '3F937CC7C7'. The 'Generate Keys' button is highlighted in blue. The radio button for 'Key 1' is selected. Two arrows from the right point to the 'Generate Keys' button and the 'Transmit Key' radio button for 'Key 1'. The text next to the arrows reads: 'Select **Generate Keys** and optionally specify which key to transmit.'

Figure 26. Generated WEP Keys

3. The first key generated is automatically set to transmit. To change the transmitted key, select **Transmit Key** next to the key you wish to transmit. Selecting **Reset** will clear the generated keys and set the VAP security mode to **none**.

- Once the security settings have been entered, select **Apply** to add them to the VAP's configuration on the AC. To apply the changes to the AP, refer to *Applying the Settings on page 20*.



*Generated WEP keys will not be part of the VAP configuration until the **Apply** button is selected.*

The basic parameters of the AOS AP and VAP have now been configured. For more information about specific configurations and commands using the CLI, refer to the *AOS Command Reference Guide* available online at <https://supportforums.adtran.com>.

Referencing VAPs

VAP referencing is a feature that allows a single VAP configuration to serve as a reference for quickly configuring other VAPs. This feature facilitates consistent settings across APs, which aids in smooth transitions between APs for mobile wireless clients. The feature allows a VAP configuration to be copied as a reference configuration for configuring other VAPs, tracks the synchronization between referenced VAPs, and also enables quick copying of a VAP configuration to other VAPs even if it is not the reference configuration.

Once a VAP configuration exists to use as a reference, the configuration can be copied to other VAPs either as they are created or as they are modified.

To copy a reference configuration as a new VAP is created, follow these steps:

- To add a VAP, select the appropriate **AP**, **Radio** interface, and **VAP** interface numbers. In the following examples, VAP 1/2.1 is created by copying the VAP configuration of VAP 1/1.1.

Add/Modify a Virtual Access Point

To view or modify an existing virtual access point, click the link in the desired row. To create and configure a new virtual access point, select an AP and a radio interface for the VAP and then click the 'Add/Modify' button.

	AP	/	Radio	.	VAP		AP	/	Radio	.	VAP
VAP:	1	/	2	.	1	Reference VAP:	none	/	1	.	1

Figure 27. VAP Referencing for a New VAP

2. Select the **AP**, **Radio** interface, and **VAP** interface numbers to be referenced from the **Reference VAP** menu.

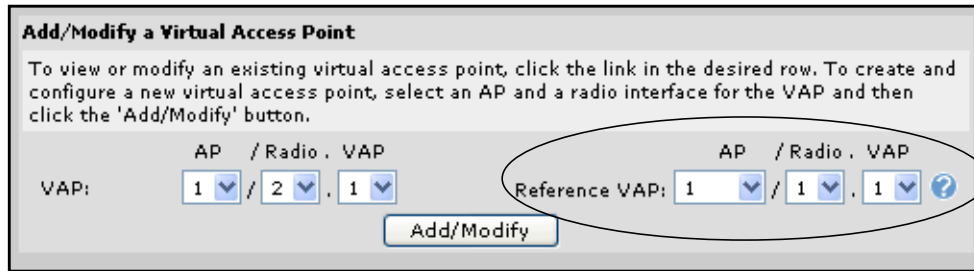


Figure 28. Entering Reference VAP Information

3. Select **Add/Modify** to create a new VAP with the same configuration settings as the selected reference VAP.
4. The new VAP will appear at the bottom of the menu, with a VAP reference listed.

	VAP ID	Reference VAP	SSID	Security Mode
<input type="checkbox"/>		none / 1 . 1		
<input type="checkbox"/>	* dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
<input type="checkbox"/>	* dot11ap 1/1.2		ADTRAN1.2	none
<input type="checkbox"/>	* dot11ap 1/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...

Figure 29. Reference VAP Appearance

To reference a VAP configuration on a previously configured VAP, follow these steps:

1. Select the VAP to which you want to add the reference by checking the box. One or more boxes can be selected.

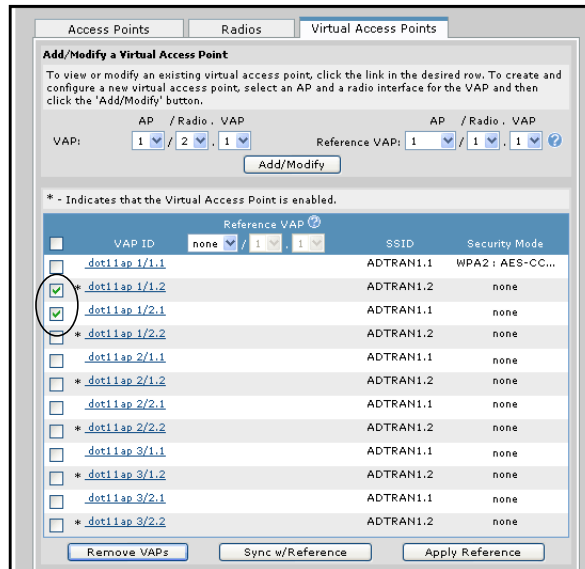


Figure 30. VAP Referencing for a Previously Configured VAP

2. Select the appropriate AP, Radio interface, and VAP interface numbers from the Reference VAP menu.

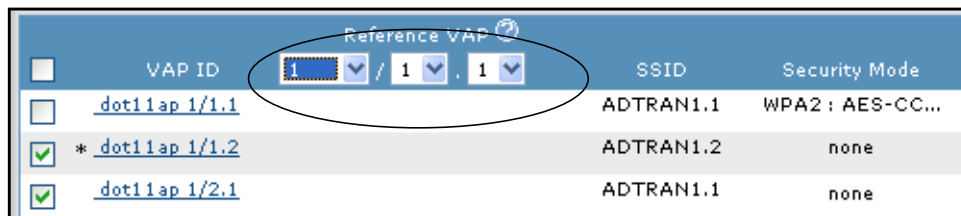


Figure 31. Reference VAP Information

3. Select the **Apply Reference** button at the bottom of the menu to copy the configuration settings from the reference VAP to the selected VAP configuration.

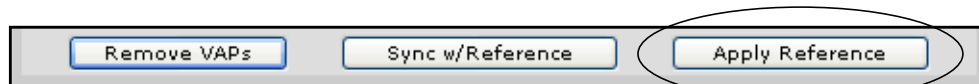


Figure 32. Apply Reference

4. The referenced VAP will appear listed next to the modified VAP.

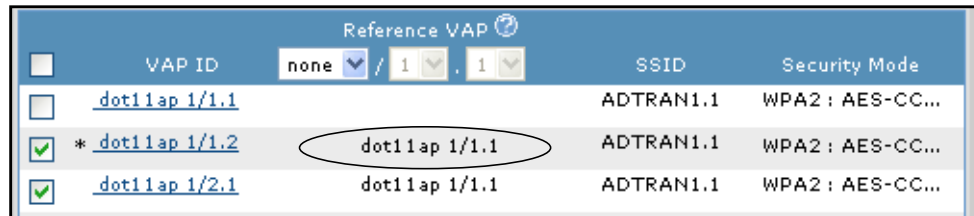


Figure 33. Referenced VAP Appearance

Synchronizing VAP References

The GUI indicates if the VAP and referenced VAP configurations are synchronized. If VAP references are not synchronized, the referenced VAPs will appear in orange. If the referenced VAP no longer exists, the referenced VAP will appear in red. The **Sync w/Reference** button allows the VAP configuration to be updated to match the referenced VAP configuration. The button can be used on a per VAP basis, or by selecting all VAPs, and then selecting the **Sync w/Reference** button.

When referenced VAPs are changed or synchronized, you must apply the changes to the AP. To apply the changes to the AP, refer to [Applying the Settings on page 20](#).

Removing VAP References

References to a VAP configuration can be removed by selecting the VAP with the reference and then selecting **none** from the AP drop-down menu.

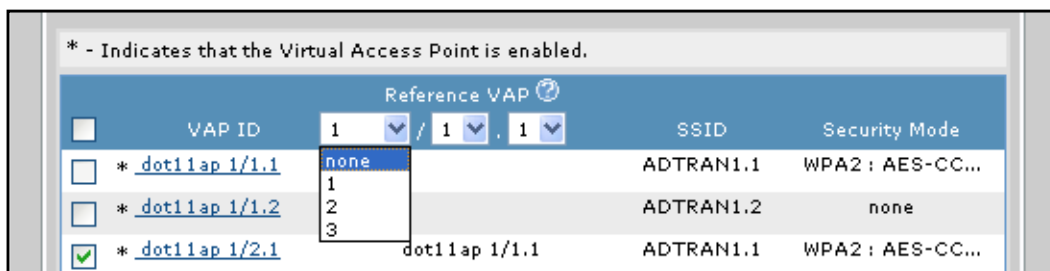


Figure 34. Reference VAP Drop-Down Menu

Once **none** is selected, select the **Apply Reference** button at the bottom of the menu. The reference VAP is removed and will no longer appear in the referenced VAP list. Removing a referenced VAP does not change the VAP configuration settings.

WLAN Topographies

The following are a few examples of typical WLAN network configurations:

- *General Hotspot Connectivity*
- *Small-Medium Business Company Model*
- *Virtual Access Point Model*

General Hotspot Connectivity

The general hotspot connectivity model is a common application of an AOS AP. In this model, there are two T1s entering the building and a NetVanta 160 Series tied to a router/switch. This type of configuration can be used for guest access, such as in an internal corporate hotspot in the lobby of a building. This model can also be used for a lab environment in which the server connects back to the LAN via the wireless connection, or for a conference room allowing attendees access to corporate resources.

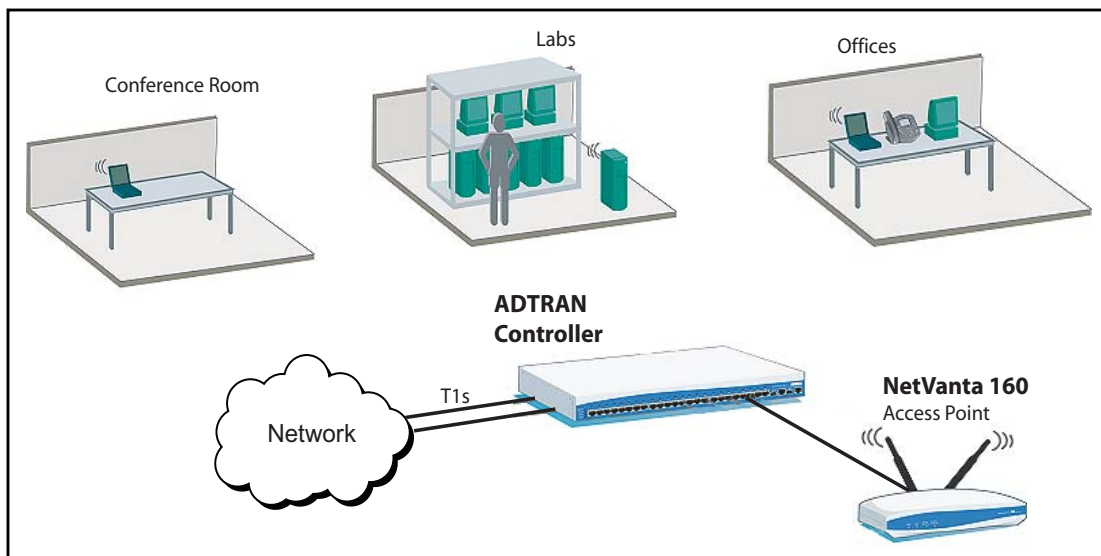


Figure 35. General Hotspot Connectivity

Small-Medium Business Company Model

This is a typical small- to medium-sized business model. There are two T1 lines entering the router/switch, to which several devices are connected. These devices are connected to the network both wired and wirelessly.

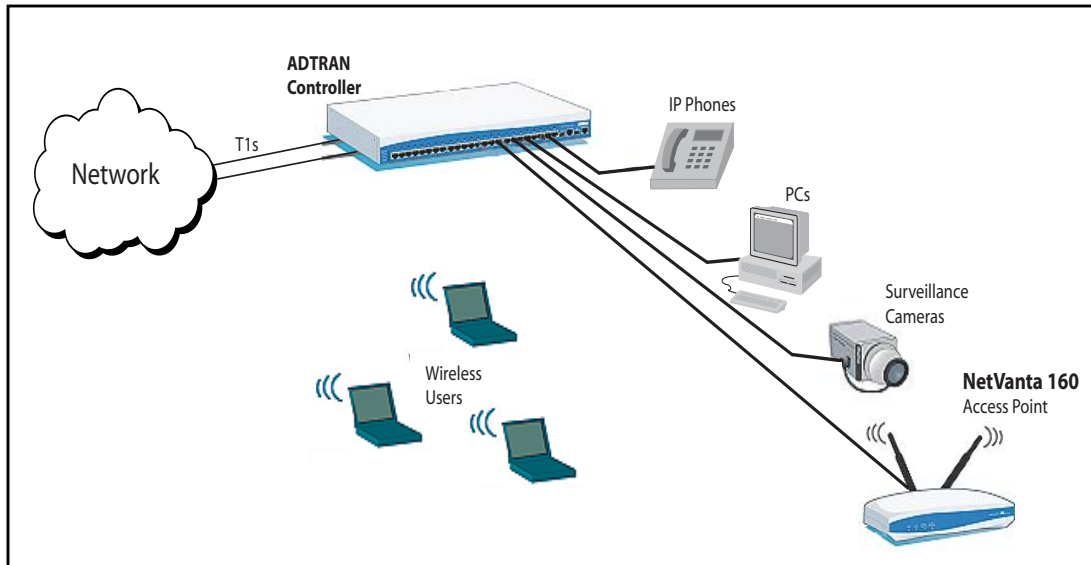


Figure 36. Small-Medium Business Company Model

Virtual Access Point Model

By using VAPs, which are identified by SSIDs, wireless users can be separated into VLANs. This allows separation between divisions of a company (for example, marketing, engineering, and accounting) on both the wired and wireless LANs.

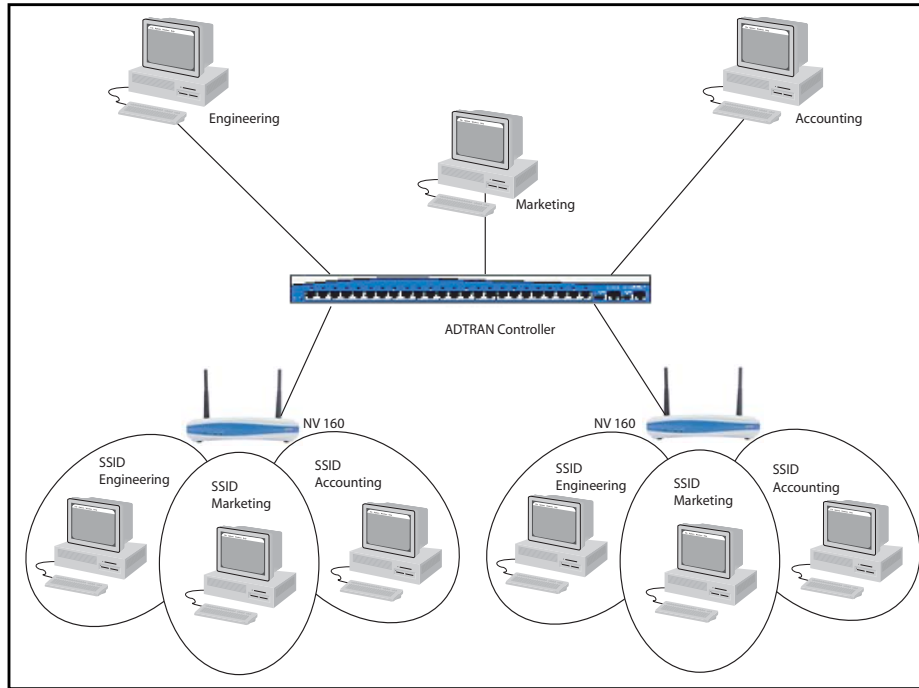


Figure 37. Virtual Access Point Model

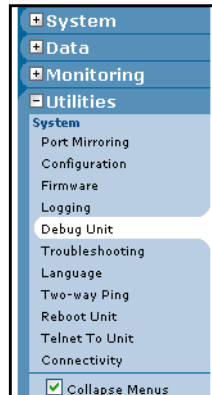
Troubleshooting

Debug statistics and general statistics for each AP, radio, and VAP are available through the GUI. These statistics aid in verifying configuration and troubleshooting.

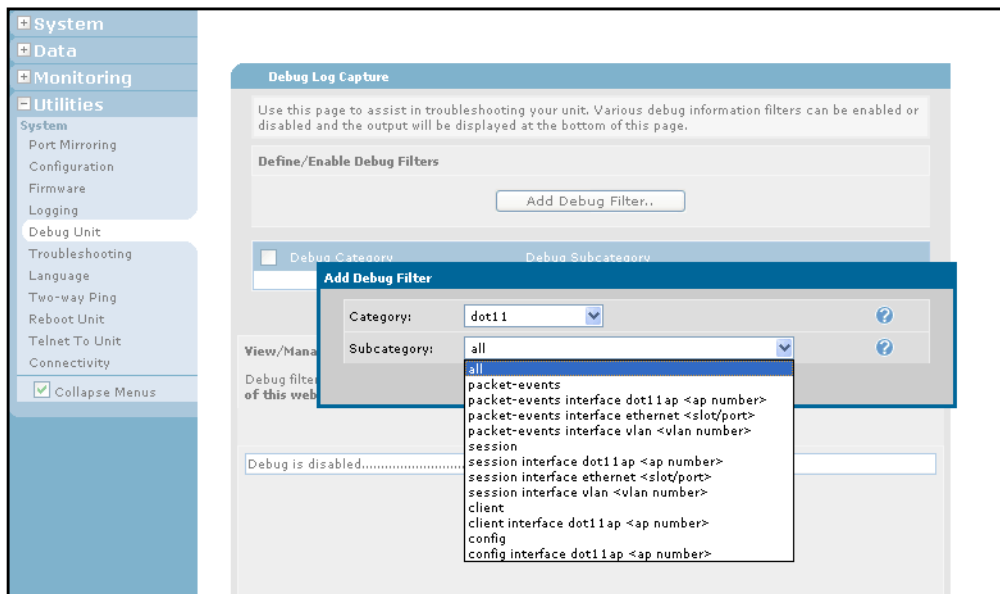
Using Debug Messaging

To access GUI debug messaging abilities, follow these steps:

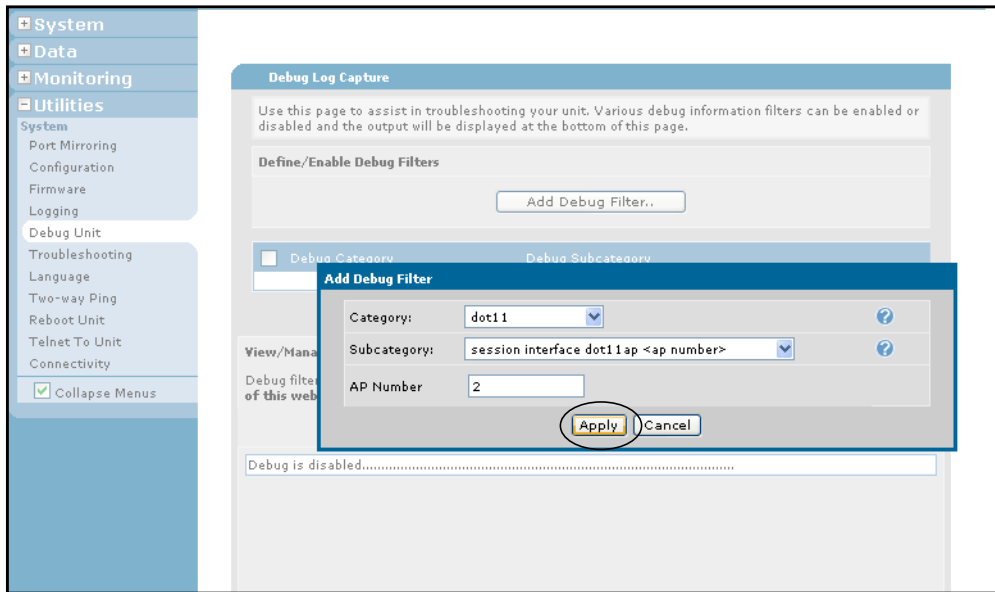
1. Navigate to **Utilities > Debug Unit**.



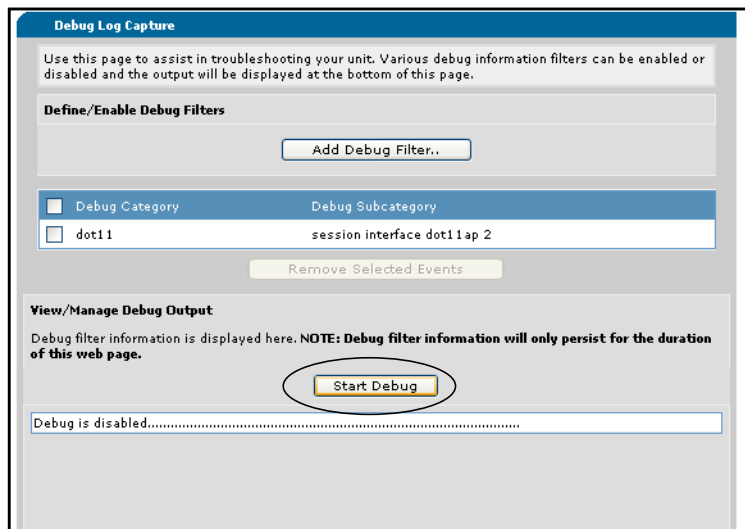
2. Select **Add Debug Filter** and choose the desired item to debug from the **Category** drop-down menu. Select the appropriate entries from the **Subcategory** menu if necessary.



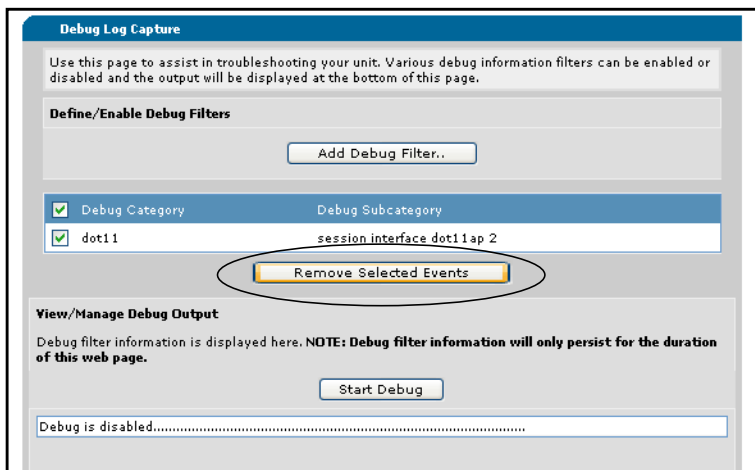
3. Select **Apply** when the correct items are chosen.



4. The item you have selected will appear in the **Debug Category** list in the middle of the menu. To start receiving debug information, select the **Start Debug** tab.



- To remove a debug filter, check the box next to the filter to remove and select **Remove Selected Events**.



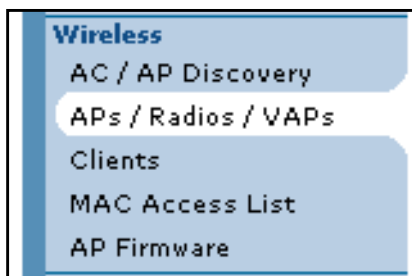
NOTE *Enabling debug messaging can be very processor intensive. Use debug messaging with caution.*

NOTE *Debug messages are generated on the AC, so you do not need to apply any configuration to the AP when enabling or disabling debug messaging.*

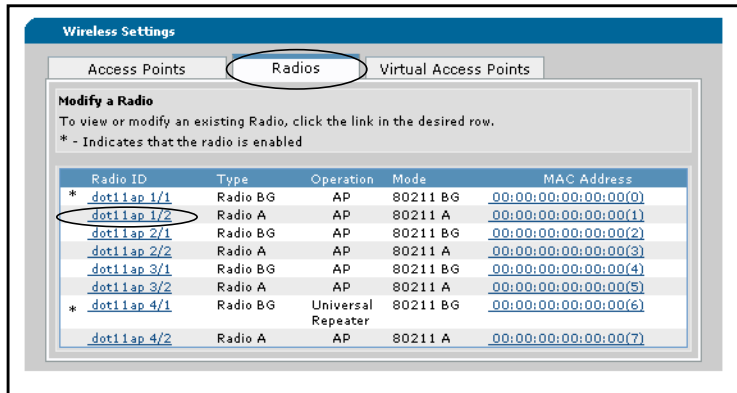
Viewing Unit Statistics

To view statistics for an AP, radio, or VAP, follow these steps:

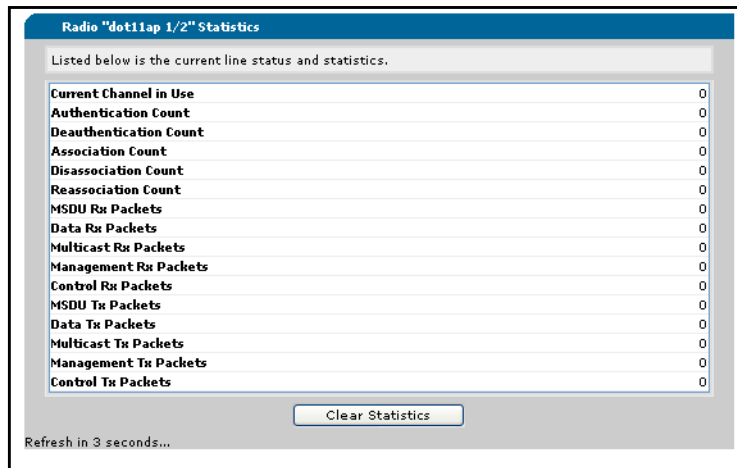
- Select **Data > Wireless > APs/Radios/VAPs**.



2. Select the appropriate tab (**Access Points**, **Radios**, or **Virtual Access Points**) and select the appropriate interface using its hyperlink.



3. Scroll to the bottom of the menu for statistics of the selected interface.



4. To clear statistics, select the **Clear Statistics** button.

CLI Configuration Example

The NetVanta 160 Series wireless APs, radios, and VAPs can also be configured using the CLI. The following is a configuration example, that outlines the various wireless commands used to configure the NetVanta 160 Series. This configuration is provided for example purposes only. For more information about the commands used to configure the NetVanta 160 Series, refer to the *AOS Command Reference Guide*, available online at <https://supportforums.adtran.com>.

```
interface dot11ap 1 ap-type nv16x
  access-point mac-address 00:19:92:08:93:90
  name 160-9444
  ip address 10.10.10.1 255.255.255.0
  ip default-gateway 10.10.10.2
!
!
interface dot11ap 1/1 radio-type 802.11bg
  no shutdown
!
!
interface dot11ap 1/1.1
  ssid broadcast-mode "160bg"
  security mode wpa tkip aes-ccmp psk bluesocket
  no shutdown
!
!
interface dot11ap 1/2 radio-type 802.11a
  radio-mode a
  shutdown
!
!
interface dot11ap 1/2.1
  security mode none
  shutdown
!
end
!
dot11ap apply-changes all
```



*Any settings configured or changed on the NetVanta 160 Series must be applied twice: once to the AC controlling the AP and once to the AP itself. To apply the changes using the CLI, enter the **dot11ap apply-changes** [*<ap number>* | **all**] command from the Enable mode. You will need to exit the Global Configuration mode to apply the changes to the AP.*

Appendix A: Supported Country-Region Radio Channels

The following table outlines the supported radios and channels for all listed countries on the NetVanta 160 Series APs. In addition, the table gives the country code for each country and states whether the country is certified.

Table A-1: Country-Region Radio Channel Support Matrix

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
Albania	8	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Algeria	12	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Argentina	32	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	56, 60, 64, 149, 153, 157, 161	
Armenia	51	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Australia	36	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	Yes
Austria	40	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Azerbaijan	31	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Bahrain	48	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Belarus	112	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Belgium	56	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Belize	84	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Bolivia	68	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
Brazil	76	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Brunei Darussalam	96	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Bulgaria	100	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Canada	124	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 149, 153, 157, 161	Yes
Chile	152	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
China	156	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Colombia	170	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Costa Rica	188	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Croatia	191	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Cyprus	196	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Czech Republic	203	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Denmark	208	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Dominican Republic	214	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
Ecuador	218	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Egypt	818	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
El Salvador	222	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Estonia	233	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Finland	246	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
France	250	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Georgia	268	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Germany	276	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Greece	300	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Guatemala	320	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Honduras	340	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Hong Kong	344	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Hungary	348	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Iceland	352	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
India	356	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Indonesia	360	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Iran	364	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Ireland	372	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Israel	376	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Italy	380	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Jamaica	388	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Jordan	400	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Korea Republic	410	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Kuwait	414	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Latvia	428	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Lebanon	422	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Liechtenstein	438	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Lithuania	440	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Luxembourg	442	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
Macau	446	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Macedonia	807	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Malaysia	458	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	52, 56, 60, 64, 149, 153, 157, 161	
Malta	470	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Mexico	484	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	Yes
Monaco	492	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Morocco	504	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Netherlands	528	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
New Zealand	554	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	Yes
North Korea	408	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Norway	578	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Oman	512	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Pakistan	586	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
Panama	591	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Peru	604	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Philippines	608	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Poland	616	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Portugal	620	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Puerto Rico	630	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	
Qatar	634	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Romania	642	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		Yes
Russia	643	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Russia (2.4 GHz)	1643	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Saudi Arabia	682	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Serbia & Montenegro	891	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Singapore	702	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	Yes
Slovak Republic	703	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Slovenia	705	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
South Africa	710	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	
Spain	724	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Sweden	752	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Switzerland	756	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
Syria	760	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Taiwan	158	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	56, 60, 64, 149, 153, 157, 161	Yes
Thailand	764	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Trinidad & Tobago	780	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Tunisia	788	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Turkey	792	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	
Ukraine	804	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
United Arab Emirates	784	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
United Kingdom	826	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48	Yes
United States	840	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	36, 40, 44, 48, 149, 153, 157, 161	Yes
Uruguay	858	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Uzbekistan	860	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	36, 40, 44, 48, 149, 153, 157, 161	

Table A-1: Country-Region Radio Channel Support Matrix (Continued)

Country Name	Country Code	802.11b/g Supported Channels	802.11a Supported Channels	Certified
Venezuela	862	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	149, 153, 157, 161	
Viet Nam	704	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Yemen	887	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		
Zimbabwe	716	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		

Appendix B. Creating MAC ACLs Using the GUI and CLI

MAC ACLs allow tighter security in wireless networks by blocking unwanted computer or device connections. The MAC ACL is a common filtering option, based on source MAC addresses, that only allows specified devices to access the network. MAC ACLs are applicable to the NetVanta 160 Series Wireless Access Point and any unit acting as an access controller. A MAC ACL can be created by entering the MAC address for each computer or device that you want to allow access through either the CLI or GUI. The CLI provides direct interaction with your unit through a text-based user interface, and the GUI provides direct interaction with your unit through a Web-based user interface.



MAC ACLs are used as packet selectors by the wireless features. By themselves, the MAC ACLs do nothing. AOS provides only standard MAC ACLs, that match based on the source of the packet.

Creating a MAC ACL Using the GUI

To create a MAC ACL using the GUI, follow these steps:



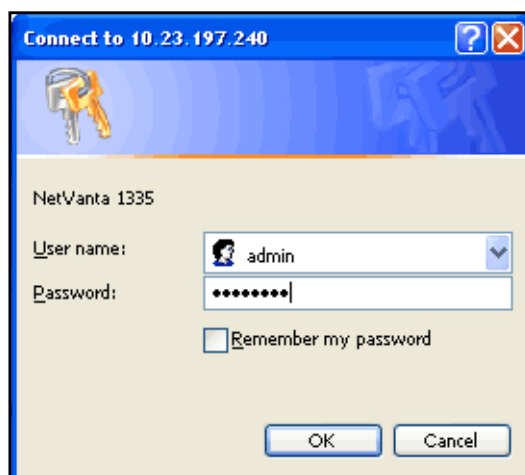
If restrictions in your network prevent you from accessing the GUI, proceed to [Creating a MAC ACL Using the CLI on page 55](#).

1. Open a new page in your Web browser.
2. Type your unit's IP address in the browser's address field in the **http://<ip address>** format.

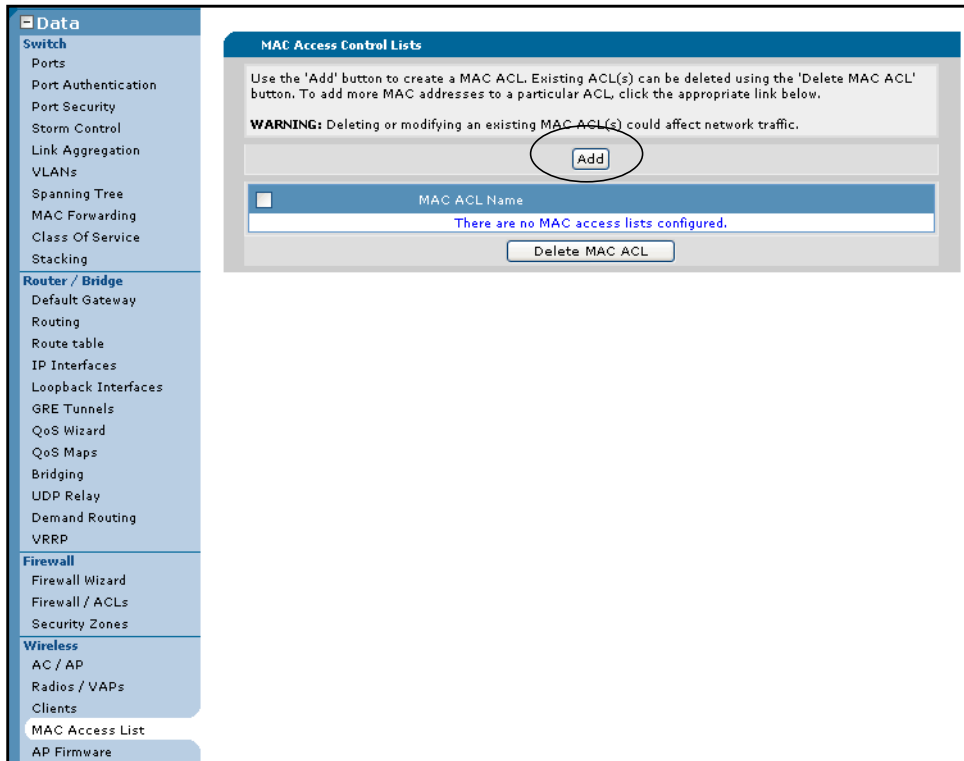


*The IP address may also be entered in **https://** if your unit has **ip http secure-server** enabled.*

3. At the prompt, enter your user name and password and select **OK**.



4. Navigate to **Data > Wireless > MAC Access List** on the left of the GUI menu as seen below:



5. Select **Add** to add a MAC ACL.

- Enter the **MAC ACL Name** and the source **MAC Address** in the appropriate fields.

Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name: *The name to uniquely identify this ACL.*

MAC Address: : : : : : *Set the source Media Access Control address to permit.*

<input type="checkbox"/>	MAC ACL Name	ACL Type	MAC Address
There are no MAC access list configured.			

Enter the **MAC ACL Name**.

Enter the **MAC Address**.

NOTE *MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, 00:A0:C8:00:00:01).*

- Select **Apply** to create the MAC ACL.

Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name: *The name to uniquely identify this ACL.*

MAC Address: : : : : : *Set the source Media Access Control address to permit.*

<input type="checkbox"/>	MAC ACL Name	ACL Type	MAC Address
There are no MAC access list configured.			

- The new MAC ACL will appear on the bottom portion of the menu.

Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name: *The name to uniquely identify this ACL.*

MAC Address: : : : : : *Set the source Media Access Control address to permit.*

<input type="checkbox"/>	MAC ACL Name	ACL Type	MAC Address
<input type="checkbox"/>	allowadtrn	Permit	00:A0:C8:00:00:01

- To add additional source MAC addresses to the MAC ACL, select the MAC ACL name hyperlink from the bottom of the menu. Enter additional MAC addresses you want to give access to your network and select **Apply**. You can add as many new addresses to the MAC ACL as you need.

Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name: *The name to uniquely identify this ACL.*

MAC Address: : : : : : *Set the source Media Access Control address to permit.*

<input type="checkbox"/>	MAC ACL Name	ACL Type	MAC Address
<input type="checkbox"/>	allowadtrn	Permit	00:A0:C8:00:00:01

- Configuration of the MAC ACL is complete. You can make additional changes to each MAC ACL by selecting its hyperlink.

- To delete an address from a MAC ACL, select the check box next to the MAC address you want to delete and select the **Delete ACL Entry** button at the bottom of the menu.

Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

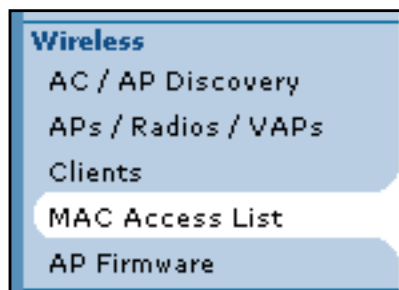
MAC ACL Name: *The name to uniquely identify this ACL.*

MAC Address: : : : : : *Set the source Media Access Control address to permit.*

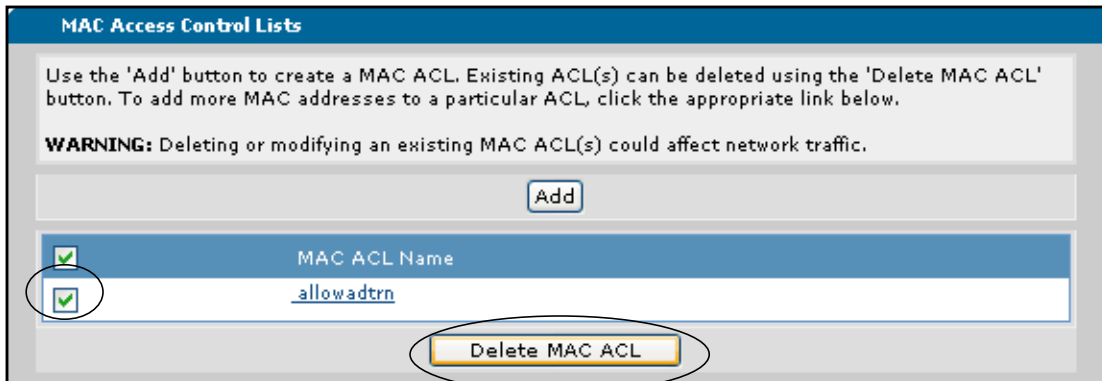
<input type="checkbox"/>	MAC ACL Name	ACL Type	MAC Address
<input type="checkbox"/>	allowadtrn	Permit	00:A0:C8:00:00:01
<input checked="" type="checkbox"/>	allowadtrn	Permit	00:A0:C8:00:00:02

NOTE *Deleting MAC ACL entries will only delete the selected MAC address entries in the ACL, not the MAC ACL itself.*

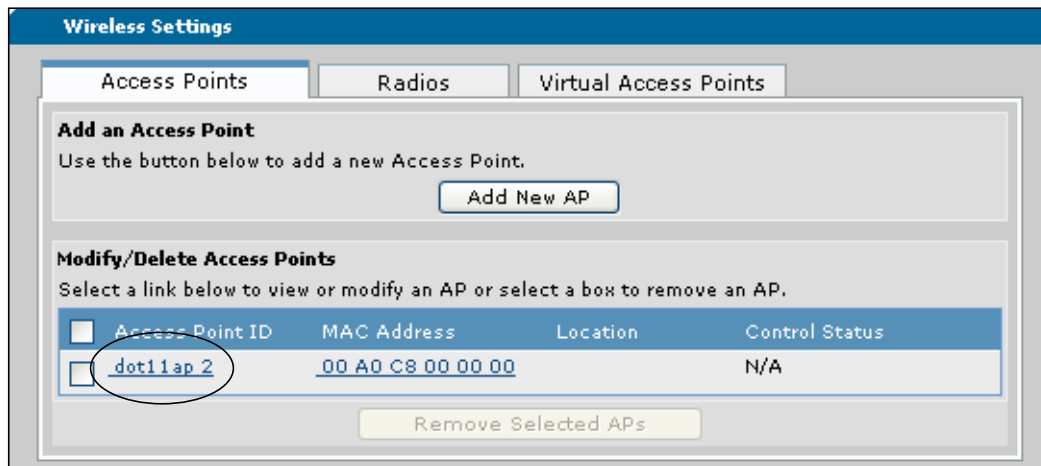
- To delete an entire MAC ACL, return to the main MAC ACL menu by selecting **MAC Access List** from the menu on the left.



13. Check the box next to the MAC ACL you want to delete, and select **Delete MAC ACL**.



14. Once the MAC ACL is configured, it must be applied to the radio. To apply the ACL to the radio, navigate to **Wireless > APs/Radios/VAPs** and select the access point ID from the list.



15. After selecting the appropriate AP ID, select the MAC ACL you want to apply to the radio from the **MAC Access List** drop-down menu.

The screenshot shows the 'Access Point Configuration' window. The 'MAC Access List' dropdown menu is open, displaying 'None' and 'allowadtran'. The 'None' option is highlighted. Other fields include 'Access Point Interface: 2', 'Name: AP2', 'Location: ', 'MAC Address: 00 : A0 : C8 : 00 : 00 : 00', 'Speed/Duplex: AUTO', and 'Country/Region: United States'.

16. After selecting the MAC ACL, apply it to the radio using the **Apply** button at the bottom of the menu. The ACL is applied to the radio once the changes are applied to the AP (refer to [Applying the Settings on page 20](#)).
17. You can save your configuration (recommended) and exit the GUI using the **Save** and **Logout** links (at the upper right corner of your current menu).

Creating a MAC ACL Using the CLI

To create a MAC ACL through the CLI, follow these steps:

1. Boot up the unit.
2. Telnet to the unit using the format **telnet <ip address>**, for example: **telnet 208.61.209.1**
3. Enter your user name and password at the prompt.



*The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the > prompt as follows:
>enable
5. Enter your Enable mode password at the prompt.

6. Enter the Global Configuration mode by entering the following command at the # prompt:

```
#configure terminal
```

7. From the Global Configuration mode prompt, enter the **mac access-list standard** command followed by the MAC ACL name. In the following example, a MAC ACL name **Allowadtrn** will be created.

```
(config)#mac access-list standard Allowadtrn  
(config-std-mac-acl)#
```

8. You have now entered the Standard MAC Access List Configuration mode. Here you can enter the MAC addresses to be included in the MAC ACL that will allow other devices to connect to your network. To give access to a specific MAC address, enter the **permit** command followed by the MAC address. Enter addresses in the following format: **xx:xx:xx:xx:xx:xx**. For example:

```
(config-std-mac-acl)# permit 00:A0:C8:00:00:01  
(config-std-mac-acl)#
```

Enter each address to add to the specified MAC ACL. Address entries can be removed from the list by using the **no** parameter in the following manner:

```
(config-std-mac-acl)#no permit 00:A0:C8:00:00:01
```

To exit the Standard MAC Access List Configuration mode, enter the **exit** keyword at the prompt. For example:

```
(config-std-mac-acl)#exit  
(config)#
```

From the Global Configuration mode, entire MAC ACLs can be deleted by using the **no** parameter of the **mac access-list standard** command followed by the MAC ACL name, for example:

```
(config)#no mac access-list standard Allowadtrn
```

9. Once the MAC ACL has been created, you should save the configuration by entering **do write** from the Global Configuration mode prompt. Multiple MAC ACLs can be created by using the same process, either through the GUI or CLI.

10. After creating and saving the MAC ACL, it must be applied to the radio. To apply the ACL, use the **association access-list <name>** command from the radio interface configuration mode (reached by using the **interface dot11ap** command). Then, apply the changes to the AP using the **dot11ap apply-changes <ap number>** command. For example:

```
(config)#interface dot11ap 1 ap-type nv160  
(config)#association access-list Allowadtrn  
(config)#exit  
#dot11ap apply-changes 1
```

11. Save your configuration using the **do write memory** command from the Global Configuration mode prompt as follows:

```
(config)#do write memory
```

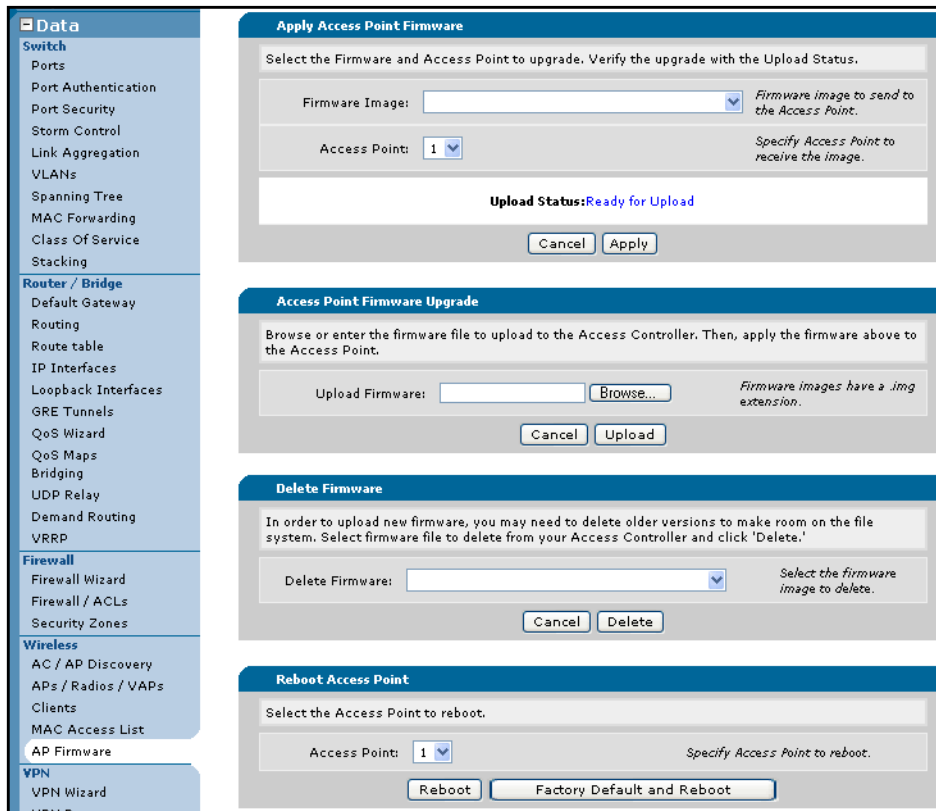

Troubleshooting Note

If unwanted clients or devices have connected to the wireless AP radio before the MAC ACL has been applied, the AP radio must be rebooted for the applied MAC ACL to filter out the unwanted client. To reboot the AP, follow the steps outlined in the following sections.

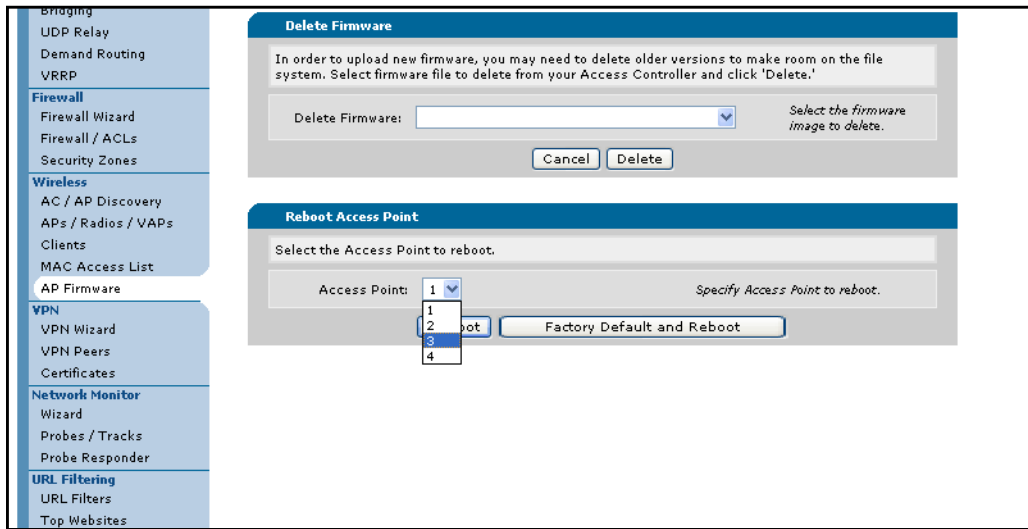
Rebooting the AP Using the GUI

To reboot the AP radio using the GUI, follow these steps:

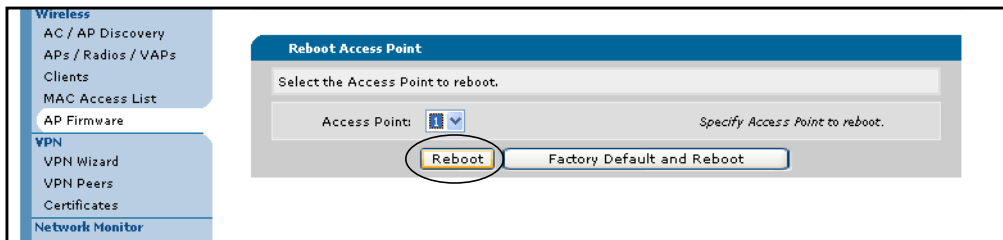
1. Navigate to **Data > Wireless > AP Firmware** in the menu on the left.



2. Select the **Access Point** number to reboot from the drop-down menu.



3. Select the **Reboot** button. The unit will take approximately 60 seconds to reboot, so traffic will be disrupted during this period.



Rebooting the AP Using the CLI

To reboot the AP using the CLI, use the following steps:

1. To reboot the unit while saving the current configuration, enter the following command from the Enable prompt:

```
#reload dot11 interface dot11ap <number>
```

The *<number>* parameter is used to specify the AP to reboot.