— For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart).

— For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.

— For 152-bit encryption, an encryption key is 32 hexadecimal characters or 16 ASCII characters.

- Encryption Transmit Key: select Key 0, Key 1, Key 2, or Key 3

  NOTE: When VLAN tagging is enabled, only Key 0 can be configured.

- **802.1x Station**:
  - Authentication Mode: 802.1x
  - Cipher: WEP
  - Encryption Key Length: 64 or 128 Bits.
    — If 802.1x is enabled simultaneously with WEP, the 802.1x Station's encryption key length is determined by the WEP encryption key.

- **WPA Station**:
  - Authentication Mode: 802.1x
  - Cipher: TKIP

- **WPA-PSK Station**:
  - Authentication Mode: PSK
  - Cipher: TKIP
  - PSK Passphrase: an 8-63 character user-defined phrase. It is recommended a passphrase of at least 13 characters, including both letters and numbers, and upper and lower case characters, be used to ensure that the generated key cannot be easily deciphered by network infiltrators.

- **802.11i Station**:
  - Authentication Mode: 802.1x
  - Cipher: CCMP based on AES

- **802.11i-PSK Station**:
  - Authentication Mode: PSK
  - Cipher: CCMP based on AES
  - PSK Passphrase: an 8-63 character user-defined phrase. It is recommended a passphrase of at least 13 characters, including both letters and numbers, and upper and lower case characters, to ensure that the generated key cannot be easily deciphered by network infiltrators.

5. When finished configuring all parameters, click **OK**.

6. If you selected a Security Mode of 802.1x Station, WPA Station, or 802.11i Station, you must configure a RADIUS 802.1x/EAP server. See the Configuring Radius Profiles section.

   Security Profile 1 will be used by default for all wireless interfaces.

7. Reboot the AP.

Figure 4-49 Security Profile Table - Add Entries

MAC Access

The MAC Access sub-tab allows you to build a list of stations, identified by their MAC addresses, authorized to access the network through the AP. The list is stored inside each AP within your network. Note that you must reboot the AP for any changes to the MAC Access Control Table to take effect. Up to 1000 entries can be made in the table.

The "MAC ACL Status" parameter (configurable on the **SSID/VLAN/Security** > **Wireless** sub-tab) is per VLAN if VLAN Management is enabled. All other parameters besides "MAC ACL Status" are configured per AP, even if VLAN is enabled.

The following list details the configurable MAC Access parameters.

NOTE: *MAC Access Control status is controlled on the **SSID/VLAN/Security > Wireless** sub-tab. When set to Strict, changes to the MAC ACL table will take effect immediately, without a unit reboot. When not set to Strict, changes will not take effect until the unit is rebooted.*

• **Operation Type:** Choose between **Passthru** and **Block**. This determines how the stations identified in the MAC Access Control Table are filtered.

  – If set to **Passthru**, only the addresses listed in the Control Table will pass through the bridge.

  – If set to **Block**, the bridge will block traffic to or from the addresses listed in the Control Table.

• **MAC Access Control Table:** Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:

  – **MAC Address:** Enter the wireless client's MAC address.

  – **Comment:** Enter an optional comment such as the client's name.

  – **Status:** The entry is enabled automatically when saved (so the Status field is only visible when editing an entry). You can also disable or delete entries by changing this field's value.

NOTE: *For larger networks that include multiple Access Points, you may prefer to maintain this list on a centralized location using the MAC Access Control Via RADIUS Authentication.*


Figure 4-50 MAC Access Configuration Screen

Wireless

Each SSID can have its own Security Profile that defines its security mode, authentication mechanism, and encryption, so that customers can have multiple types of clients (non-WEP, WEP, 802.1x, WPA, WPA-PSK, 802.11i, 802.11i-PSK) on the same system separated per VLAN. See the Security Profile section for more information. Each SSID can support a unique VLAN. In order for the AP to support multiple SSID/VLANs, VLAN Tagging must be enabled. These parameters are configurable on the **Wireless** screens.

Configuring an SSID/VLAN with VLAN Tagging Disabled

With VLAN tagging disabled (from the **SSID/VLAN/Security** > **Mgmt VLAN** tab), only one SSID can be configured. All parameters set on the Wireless tab will be applied to that SSID.

1. Click **SSID/VLAN/Security** > **Wireless**.

   The **SSID, VLAN, and Security Configuration** page is displayed.


Figure 4-51 SSID, VLAN, and Security Configuration (VLAN Tagging Disabled)

2. Enable or disable RADIUS accounting on the VLAN/SSID by selecting **Enable** or **Disable** from the **Accounting Status** drop-down menu.
3. Control the functionality of RADIUS MAC Authentication on the VLAN/SSID by selecting one of the following from the the **RADIUS Authentication Status** drop-down menu.

- **Enable**: MAC addresses in the MAC Access Control List stored on the RADIUS server are blocked or allowed, based on the MAC ACL settings. If a higher priority authentication protocol is also enabled, the higher-priority settings will override the MAC ACL settings. See Authentication Protocol Hierarchy.
- **Disable**: RADIUS MAC ACL settings are disabled.
- **Strict**: RADIUS MAC ACL settings are enabled. If a higher-priority authentication protocol is also enabled, RADIUS MAC ACL settings will be applied in addition to the higher priority authentication protocol settings. See Authentication Protocol Hierarchy.

4. Control the functionality of the MAC Access Control List on the VLAN/SSID by selecting one of the following from the **MAC ACL Status** drop-down menu:
   - **Enable**: MAC addresses in the MAC Access Control List are blocked or allowed, based on the MAC ACL settings. If a higher priority authentication protocol is also enabled, the higher-priority settings will override the MAC ACL settings. See Authentication Protocol Hierarchy.
   - **Disable**: MAC ACL settings are disabled.
   - **Strict**: MAC ACL settings are enabled. If a higher-priority authentication protocol is also enabled, MAC ACL settings will be applied in addition to the higher priority authentication protocol settings. See Authentication Protocol Hierarchy. When MAC ACL Status is set to Strict, changes to the MAC ACL table (configured on the MAC Access page) will take effect without a device reboot.

5. Enter **Rekeying Interval** in seconds (between 300 and 65525). When set to 0, this parameter is disabled. The default is 900 seconds.

6. Enter the **Security Profile** used by the VLAN in the Security Profile field. See the Security Profile section for more information.

7. Define the **RADIUS Server Profile Configuration** for the VLAN/SSID:
   - RADIUS MAC Authentication Profile
   - RADIUS EAP Authentication Profile
   - RADIUS Accounting Profile

     If 802.1x, WPA, or 802.11i security mode is used, the RADIUS EAP Authentication Profile must have a value.

     A RADIUS Server Profile for authentication for each VLAN shall be configured as part of the configuration options for that VLAN. RADIUS profiles are independent of VLANs. The user can define any profile to be the default and associate all VLANs to that profile. Four profiles are created by default, "MAC Authentication", "EAP Authentication", Accounting", and "Management"

8. If desired, scroll down to the scroll down to the **SSID and VLAN Table** and click **Edit** to modify the Network Name, VLAN ID, or QoS profile of the SSID/VLAN.

   NOTE: Because VLAN tagging is disabled, attempting to add a new SSID/VLAN will produce an error message.

   The **Edit Entries** screen will be displayed. See Figure 4-52.

Figure 4-52 SSID/VLAN Edit Entries Screen (VLAN Tagging Disabled)

9. Enter a unique **Network Name** (SSID) between 1 and 32 characters. This parameter is mandatory.

    NOTE: Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.

10. Enter a unique **VLAN ID**. This parameter is mandatory.

    *   A VLAN ID is a number from -1 to 4094. A value of -1 means that an entry is "untagged."
    *   You can set the VLAN ID to "-1" or "untagged" if you do not want clients that are using a specific SSID to be members of a VLAN workgroup.
    *   The VLAN ID must match an ID used by your network; contact your network administrator if you need assistance defining the VLAN IDs.

11. Specify a **QoS profile**. See the Policy section for more information.

12. Select the status of **Closed System** to control whether the SSID is advertised in the beacon and manage the way probe requests are handled, as follows:

    *   **Enable:** The SSID is not advertised in the beacon, and the AP will respond to probe requests with an SSID only if the client has specified the SSID in the probe request. If the client sends a probe request with a null or "ANY" SSID, the AP will not respond.
    *   **Partial:** The SSID is advertised in the beacon, and the AP will not respond to "ANY" SSID requests. The Partial setting reduces network traffic by eliminating the repeated broadcast of SSIDs in probe responses.
    *   **Disable:** The SSID is advertised in the beacon, and the AP will respond with each configured SSID, whether or not an SSID has been specified in the probe request.

13. Enable **Broadcast Unique Beacon** using the drop-down menu. When enabled, Broadcast Unique Beacon allows the broadcast of a up to four unique beacons when the AP is configured for multiple SSIDs. If **Closed System** (above) is set to Partial or Disable, each beacon (up to four) will be broadcast a single SSID. If more than four SSIDs are

configured, then three SSIDs will be broadcast in individual beacons; the fourth and subsequent SSIDs will be combined in one beacon and will not be broadcast. If **Closed System** is set to Enable, the SSID will not be broadcast in the beacon. If Broadcast Unique Beacon is disabled, a combined beacon will be broadcast.

NOTE: Enabling Broadcast Unique Beacon will lower the total throughput of the AP by 2-4%. Enabling Broadcast Unique Beacon simultaneously with Rogue Scan will cause a drift in the beacon interval and the occasional missing of beacons.

14. Set the **802.1p Priority** given to packets tagged with this VLAN ID. Enter a number between 0-7.

15. If editing an entry, enable or disable the parameters on this page by electing Enable or Disable from the **Status** drop-down menu. If adding a new entry, this drop-down menu will not appear.

16. Click **OK** to return to Wireless Security Configuration Screen.

17. Reboot the AP.

Configuring SSID/VLANs with VLAN Tagging Enabled

With VLAN Tagging enabled (from the **SSID/VLAN/Security** > **Mgmt VLAN** tab), multiple SSID/VLANs are supported. Parameters set on the Wireless tab can be enabled per SSID by choosing the **Enable Security per SSID** option.

1. Click **SSID/VLAN/Security** > **Wireless**.

2. Select the **Enable Security Per SSID** option. The screen will update to the following:
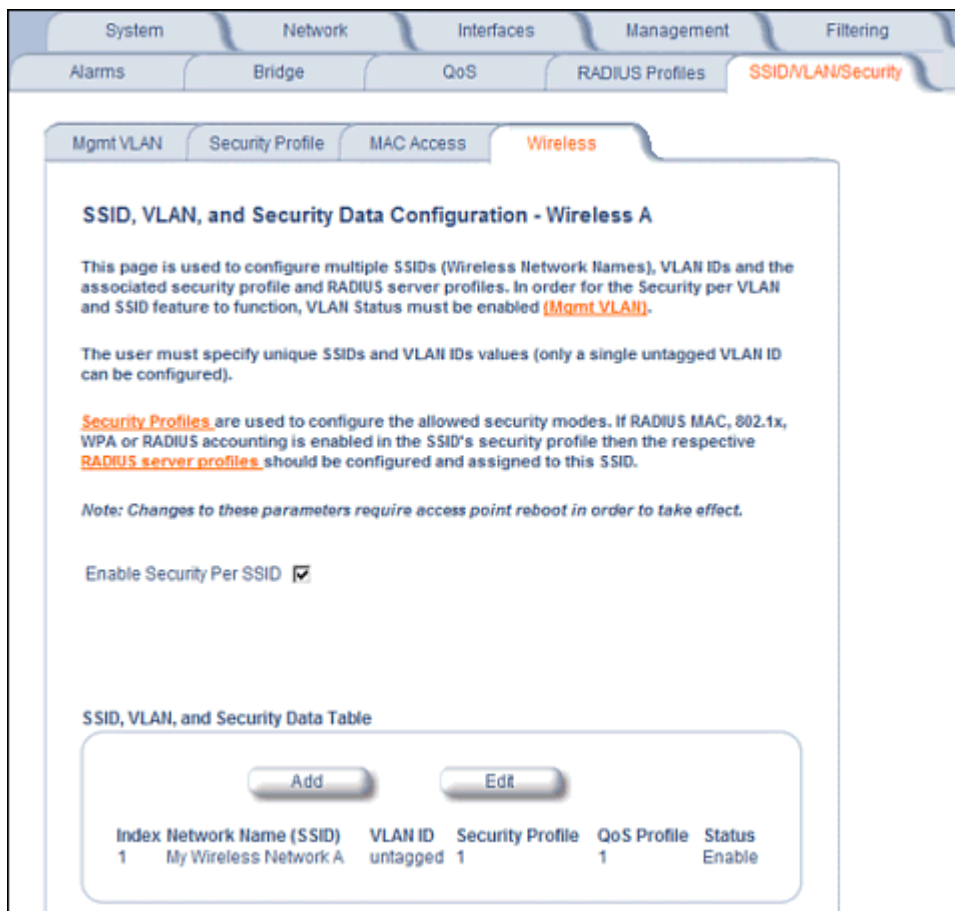
Figure 4-53 SSID/VLAN Configuration (VLAN Tagging Enabled)

*NOTE: If you disable (uncheck) the **Enable Security per SSID** option, you will be able to add multiple SSID/VLANs, but the same configuration parameters (described below) will applied to all of them.*

3. Click **Add** to configure additional SSIDs, VLANs, and their associated security profiles and RADIUS server profiles, or click **Edit** to modify existing SSIDs.

The **Add Entries** or **Edit Entries** screen appears. See Figure 4-54.

Figure 4-54 SSID/VLAN Edit Entries Screen (VLAN Tagging Enabled)

4. Enter a unique **Network Name** (SSID) between 1 and 32 characters. This parameter is mandatory.

   NOTE: Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.

5. Enter a unique **VLAN ID**. This parameter is mandatory.
   - A VLAN ID is a number from -1 to 4094. A value of -1 means that an entry is "untagged."
   - You can set the VLAN ID to "-1" or "untagged" if you do not want clients that are using a specific SSID to be members of a VLAN workgroup. Only one "untagged" VLAN ID is allowed per interface.

- The VLAN ID must match an ID used by your network; contact your network administrator if you need assistance defining the VLAN IDs.

6. Select the status of **Closed System** to control whether the SSID is advertised in the beacon and manage the way probe requests are handled, as follows:

   - **Enable:** The SSID is not advertised in the beacon, and the AP will respond to probe requests with an SSID only if the client has specified the SSID in the probe request. If the client sends a probe request with a null or "ANY" SSID, the AP will not respond.
   - **Partial:** The SSID is advertised in the beacon, and the AP will not respond to "ANY" SSID requests. The Partial setting reduces network traffic by eliminating the repeated broadcast of SSIDs in probe responses.
   - **Disable:** The SSID is advertised in the beacon, and the AP will respond with each configured SSID, whether or not an SSID has been specified in the probe request.

7. Enable **Broadcast Unique Beacon** using the drop-down menu. When enabled, Broadcast Unique Beacon allows the broadcast of a up to four unique beacons when the AP is configured for multiple SSIDs. If **Closed System** (above) is set to Partial or Disable, each beacon (up to four) will be broadcast a single SSID. If more than four SSIDs are configured, then three SSIDs will be broadcast in individual beacons; the fourth and subsequent SSIDs will be combined in one beacon and will not be broadcast. If **Closed System** is set to Enable, the SSID will not be broadcast in the beacon. If Broadcast Unique Beacon is disabled, a combined beacon will be broadcast.

   NOTE: Enabling Broadcast Unique Beacon will lower the throughput of the AP by 2-4%. Enabling Broadcast Unique Beacon simultaneously with Rogue Scan will cause a drift in the beacon interval and the occasional missing of beacons.

8. Enable or disable the **SSID Authorization** status from the drop-down menu. SSID Authorization is the RADIUS-based authorization of the SSID for a particular client. The authorized SSIDs are sent as the tunnel attributes.

9. Enable or disable RADIUS accounting on the VLAN/SSID under the **Accounting Status** drop-down menu.

10. Enable or disable RADIUS MAC authentication status on the VLAN/SSID under the **RADIUS Authentication Status** drop-down menu.

11. Enable or disable MAC Access Control List status on the VLAN/SSID under the **MAC ACL Status** drop-down menu.

12. Enter the **Rekeying Interval** in seconds (between 300 and 65525). When set to 0, this parameter is disabled. The default is 900 seconds.

13. Enter the Security Profile used by the VLAN in the **Security Profile** field.

   NOTE: If you have two or more SSIDs per interface using a Security Profile with a security mode of Non Secure, be aware that security being applied in the VLAN is not being applied in the wireless network.

14. Define the **RADIUS Server Profile Configuration** for the VLAN/SSID:

   - RADIUS MAC Authentication Profile
   - RADIUS EAP Authentication Profile
   - RADIUS Accounting Profile

   If 802.1x, WPA, or 802.11i security mode is used, the RADIUS EAP Authentication Profile must have a value.

   A RADIUS Server Profile for authentication for each VLAN shall be configured as part of the configuration options for that VLAN. RADIUS profiles are independent of VLANs. The user can define any profile to be the default and associate all VLANs to that profile. Four profiles are created by default, "MAC Authentication", "EAP Authentication", Accounting", and "Management".

15. Specify a **QoS Profile**. See the Policy section for more information.

16. Set the **802.1p Priority** given to packets tagged with this VLAN ID. Enter a number between 0-7.

17. If editing an entry, enable or disable the parameters on this page using **Status** drop-down menu. If adding a new entry, this drop-down menu will not appear.

18. Reboot the AP.

Monitoring

5

This chapter discusses the following monitoring options:

- Version: Provides version information for the Access Point's system components.
- ICMP: Displays statistics for Internet Control Message Protocol packets sent and received by the AP.
- IP/ARP Table: Displays the AP's IP Address Resolution table.
- Learn Table: Displays the list of nodes that the AP has learned are on the network.
- IAPP: Provides statistics for the Inter-Access Point Protocol messages sent and received by the AP.
- RADIUS: Provides statistics for the configured RADIUS server(s).
- Interfaces: Displays the Access Point's interface statistics (Wireless and Ethernet).
- Station Statistics: Displays statistics for stations and Wireless Distribution System links.
- Mesh Statistics: Displays statistics for the Mesh portal, including the network topology and the Neighbor Table. This page is not relevant to the AP-700.

To monitor the AP using the HTTP/HTTPS interface, you must first log in to a web browser. See Logging In for instructions.

You may also monitor the AP using the command line interface. See Command Line Interface (CLI) for more information

To monitor the AP via HTTP/HTTPS:

1. Click the **Monitor** button located on the left-hand side of the screen. The main **Monitor** screen will be displayed.
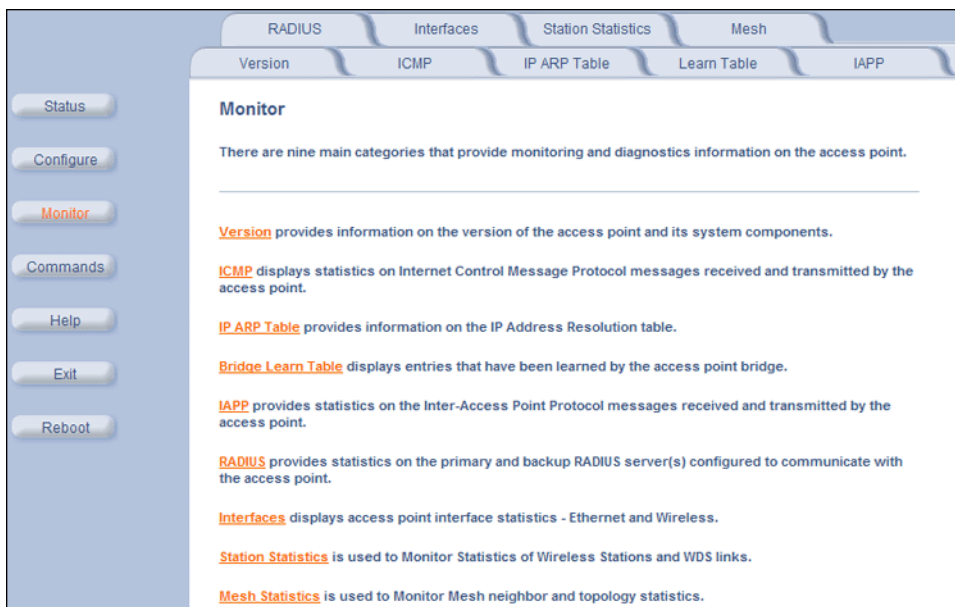
Figure 5-1 Monitor Main Screen

2. Click the tab that corresponds to the statistics you want to review. For example, click **Learn Table** to see the list of nodes that the AP has discovered on the network.
3. If necessary, click the **Refresh** button to update the statistics.

Each **Monitor** tab is described in the remainder of this chapter.

Version

From the HTTP interface, click the **Monitor** button and select the **Version** tab. The list displayed provides you with information that may be pertinent when calling Technical Support. With this information, your Technical Support representative can verify compatibility issues and make sure the latest software are loaded. This screen displays the following information for each Access Point component:

- **Serial Number:** The component's serial number, if applicable.
- **Name/ID:** The AP identifies a system component based on its name or ID. Each component has a unique identifier.
- **Variant:** Several variants may exist of the same component (for example, a hardware component may have two variants, one with more memory than the other).
- **Version:** Specifies the component's version or build number. The Software Image version is the most useful information on this screen for the typical end user.

Figure 5-2 Version Monitoring Tab

ICMP

This tab provides statistical information for both received and transmitted messages directed to the AP. Not all ICMP traffic on the network is counted in the ICMP (Internet Control Message Protocol) statistics.
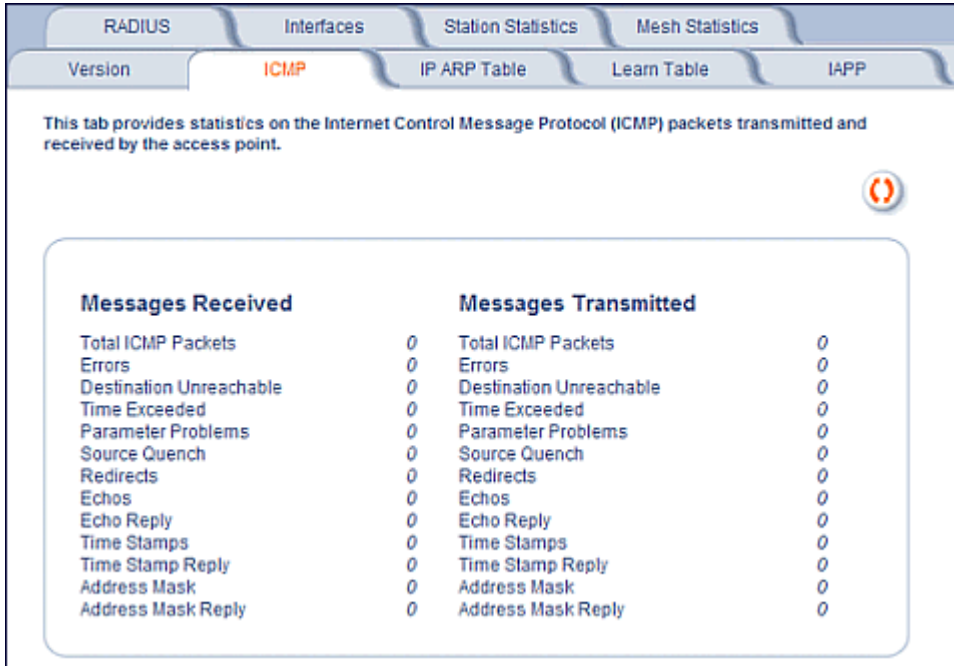
Figure 5-3 ICMP Monitoring Tab

IP/ARP Table

This tab provides information based on the Address Resolution Protocol (ARP), which relates MAC Address and IP Addresses.
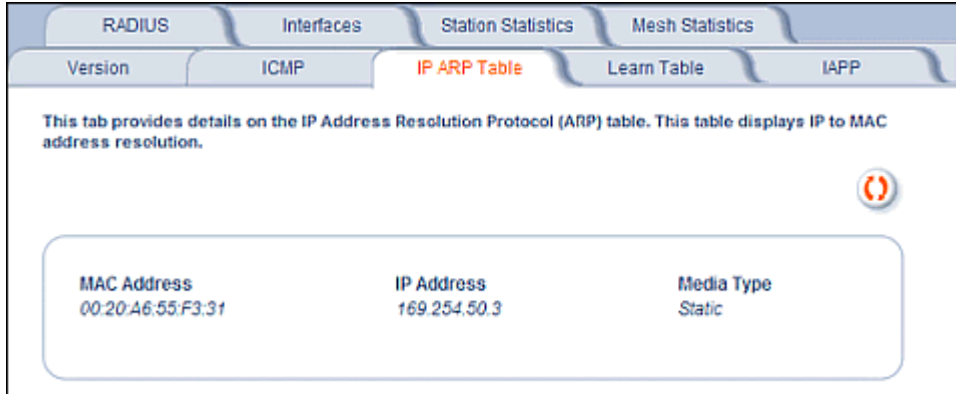
Figure 5-4 IP/ARP Table Monitoring Tab

Learn Table

This tab displays information relating to network bridging. It reports the MAC address for each node that the device has learned is on the network and the interface on which the node was detected. There can be up 10,000 entries in the Learn Table.
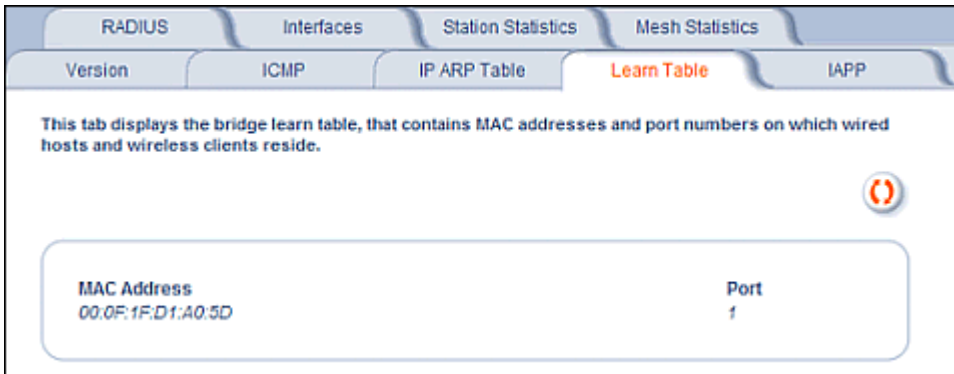
Figure 5-5 Learn Table Monitoring Tab

IAPP

This tab displays statistics relating to client handovers and communications between Access Points.
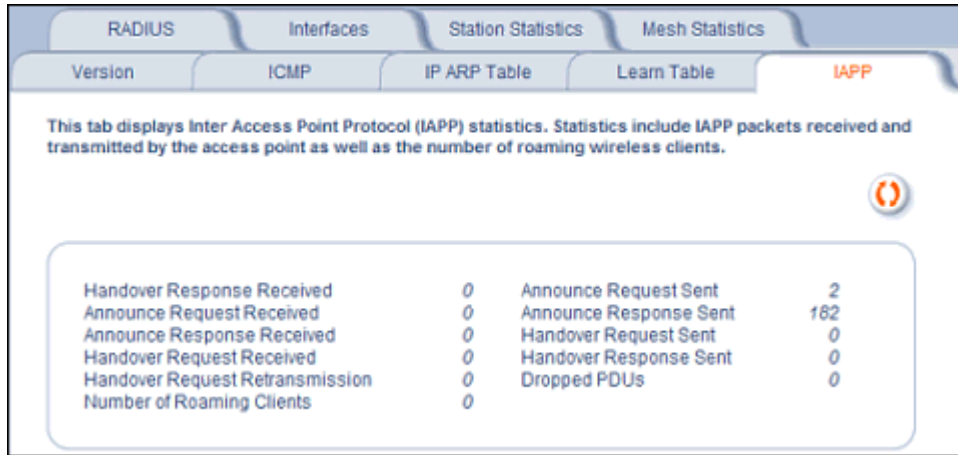
Figure 5-6 IAPP Monitoring Tab

RADIUS

This tab provides RADIUS authentication, EAP/802.1x authentication, and accounting information for both the Primary and Backup RADIUS servers for each RADIUS Server Profile.

NOTE: Separate RADIUS servers can be configured for each RADIUS Server Profile.

Select the RADIUS Server Profile to view statistics on from the **Select Server Profile** drop-down menu.

Figure 5-7 RADIUS Monitoring Tab

Interfaces

This tab displays statistics for the Ethernet and wireless interfaces.

Figure 5-8 Interface Monitoring Tab (Ethernet)

Description of Interface Statistics

The following statistics are displayed for the Ethernet interface only, the wireless interface only, or for both the Ethernet and Wireless interfaces:

- **Admin Status** (*Ethernet/Wireless*): The desired state of the interface: Up (ready to pass packets), Down (not ready to pass packets, or Testing (testing and unable to pass packets).

- **Alignment Error** *(Ethernet)*: The number of frames received that are not an integral number of octets in length and do not pass the Frame Check Sequence check.

- **Carrier Sense Errors** *(Ethernet)*: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame. The count increments at most once per transmission attempt.

- **Deferred Transmission** *(Ethernet)*: The number of frames for which the first transmission attempt is delayed because the medium is busy.This number does not include frames involved in collisions.

- **Description** *(Ethernet/Wireless)*: Information about the interface (e.g., the name of the manufacturer, the product name and the version of the hardware interface).

- **Duplicate Frame Count** *(Wireless)*: The number of duplicate frames received.

- **Ethernet Chipset** *(Ethernet)*: Identifies the chipset used to realize the interface.
- **Excessive Collisions** *(Ethernet)*: The number of frames for which transmission fails due to excessive collisions.
- **Failed ACK Count** *(Wireless)*: The number of times an acknowledgment (or ACK) is not received when expected.
- **Failed Count** *(Wireless)*: The number of packets not transmitted successfully due to too many transmit attempts.
- **Failed RTS Count** *(Wireless*: The number of times a Clear to Send (CTS) is not received in response to a Request to Send (RTS).
- **FCS Error** *(Wireless)*: The number of Frame Check Sequence errors detected in received MAC Protocol Data Units (MPDUs).
- **FCS Errors** *(Ethernet)*: The number of frames received that are an integral number of octets in length but do not pass the Frame Check Sequence check.
- **Frames Too Long** *(Ethernet)*: The number of frames received that exceed the maximum permitted frame size.
- **In Discards** *(Ethernet/Wireless)*: The number of error-free inbound packets that were chosen to be discarded to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- **In Errors** *(Ethernet/Wireless)*: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **In Non-unicast Packets** *(Ethernet/Wireless)*: The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
- **In Octets (bytes)** *(Ethernet/Wireless)*: The total number of octets received on the interface, including framing characters.
- **In Unicast Packets** *(Ethernet/Wireless)*: The number of subnetwork unicast packets delivered to a higher-layer protocol.
- **Internal MAC Receive Errors** *(Ethernet)*: The number of frames for which reception fails due to an internal MAC sublayer transmit error. A frame is only counted if it is not counted by the Frames Too Long, Alignment Error, or FCS Error counters.
- **Internal MAC Transmit Errors** *(Ethernet)*: The number of frames for which transmission fails due to an internal MAC sublayer transmit error. A frame is only counted if it is not counted by Late Collision, Excession Collision, or Carrier Sense Error counters.
- **Last Change** *(Ethernet/Wireless)*: The value of the sysUpTime object at the time the interface entered its current operational state.
- **Late Collisions** *(Ethernet)*: The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet
- **MAC Address** *(Wireless)*: The station's assigned, unique MAC address,
- **Maximum Packet Size** *(Ethernet/Wireless)*: The size (in octets) of the largest datagram which can be sent/received
- **MIB Specific Definition** *(Ethernet/Wireless)*: A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is an Ethernet interface, then this field refers to a document defining objects specific to ethernet.
- **Multicast Received Frame Count** *(Wireless)*: The number of multicast packets received.
- **Multicast Transmitted Frame Count** *(Wireless)*: The number of multicast packets transmitted.
- **Multiple Collision Frames** *(Ethernet)*: The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
- **Multiple Retry Count** *(Wireless)*: The number of packets successfully transmitted after more than one retransmission.
- **Operational Status** *(Ethernet/Wireless)*: The current state of the interface: Up (ready to pass packets), Down (not ready to pass packets, or Testing (testing and unable to pass packets).
- **Out Discards** *(Ethernet/Wireless)*: The number of error-free outbound packets chosen to be discarded to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

- **Out Errors** *(Ethernet/Wireless)*: The number of outbound packets that could not be transmitted because of errors.
- **Out Non-unicast Packets** *(Ethernet/Wireless)*: The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast orsubnetwork-multicast) address, including those that were discarded or not sent.
- **Out Octets (bytes)** *(Ethernet/Wireless)*: The total number of octets transmitted out of the interface, including framing characters.
- **Out Unicast Packets** *(Ethernet/Wireless)*: The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Output Queue Length** *(Ethernet/Wireless)*: The length of the output packet queue (in packets).
- **Physical Address** *(Ethernet):* The interface's address at the protocol layer immediately below the network layer in the protocol stack.
- **Received Fragment Count** *(Wireless)*: The number of successfully received Data or Management MAC Protocol Data Units (MPDUs).
- **Retry Count** *(Wireless)*: The number of packets successfully transmitted after one or more retransmissions.
- **Single Collision Frames** *(Ethernet)*: The number of successfully transmitted frames for which transmission is inhibited by exactly one collision
- **Speed** *(Ethernet/Wireless)*: An estimate of the interface's current bandwidth in bits per second.
- **SQE Test Errors** *(Ethernet)*: The number of times that the Signal Quality Error (SQE) Test Error message is generated by the physical layer signalling (PLS) sublayer.
- **Successful RTS Count** *(Wireless)*: The number of times a Clear to Send (CTS) is received in response to an Request to Send (RTS).
- **Transmitted Fragment Count** *(Wireless)*: The number of transmitted fragmented packets.
- **Transmitted Frame Count** *(Wireless)*: This number of successfully transmitted packets.
- **Type** *(Ethernet/Wireless)*: The type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack.
- **Unknown Protocols** *(Ethernet/Wireless)*: The number of packets received that were discarded because of an unknown or unsupported protocol.
- **WEP Undecryptable Count** *(Wireless)*: The number of undecryptable WEP frames received.

Station Statistics

This tab displays information on wireless clients attached to the AP and on Wireless Distribution System.

Enable the Monitoring Station Statistics feature (Station Statistics are disabled by default) by checking **Enable Monitoring Station Statistics** and click **OK**.

You do not need to reboot the AP for the changes to take effect. If clients are connected to the device or WDS links are configured for the device, the statistics will now be shown on the screen. Click **Select** to view the more detailed statistics for a client.

Click on the **Refresh** button in the browser window to view the latest statistics. If any new clients associate to the AP, you can see the statistics of the new clients after you click the refresh button.
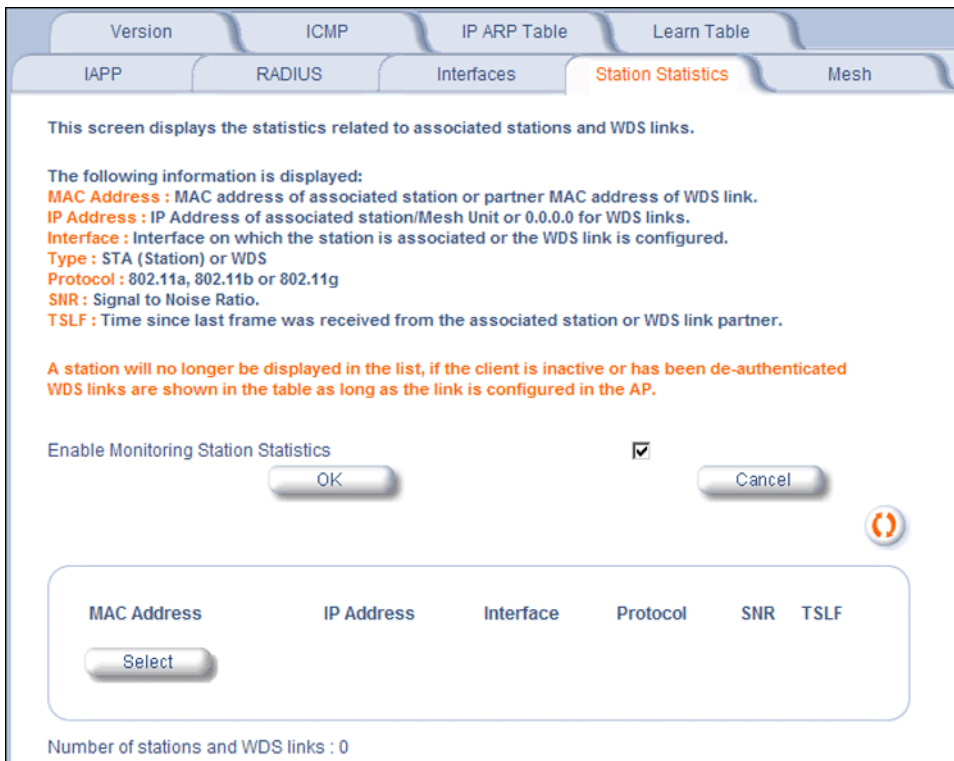
Figure 5-9 Station Statistics Monitoring Tab

Description of Station Statistics

The following stations statistics are displayed:

- **MAC Address**: The MAC address of the wireless client for which the statistics are gathered. For WDS links, this is the partner MAC address of the link.
- **IP Address**: The IP address of the associated wireless station for which the Statistics are gathered. (0.0.0.0 for WDS links)
- **Interface to which the Station is connected**: The interface number on which the client is connected with the AP. For WDS links this is the interface on which the link is configured.
- **MAC Protocol**: The MAC protocol for this wireless client (or WDS link partner). The possible values are 802.11a, 802.11b, 802.11g.
- **Signal / Noise**: The Signal /Noise Level measured at the AP when frames are received from the associated wireless station (or WDS link partner).

- **Time since Last Frame Received**: The time elapsed since the last frame from the associated wireless station (or WDS link partner) was received.
- **Number of Stations and WDS Links**: The number of stations and WDS links monitored.

The following stations statistics are available through SNMP:

- **Octets Received**: The number of octets received from the associated wireless station (or WDS link partner) by the AP.
- **Unicast Frames Received**: The number of Unicast frames received from the associated wireless station (or WDS link partner) by the AP.
- **Non-Unicast Frames Received**: The number of Non-Unicast frames received (i.e. broadcast or multicast) from the associated wireless station (or WDS link partner) by the AP.
- **Octets Transmitted**: The number of octets sent to the associated wireless station (or WDS link partner) from the AP.
- **Unicast Frames Transmitted**: The number of Unicast frames transmitted to the associated wireless station (or WDS link partner) from the AP.

Mesh Statistics

As the AP-700 does not support Mesh functionality, this tab contains no information. Visit www.proxim.com for information on Mesh.
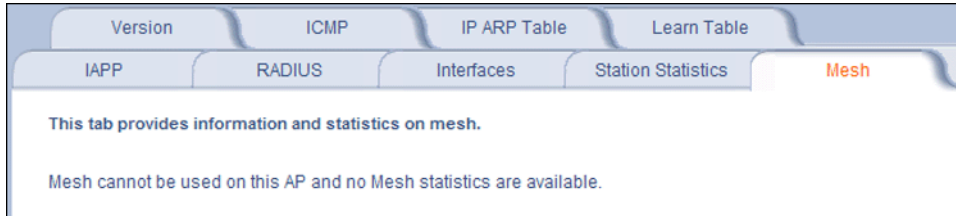
Figure 5-10 Mesh Monitoring Tab

6

Commands

This chapter contains information on the following Command functions:

- Introduction to File Transfer via TFTP or HTTP: Describes the available file transfer methods.
- Update AP: Download files via TFTP or HTTP to the AP.
- Retrieve File: Upload configuration files from the AP to a TFTP server.
- Reboot: Reboot the AP in the specified number of seconds.
- Reset: Reset all of the Access Point's configuration settings to factory defaults.
- Help Link: Configure the location where the AP Help files can be found.

To perform commands using the HTTP/HTTPS interface, you must first log in to a web browser. See Logging In for instructions.

You may also perform commands using the command line interface. See Command Line Interface (CLI) for more information.

To perform commands via HTTP/HTTPS:

1. Click the **Commands** button located on the left-hand side of the screen.

Figure 6-1 Commands Main Screen

2. Click the tab that corresponds to the command you want to issue. For example, click **Reboot** to restart the unit.

Following a brief introduction to TFTP and HTTP file transfer, each **Commands** tab is described in the remainder of this chapter.

Introduction to File Transfer via TFTP or HTTP

There are two methods of transferring files to or from the AP: TFTP or HTTP (or HTTPS if enabled):

- Downloading files (Configuration, AP Image, Bootloader, License, Private Key, Certificate, CLI Batch File) to the AP using one of these two methods is called "Updating the AP."
- Uploading files (Configuration, CLI Batch File, etc) from the AP is called "Retrieving Files."

TFTP File Transfer Guidelines

A TFTP server must be running and configured to point to the directory containing the file.

If you do not have a TFTP server installed on your system, install the TFTP server from the installation CD.

HTTP File Transfer Guidelines

HTTP file transfer can be performed either with or without SSL enabled.

HTTP file transfers with SSL require enabling Secure Management and Secure Socket Layer. HTTP transfers that use SSL may take additional time.

NOTE: SSL requires Internet Explorer version 6, 128 bit encryption, Service Pack 1, and patch Q323308.

Image Error Checking During File Transfer

The Access Point performs checks to verify that an image downloaded through HTTP or TFTP is valid. The following checks are performed on the downloaded image:

- Zero Image size
- Large image size
- Non VxWorks image
- AP image
- Digital signature verification

If any of the above checks fail on the downloaded image, the Access Point deletes the downloaded image and retains the old image. Otherwise, if all checks pass successfully, the AP deletes the old image and retains the downloaded image.

These checks are to ensure that the AP does not enter an invalid image state. The storage of the two images is only temporary to ensure the proper verification; the two images will not be stored in the AP permanently.

Image error checking functions automatically in the background. No user configuration is required.

Update AP

Update AP via TFTP

Use the Update AP via TFTP tab to download Configuration, AP Image, Bootloader files, Certificate and Private Key files, and CLI Batch File to the AP. A TFTP server must be running and configured to point to the directory containing the file.

Figure 6-2 Update AP via TFTP Command Screen

If you do not have a TFTP server installed on your system, install the TFTP server from the installation CD. You can either install the TFTP server from the CD Wizard or run **OEM-TFTP-Server.exe** found in the CD's *Xtras/SolarWinds* sub-directory.

The **Update AP via TFTP** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address:** Enter the TFTP server IP Address.
  - Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server.

    NOTE: This is the IP address that will be used to point the Access Point to the AP Image file.

- **File Name:** Enter the name of the file to be downloaded (including the file extension).
  - Copy the file to the TFTP server's root folder.
- **File Type:** Select the proper file type. Choices include:
  - **Config**: configuration information, such as System Name, Contact Name, and so on.

    NOTE: The AP will reboot automatically when downloading a Config file.

  - **Image**: AP Image (executable program).
  - **Upgrade BspBl**: Bootloader software.
  - **SSL Certificate**: the digital certificate for authentication in SSL communications.
  - **SSL Private Key**: the private key for encryption in SSL communications.
  - **SSH Public Key**: the public key in SSH communications. See Secure Shell (SSH) Settings for more information.
  - **SSH Private Key**: the private key in SSH communications. See Secure Shell (SSH) Settings for more information.

–   **CLI Batch File**: a CLI Batch file that contains CLI commands to configure the AP. This file will be executed by the AP immediately after being uploaded. See CLI Batch File for more information.

•   **File Operation: Select either Update AP or Update AP & Reboot**. You should reboot the AP after downloading files.

Update AP via HTTP

Use the **Update AP via HTTP** tab to download Configuration, AP Image, Bootloader files, and Certificate and Private Key files to the AP.

Once on the Update AP screen, click on the **via HTTP** tab.
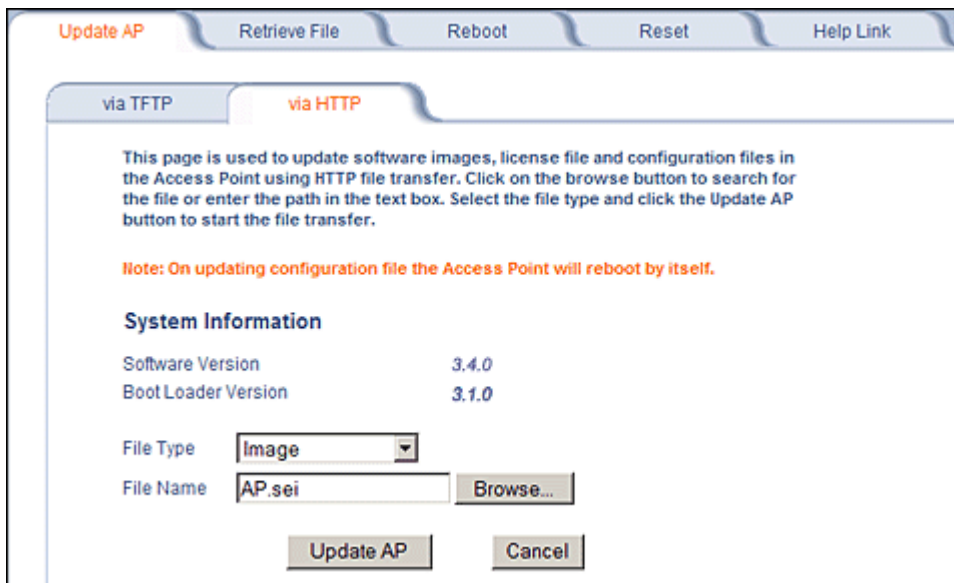
Figure 6-3 Update AP via HTTP Command Screen

The **Update AP via HTTP** tab shows version information and allows you to enter HTTP information as described below.

1. Select the File Type that needs to be updated from the drop-down box. Choices include:
   –   **Image** for the AP Image (executable program).
   –   **Config** for configuration information, such as System Name, Contact Name, and so on.

   NOTE: The AP will reboot automatically when downloading a Config file.

   –   **SSL Certificate**: the digital certificate for authentication in SSL communications.
   –   **SSL Private Key**: the private key for encryption in SSL communications.
   –   **Upgrade BSPBL**: the Bootloader software.
   –   **CLI Batch File**: a CLI Batch file that contains CLI commands to configure the AP. This file will be executed by the AP immediately after being uploaded. See CLI Batch File for more information.
   –   **SSH Public Key**: the public key in SSH communications. See Secure Shell (SSH) Settings for more information.
   –   **SSH Private Key**: the private key in SSH communications. See Secure Shell (SSH) Settings for more information.
2. Use the **Browse** button or manually type in the name of the file to be downloaded (including the file extension) in the File Name field. If typing the file name, you must include the full path and the file extension in the file name text box.
3. To initiate the HTTP Update operation, click the **Update AP** button.

   A warning message gets displayed that advises the user that a reboot of the device will be required for changes to take effect.
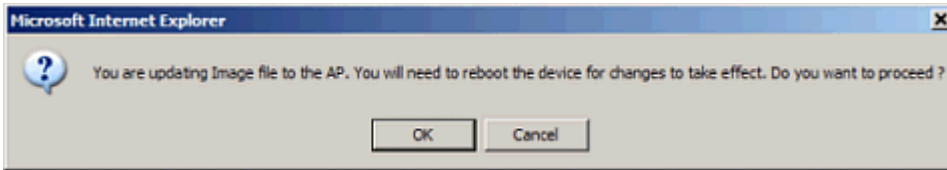
Figure 6-4 Warning Message

4. Click **OK** to continue with the operation or Cancel to abort the operation.

   NOTE: An HTTP file transfer using SSL may take extra time.

   If the operation completes successfully the following screen appears.
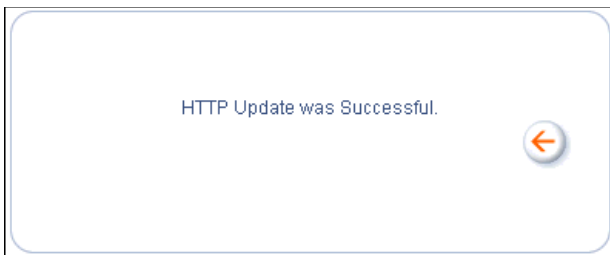
Figure 6-5 Update AP Successful

If the operation did not complete successfully the following screen appears, and the reason for the failure is displayed.

Figure 6-6 Update AP Unsuccessful

Retrieve File

Retrieve File via TFTP

Use the **Retrieve File via TFTP** tab to upload files from the AP to the TFTP server. The TFTP server must be running and configured to point to the directory to which you want to copy the uploaded file. We suggest you assign the file a meaningful name, which may include version or location information.

If you don't have a TFTP server installed on your system, install the TFTP server from the installation CD. You can either install the TFTP server from the CD Wizard or run **OEM-TFTP-Server.exe** found in the CD's *Xtras/SolarWinds* sub-directory.

The **Retrieve AP via TFTP** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address:** Enter the TFTP server IP Address.
  – Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server.
- **File Name:** Enter the name of the file to be uploaded.
- **File Type**: Select the type of file to be uploaded: Config file, CLI Batch File, or CLI Batch (Error) Log.

Use the following procedure to retrieve a file from an AP to a TFTP server:

1. If retrieving a Config file, configure all the required parameters in their respective tabs. Reboot the device.
2. Retrieve and store the file. Click the **Retrieve File** button to initiate the upload of the file from the AP to the TFTP server.
3. If you retrieved a Configuration file, update the file as necessary.
4. If you retrieved a CLI Batch File or CLI Batch Log, you can examine the file using a standard text editor. For more information on CLI Batch Files, see CLI Batch File.

Figure 6-7 Retrieve File via TFTP Command Screen

Retrieve File via HTTP

Use the **Retrieve File via HTTP** tab to retrieve configuration files, CLI Batch Files, or CLI Batch Logs from the AP. For more information on CLI Batch Files and CLI Batch Logs see CLI Batch File.

1. Select the type of file (Config, CLI Batch File, CLI Batch Log) from the **File Type** drop-down menu.
2. Click on the **Retrieve File** button to initiate the operation.
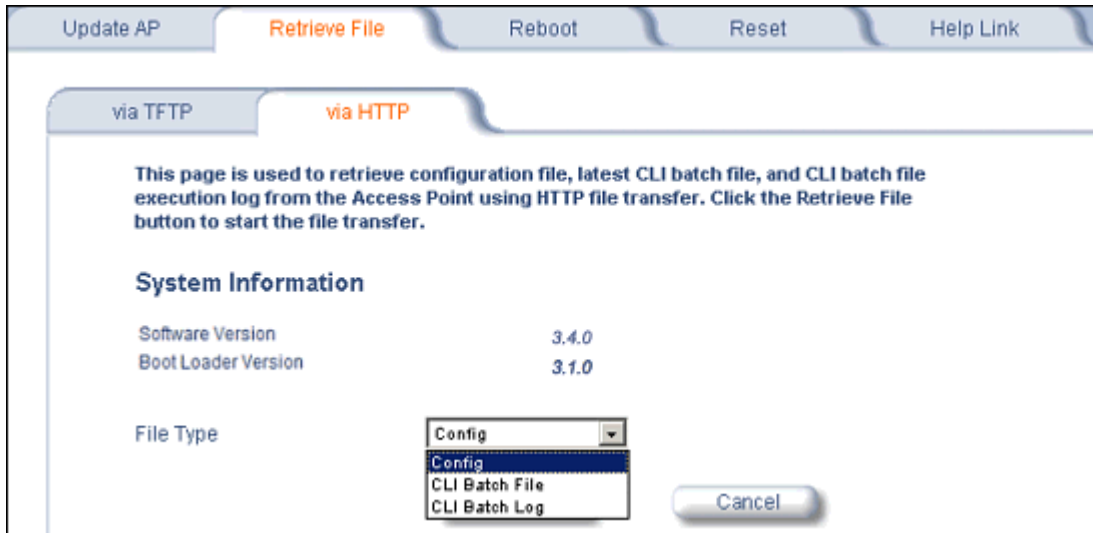
Figure 6-8 Retrieve File via HTTP Command Screen

A confirmation message is displayed, asking if the user wants to proceed with retrieving the file.
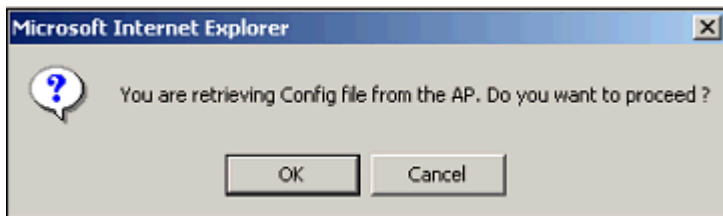
Figure 6-9 Retrieve File Confirmation Dialog

3. Click **OK** to continue with the operation or Cancel to abort the operation. On clicking **OK**, the File Download window appears.
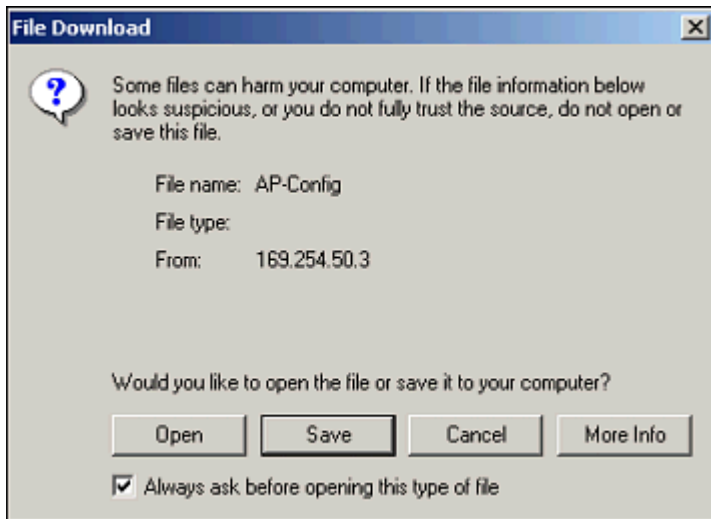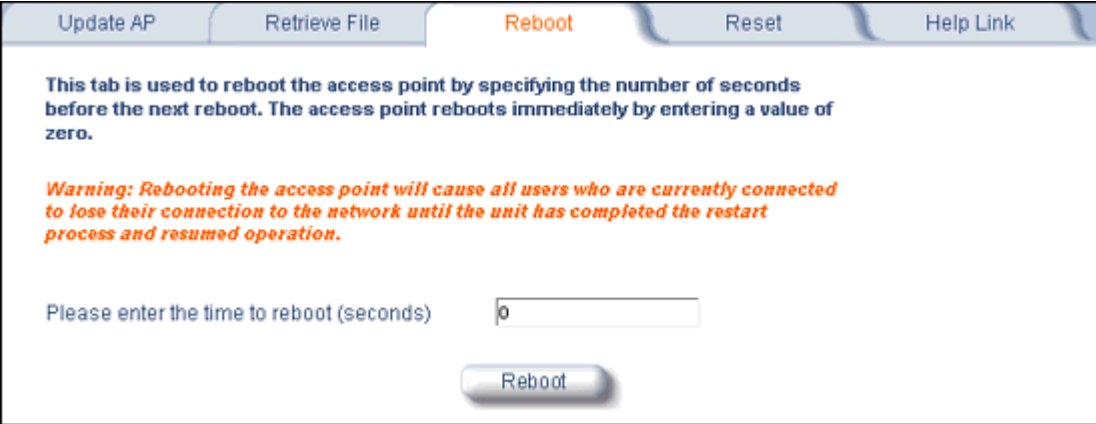
Figure 6-10 File Download Dialog Box

4. On clicking the **Save** button the Save As window displays. Select an appropriate filename and location and click **OK**.

Reboot

Use the **Reboot** tab to save configuration changes (if any) and reset the AP. Enter a value between 0 and 65535 seconds; entering a value of 0 (zero) seconds causes an immediate reboot. Note that **Reset**, described below, does not save configuration changes.

CAUTION: *Rebooting the AP will cause all users who are currently connected to lose their connection to the network until the AP has completed the restart process and resumed operation.*

Figure 6-11 Reboot Command Screen

Reset

Use the **Reset** tab to restore the AP to factory default conditions. Since this will reset the AP's current IP address, a new IP address must be assigned. See Initialization for more information.

CAUTION: *Resetting the AP to its factory default configuration will permanently overwrite all changes that have made to the unit. The AP will reboot automatically after this command has been issued.*
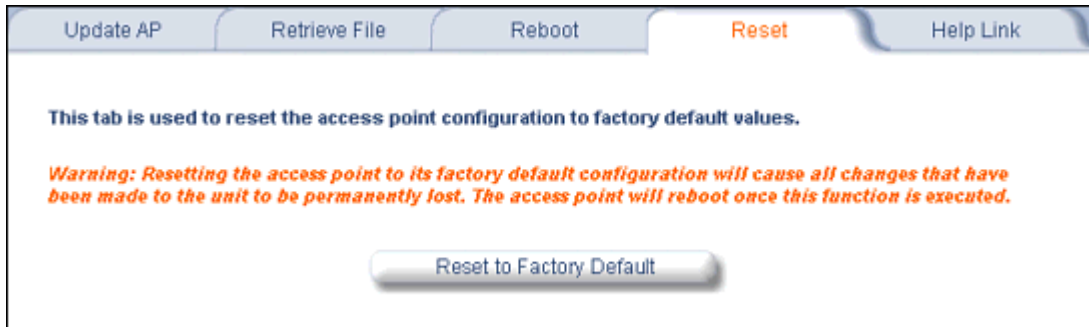
Figure 6-12 Reset to Factory Defaults Command Screen

Help Link

Use the **Help** tab to configure the location of the AP Help files.

During initialization, the AP on-line help files are downloaded to the default location:
C:/Program Files/ORiNOCO/AP700/HTML/index.htm.

To enable the Help button on each page of the Web interface to access the help files, however, copy the entire Help folder to a web server, then specify the new HTTP path in the **Help Link** box.

NOTE: *The configured Help Link must point to an HTTP address in order to enable the Help button on each page of the Web interface.*

NOTE: *Use the forward slash character ("/") rather than the backslash character ("\") when configuring the **Help Link** location.*

NOTE: *Add the AP's management IP address into the Internet Explorer list of Trusted Sites.*

Figure 6-13 Help Link Configuration Screen

Troubleshooting

7

This chapter provides information on the following:

- Troubleshooting Concepts
- Symptoms and Solutions
- Recovery Procedures
- Related Applications

NOTE: *This section helps you locate problems related to the AP device setup. For details about RADIUS, TFTP, serial communication programs (such as HyperTerminal), Telnet applications, or web browsers, please see the documentation that came with the respective application for assistance.*

Troubleshooting Concepts

The following list identifies important troubleshooting concepts and topics. The most common initialization and installation problems relate to IP addressing. For example, you must have valid IP addresses for both the AP and the management computer to access the unit's HTTP interface.

- **IP Address management is fundamental.**
- **Factory default units are set for "Dynamic" (DHCP) IP Address assignment.** The default IP address for the AP is **169.254.128.132** if your network does not have a DHCP server. If you connect the AP to a network with an active DHCP server, then use ScanTool to locate the IP address of your unit. If a DHCP server is not active on your subnet, then use ScanTool to assign a static IP address to the unit.
- **The Trivial File Transfer Protocol (TFTP) provides a means to download and upload files.** These files include the AP Image (executable program) and configuration files.
- **If the AP password is lost or forgotten, you will need to reset to default values.** The Soft Reset to Factory Defaults or Hard Reset to Factory Defaults procedures reset the configuration, but do not change the current AP Image.
- **The AP Supports a Command Line Interface (CLI).** If you are having trouble locating your AP on the network, connect to the unit directly using the serial interface and see Command Line Interface (CLI) for CLI command syntax and parameter names.
- **ScanTool does not work over routers.** You must be connected to the same subnet/physical LAN segment to use ScanTool. Note that ScanTool also works over the wireless interface; you can run it on a wireless client connected to the target AP or an AP connected to the same LAN segment/subnet.
- **If all else fails…** Use the Forced Reload procedure to erase the current AP Image and configuration file and then download a new image.

Symptoms and Solutions

Connectivity Issues

Connectivity issues include any problem that prevents you from powering up or connecting to the AP.

AP Unit Will Not Boot - No LED Activity

1. Make sure your power source is operating.
2. Make sure all cables are connected to the AP correctly.
3. If you are using PoE, make sure you are using a Category 5, foiled, twisted pair cable to power the AP.

Serial Link Does Not Work

1. Make sure you are using a standard, straight-through, 9-pin serial cable.
2. Double-check the physical network connections.
3. Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values:
   - Com Port: (COM1, COM2, etc. depending on your computer);
   - Baud rate: 9600; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None;
   - Line Feeds with Carriage Returns
     (In HyperTerminal select: **File > Properties > Settings > ASCII Setup > Send Line Ends with Line Feeds**)

Ethernet Link Does Not Work

1. Double-check the physical network connections. Use a known-good unit to make sure the network connection is present. Once you have the AP IP address, you can use the "Ping" command over Ethernet to test the IP Address. If the AP responds to the Ping, then the Ethernet Interface is working properly.
2. By default, the Access Point will attempt to automatically detect the Ethernet settings. However, if you are having problems with the Ethernet link, manually configure the Access Point's Ethernet settings. For example, if your switch operates at 100 Mbits/sec/Full Duplex, manually configure the Access Point to use these settings (see Ethernet). If you cannot access the unit over Ethernet, then use the CLI interface over the serial port to configure the Ethernet port (see Command Line Interface (CLI) and Set Ethernet Speed and Transmission Mode).
3. Perform network infrastructure troubleshooting (check switches, routers, etc.).

Basic Software Setup and Configuration Problems

Lost AP, Telnet, or SNMP Password

1. Perform the Soft Reset to Factory Defaults in this guide. This procedure resets system and network parameters, but does not affect the AP Image. The default AP HTTP, Telnet, and SNMP passwords are all **public**.

Client Computer Cannot Connect

1. Client computers should have the same Network Name and security settings as the AP.
2. Network Names should be allocated and maintained by the Network Administrator.
3. See the documentation that came with your client card for additional troubleshooting suggestions.

AP Has Incorrect IP Address

1. Default IP Address Assignment mode is dynamic (DHCP). If you do not have a DHCP server on your network, the default IP Address is **169.254.128.132**. If you have more than one unintialized AP connected to the network, they will all have the same default IP address and you will not be able to communicate with them (due to an IP address conflict). In this case, assign each AP a static IP address via the serial cable or turn off all units but one and change the IP address using ScanTool one at a time.

2. The AP only contacts a DHCP server during boot-up. If your network's DHCP server is not available while the AP is booting, the device will use the default IP address (**169.254.128.132)**. Reboot the AP once your DHCP server is on-line again or use the ScanTool to find the Access Point's current IP address.

3. To find the unit's current IP address if using DHCP, open the IP Client Table in the DHCP Server and match the Access Point's IP address to its MAC address (found on the product label). Alternatively, use ScanTool to identify an Access Point's current IP address.

4. Once you have the current IP address, use the HTTP or CLI Interface to change the unit's IP settings, if necessary.

5. If you use static IP Address assignments, and cannot access the unit over Ethernet, use the Initializing the IP Address using CLI procedure. Once the IP Address is set, you can use the Ethernet Interface to complete configuration.

6. Perform the Soft Reset to Factory Defaults in this guide. This will reset the unit to "DHCP" mode. If there is a DHCP Server on the network, the DHCP Server will assign an IP Address to the AP.

HTTP Interface or Telnet Interface Does Not Work

1. Make sure you are using a compatible browser:
   – Microsoft Internet Explorer 6 with Service Pack 1 or later
   – Netscape 7.1 or later

2. Make sure you have the proper IP address. Enter your Access Point's IP Address in the browser address bar, similar to this example:
   http://192.168.1.100
   When the **Enter Network Password** window appears, leave the **User Name** field empty and enter the HTTP password in the **Password** field. The default HTTP password is **public**.

3. Use the CLI over the serial port to check the IP Access Table, which can be restricting access to Telnet and HTTP.

HTML Help Files Do Not Appear

1. Verify that the HTML Help files are installed in the default directory:
   C:/Program Files/ORiNOCO/AP700**/HTML.**

   If the Help files are not located in this folder, contact your network administrator to find out where the Help files are located on your server.

2. Copy the entire folder to your Web server.

3. Perform the following steps to specify the path for the Help files:
   a. Click the **Commands** button in the HTTP interface.
   b. Select the **Help** tab located at the top of the screen.
   c. Enter the pathname where the Help files are located in the **Help Link** box. This must be an HTTP address.
   d. Click **OK**.

Telnet CLI Does Not Work

1. Make sure you have the proper IP Address. Enter your AP IP address in the Telnet connection dialog, from a DOS prompt, type:
   C:\> telnet <AP IP Address>

2. Use the CLI over the serial port to check the IP Access Table, which can be restricting access to Telnet and HTTP.

TFTP Server Does Not Work

1. Make sure the TFTP Server has been started.

2. Verify the IP address of the TFTP Server. The server may be local or remote, so long as it has a valid IP address.

3. Configure the TFTP Server to "point" to the folder containing the file to be downloaded (or to the folder in which the file is to be uploaded).

4. Verify that you have entered the proper AP Image file name (including the file extension) and directory path (if needed).

5. If you have a problem uploading a file, verify that the TFTP server is configured to allow uploads (typically the default setting is to allow only downloads).

Client Connection Problems

Client Software Finds No Connection

Make sure you have configured your client software with the proper Network Name and Security settings. Network Names and WEP Keys are typically allocated and maintained by your network administrator.

Client PC Card Does Not Work

1. Make sure you are using the latest PC Card driver software.
2. Download and install the latest ORiNOCO client software from http://support.proxim.com.

Intermittent Loss of Connection

1. Make sure you are within range of an active AP.
2. You can check the signal strength using the signal strength gauge on your client software.

Client Does Not Receive an IP Address - Cannot Connect to Internet

1. If the AP is configured as a DHCP server, open the Web-browser Interface and select the **Configure** button and then the **Network** tab to make sure the proper DHCP settings are being used.
2. If you are not using the DHCP server feature on the AP, then make sure that your local DHCP server is accessible from the Access Point's subnet.
3. If using PoE, make sure you are not using a crossover Ethernet cable between the AP and the hub.

VLAN Operation Issues

Verifying Proper Operation of the VLAN Feature

The correct VLAN configuration can be verified by "pinging" both wired and wireless hosts from both sides of the AP device and the network switch. Traffic can be "sniffed" on both the wired (Ethernet) and wireless (WDS) backbones (if configured). Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the AP.

NOTE: The AP-700 supports 16 VLAN/SSID pairs, each with a configured security profile.

VLAN Workgroups

The correct VLAN assignment can be verified by pinging the AP to ensure connectivity, by pinging the switch to ensure VLAN properties, and by pinging hosts past the switch to confirm the switch is functional. Ultimately, traffic can be "sniffed" on the Ethernet or WDS interfaces (if configured) using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the user's assigned network name.

What if network traffic is being directed to a nonexistent host?

• All sessions are disconnected, traffic is lost, and a Forced Reload is necessary.
• Workaround: you can configure the switch to mimic the nonexistent host.

I have just configured the Management ID and now I can't manage the AP?

• Check to ensure your password is correct. If your password is incorrect or all inbound packets do NOT have the correct tag, then a Forced Reload is necessary.

CAUTION: *The* Forced Reload *procedure disconnects all users and resets all values to factory defaults.*

Power-Over-Ethernet (PoE)

The AP Does Not Work

1. Verify that you are using a standard UTP Category 5 cable.
2. Try a different port on the same PoE hub (remember to move the input port accordingly) – if it works, there is probably a faulty port or bad RJ-45 port connection.
3. If possible, try to connect the AP to a different PoE hub.
4. Try using a different Ethernet cable – if it works, there is probably a faulty connection over the long cable, or a bad RJ-45 connection.
5. Check power plug and hub.
6. If the Ethernet link goes down, check the cable, cable type, switch, and hub.

There Is No Data Link

1. Verify that the indicator for the port is "on."
2. Verify that the PoE hub is connected to the Ethernet network with a good connection.
3. Verify that the Ethernet cable is Category 5 or better and is less than 100 meters (approximately 325 feet) in length from the Ethernet source to the AP.
4. Try to connect a different device to the same port on the PoE hub – if it works and a link is established, there is probably a faulty data link in the AP.
5. Try to re-connect the AP to a different output port (remember to move the input port accordingly) – if it works, there is probably a faulty output or input port in the PoE hub or a bad RJ-45 connection.

"Overload" Indications

1. Verify that you are not using a cross-over cable between the PoE output port and the AP.
2. Verify that there is no short over any of the twisted pair cables.
3. Move the device into a different output port (remember to move the input port accordingly); if it works, there is probably a faulty port or bad RJ-45 connection.

Recovery Procedures

The most common installation problems relate to IP addressing. For example, without the TFTP server IP Address, you will not be able to download a new AP Image to the AP. IP Address management is fundamental. We suggest you create a chart to document and validate the IP addresses for your system.

If the password is lost or forgotten, you will need to reset the AP to default values. The Soft Reset to Factory Defaults and Hard Reset to Factory Defaults procedures reset configuration settings, but do not change the current AP Image.

If the AP has a corrupted software image, follow the Forced Reload procedure to erase the current AP Image and download a new image.

Soft Reset to Factory Defaults

Use this procedure to reset the network configuration values, including the password, IP address, and subnet mask. The current AP Image is not deleted.

1. Click **Commands** > **Reset**.
2. Click **Reset to Factory Default**; the device is reset to its factory default state.
3. If not using DHCP, use the ScanTool or use CLI over a serial connection to set the IP address, subnet mask, and other IP parameters. See Command Line Interface (CLI) for CLI information.

If you do not have access to the HTTP or CLI interfaces, use the procedure described in Hard Reset to Factory Defaults.

Hard Reset to Factory Defaults

If you cannot access the unit or you have lost its password, you can reset the unit to the factory default settings using the Reload button on the unit, as described below.

1. Using the end of a paper clip or pin, depress and hold the Reload button on the back of the unit for a minimum of 5 seconds but no more than 10 seconds. The configuration is deleted from the unit and the unit reboots, using a factory default configuration.

   NOTE: You need to use a pin or the end of a paperclip to press the button.

   CAUTION: If you hold the Reload button for longer than 20 seconds, you may go into Forced Reload mode, which erases the unit's embedded software. This software must be reloaded through an Ethernet connection with access to a TFTP server. See Forced Reload *below for instructions.*

2. If not using DHCP, use the ScanTool or use CLI over a serial connection to set the IP address, subnet mask, and other IP parameters. See Command Line Interface (CLI) for CLI information.

Forced Reload

With Forced Reload, you bring the unit into bootloader mode by erasing the embedded software. Use this procedure only as a last resort if the unit does not boot and the procedure did not help.

CAUTION: By completing this procedure, the embedded software in the AP will be erased. You will need to reload the software before the unit is operational.

To do a forced reload:

1. While the unit is running, use a pin or the end of a paperclip to press the **RESET** button.

   The AP reboots and the indicators begin to flash.
2. Press and hold the **RELOAD** button for about 20 seconds until the **POWER LED** turns amber.

   The AP deletes the current AP Image.
3. Follow one of the procedures below to load a new AP Image to the Access Point:

   – Download a New Image Using ScanTool

– Download a New Image Using the Bootloader CLI

Because the CLI option requires a physical connection to the unit's serial port, Proxim recommends the ScanTool option.

Download a New Image Using ScanTool

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides and to a computer that is running ScanTool (this is either two separate computers connected to the same network or a single computer running both programs).

ScanTool detects if an Access Point does not have a valid software image installed. In this case, the **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's *Change* screen so you can download a new image to the unit. (These fields are grayed out if ScanTool does not detect a software image problem.)

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

Follow these steps to use ScanTool to download a software image to an Access Point with a missing image:

1. Download the latest software from http://support.proxim.com. See Download the Software for more detailed instructions.
1. Copy the latest software updates to your TFTP server.
2. Launch ScanTool.
3. Highlight the entry for the AP you want to update and click **Change**.
4. Set **IP Address Type** to **Static**.

NOTE: *You need to assign static IP information temporarily to the Access Point since its DHCP client functionality is not available when no image is installed on the device.*

5. Enter an unused IP address that is valid on your network in the **IP Address** field. You may need to contact your network administrator to get this address.
6. Enter the network's **Subnet Mask** in the field provided.
7. Enter the network's **Gateway IP Address**, if necessary. You may need to contact your network administrator to get this address. You should only need to enter the default gateway address (169.254.128.133) if the Access Point and the TFTP server are separated by a router.
8. Enter the IP address of your TFTP server in the field provided.
9. Enter the **Image File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.
10. Click **OK**.

The Access Point will reboot and the download will begin automatically. You should see downloading activity begin after a few seconds within the TFTP server's status screen.

11. Click **OK** when prompted that the device has been updated successfully to return to the *Scan List* screen.
12. Click **Cancel** to close the ScanTool.
13. When the download process is complete, configure the AP.

Download a New Image Using the Bootloader CLI

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN or connected to the AP with a cross-over Ethernet cable.

You must also connect the AP to a computer with a standard serial cable and use a terminal client, such as HyperTerminal. From the terminal, enter CLI Commands to set the IP address and download an AP Image.

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

1. Download the latest software from http://support.proxim.com. See Download the Software for more detailed instructions.
2. Copy the latest software updates to your TFTP server's default directory.
3. Use a straight-through serial cable to connect the Access Point's serial port to your computer's serial port.
4. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
5. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.

   HyperTerminal sends a line return at the end of each line of code.
6. Press the **RESET** button on the AP.

   The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Sending Traps to SNMP manager periodically.** After this message appears, press the **ENTER** key repeatedly until the following prompt appears:

   `[Device name]>`
7. Enter only the following statements:

   `[Device name]> `**`show`** (to view configuration parameters and values)

   `[Device name]> `**`set ipaddrtype static`**

   `[Device name]> `**`set ipaddr <Access Point IP Address>`**

   `[Device name]> `**`set ipsubmask <IP Mask>`**

   `[Device name]> `**`set tftpipaddr <TFTP Server IP Address>`**

   `[Device name]> `**`set tftpfilename <AP Image File Name, including file extension>`**

   `[Device name]> `**`set ipgw <Gateway IP Address>`**

   `[Device name]> `**`show`** (to confirm your new settings)

   `[Device name]> `**`reboot`**

   Example:

   `[Device name]> `**`show`**

   `[Device name]> `**`set ipaddrtype static`**

   `[Device name]> `**`set ipaddr 10.0.0.12`**

   `[Device name]> `**`set ipsubmask 255.255.255.0`**

   `[Device name]> `**`set tftpipaddr 10.0.0.20`**

   `[Device name]> `**`set tftpfilename MyImage.bin`**

   `[Device name]> `**`set ipgw 10.0.0.30`**

```
[Device name]> show
```
```
[Device name]> reboot
```

The AP will reboot and then download the image file. You should see downloading activity begin after a few seconds within the TFTP server's status screen.

8. When the download process is complete, configure the AP.

Setting IP Address using Serial Port

Use the following procedure to set an IP address over the serial port using the CLI. The network administrator typically provides the AP IP address.

Hardware and Software Requirements

- Standard straight-through serial data (RS-232) cable (not included with shipment).
- ASCII Terminal software, such as HyperTerminal.

Attaching the Serial Port Cable

1. Connect one end of the serial cable to the AP and the other end to a serial port on your computer.
2. Power on the computer and AP, if necessary.

Initializing the IP Address using CLI

After installing the serial port cable, you may use the CLI to communicate with the AP. CLI supports most generic terminal emulation programs, such as HyperTerminal (which is included with the Windows operating systems). In addition, many web sites offer shareware or commercial terminal programs you can download. Once the IP address has been assigned, you can use the HTTP interface or the CLI over Telnet to complete configuration.

Follow these steps to assign the AP an IP address:

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
    - Com Port: <COM1, COM2, etc., depending on your computer>
    - Baud rate: 9600
    - Data Bits: 8
    - Stop bits: 1
    - Flow Control: None
    - Parity: None
2. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.

    HyperTerminal sends a line return at the end of each line of code.
3. Press the **RESET** button on the AP.

    The terminal display shows Power On Self Tests (POST) activity, and then displays a CLI prompt, similar to the example below. This process may take up to 90 seconds.
    ```
    [Device name]> Please enter password:
    ```
4. Enter the CLI password (default is **public**).

    The terminal displays a welcome message and then the CLI Prompt:
    ```
    [Device name]>
    ```
5. Enter **show ip**. Network parameters appear:

```
[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr         :       10.0.0.1
ipsubmask      :       255.0.0.0
ipgw           :       10.0.0.1
ipttl          :       64
ipaddrtype     :       static


[Device Name]> _
```

Figure 7-1 Result of "show ip" CLI Command

6. Change the IP address and other network values using **set** and **reboot** CLI commands, similar to the example below (use your own IP address and subnet mask). Note that IP Address Type is set to Dynamic by default. If you have a DHCP server on your network, you should not need to manually configure the Access Point's IP address; the Access Point will obtain an IP address from the network's DHCP server during boot-up.

   After each entry the CLI reminds you to reboot; however wait to reboot until all commands have been entered.

   [Device name]> **set ipaddrtype static**

   [Device name]> **set ipaddr <IP Address>**

   [Device name]> **set ipsubmask <IP Subnet Mask>**

   [Device name]> **set ipgw <Default Gateway IP Address>**

   [Device name]> **show ip (to confirm your new settings)**

   [Device name]> **reboot 0**

7. After the AP reboots, verify the new IP address by reconnecting to the CLI and enter a **show ip** command. Alternatively, you can ping the AP from a network computer to confirm that the new IP address has taken effect.

8. When the proper IP address is set, use the HTTP interface or CLI over Telnet to configure the rest of the unit's operating parameters.

Related Applications

RADIUS Authentication Server

If you enabled RADIUS Authentication on the AP, make sure that your network's RADIUS servers are operational. Otherwise, clients will not be able to log in. There are several reasons the authentication server services might be unavailable, here are two typical things to check:

- Make sure you have the proper RADIUS authentication server information setup configured in the AP. Check the RADIUS Authentication Server's Shared Secret and Destination Port number (default is 1812; for RADIUS Accounting, the default is 1813).
- Make sure the RADIUS authentication server RAS setup matches the AP.

TFTP Server

The "Trivial File Transfer Protocol" (TFTP) server allows you to transfer files across a network. You can upload configuration files from the AP for backup or copying, and you can download configuration files or new software images. The TFTP software is located on the installation CD.

If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP address. Note that you do not need a TFTP server running unless you want to transfer files to or from the AP.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP Address, the proper AP Image file name, and that the TFTP server is connected.
- Make sure the TFTP server is configured to both Transmit and Receive files (on the TFTP server's **Security** tab), with no automatic shutdown or time-out (on the **Auto Close** tab).

Command Line Interface (CLI)

A

This section discusses the following:

CLI commands can be used to initialize, configure, and manage the Access Point.

- CLI commands may be entered in real time through a keyboard or submitted with CLI scripts.

- A *CLI Batch file* is a user-editable configuration file that provides a user-friendly way to change the AP configuration through a file upload. The CLI Batch file is an ASCII file that facilitates Auto Configuration because it does not require the user to access one of the AP's management interfaces to make configuration changes as is required with the proprietary LTV format configuration file.

- The CLI is available through both the Serial Port interface and over the Ethernet interface using Telnet.

NOTE: All CLI commands and parameters are case-sensitive.

General Notes

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts, network access infrastructures, and client-server relationships. In addition, you should be familiar with software setup procedures for typical network operating systems and servers.

Notation Conventions

- Computer prompts are shown as constant width type. For example: `[Device-Name]>`
- Information that you input as shown is displayed in bold constant width type. For example:
  `[Device name]> `**`set ipaddr 10.0.0.12`**
- The names of keyboard keys, software buttons, and field names are displayed in bold type. For example: Click the **Configure** button.
- Screen names are displayed in bold italics. For example, the ***System Status*** screen.

Important Terminology

- Configuration Files - Database files containing the current Access Point configuration. Configuration items include the IP Address and other network-specific values. Config files may be downloaded to the Access Point or uploaded for backup or troubleshooting.
- Download vs. Upload - Downloads transfer files to the Access Point. Uploads transfer files from the Access Point. The TFTP server performs file transfers in both directions.
- Group - A logical collection of network parameter information. For example, the System Group is composed of several related parameters. Groups can also contain Tables. All items for a given Group can be displayed with a **show <Group>** CLI Command.
- Image File - The Access Point software executed from RAM. To update an Access Point you typically download a new Image File. This file is often referred to as the "AP Image".
- Parameter - A fundamental network value that can be displayed and may be changeable. For example, the Access Point must have a unique IP Address and the Wireless interface must be assigned an SSID. Change parameters with the CLI **set** Command, and view them with the CLI **show** Command.
- Table - Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP Table. All items for a given Table can be displayed with a **show <Table>** CLI Command.
- TFTP - Refers to the TFTP Server, used for file transfers.

Navigation and Special Keys

This CLI supports the following navigation and special key functions to move the cursor along the prompt line.

Key Combination	Operation
Delete or Backspace	Delete previous character
Ctrl-A	Move cursor to beginning of line
Ctrl-E	Move cursor to end of line
Ctrl-F	Move cursor forward one character
Ctrl-B	Move cursor back one character
Ctrl-D	Delete the character the cursor is on
Ctrl-U	Delete all text to left of cursor
Ctrl-P	Go to the previous line in the history buffer
Ctrl-N	Go to the next line in the history buffer
Ctrl-W	Delete the previous word

Key Combination	Operation
Tab	Complete the command line
?	List available commands

CLI Error Messages

The following table describes the error messages associated with improper inputs or expected CLI behavior.

Error Message	Description
Syntax Error	Invalid syntax entered at the command prompt.
Invalid Command	A non-existent command has been entered at the command prompt.
Invalid Parameter Name	An invalid parameter name has been entered at the command prompt.
Invalid Parameter Value	An invalid parameter value has been entered at the command prompt.
Invalid Table Index	An invalid table index has been entered at the command prompt.
Invalid Table Parameter	An invalid table parameter has been entered at the command prompt.
Invalid Table Parameter Value	An invalid table parameter value has been entered at the command prompt.
Read Only Parameter	User is attempting to configure a read-only parameter.
Incorrect Password	An incorrect password has been entered in the CLI login prompt.
Download Unsuccessful	The download operation has failed due to incorrect TFTP server IP Address or file name.
Upload Unsuccessful	The upload operation has failed due to incorrect TFTP server IP Address or file name.

Command Line Interface (CLI) Variations

Administrators use the CLI to control Access Point operation and monitor network statistics. The AP supports two types of CLI: the Bootloader CLI and the normal CLI. The Bootloader CLI provides a limited command set, and is used when the current AP Image is bad or missing. The Bootloader CLI allows you to assign an IP Address and download a new image. Once the image is downloaded and running, the Access Point uses the normal CLI. This guide covers the normal CLI unless otherwise specified.

Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI used to perform initial configuration of the AP. This interface is only accessible via the serial interface if the AP does not contain a software image or a download image command over TFTP has failed.

The Bootloader CLI provides you with the ability to configure the initial setup parameters as well as download a software image to the device.

The following functions are supported by the Bootloader CLI:

- configuration of initial device parameters using the **set** command
- **show** command to view the device's configuration parameters
- **help** command to provide additional information on all commands supported by the Bootloader CLI
- **reboot** command to reboot the device

The parameters supported by the Bootloader CLI (for viewing and modifying) are:

- System Name
- IP Address Assignment Type
- IP Address
- IP Mask
- Gateway IP Address
- TFTP Server IP Address
- Image File Name (including the file extension)

The following lists display the results of using the **help** command in the Bootloader CLI:

```
[Device name]> help

Command List        Description
============        ===========
set                 Set system parameters
show                Show running system information
help                Description of commands, command usage and parameters
reboot              reboot the target

Command Usage
=============
set <parameter name> <parameter value> <cr>
show <cr>
help <cr>
reboot <cr>

Parameter List      Description
==============      ===========
sysname             System Name
ipaddr              System IP Address
ipsubmask           System Subnet Mask
ipgw                System Default Gateway IP Address
tftpipaddr          TFTP Server IP Address
tftpfilename        Image or Binary File name
ipaddrtype          System IP Address Type - STATIC or DYNAMIC

[Device name]>
```

Figure A-1 Results of "help" bootloader CLI command

The following lists display the results of using the **show** command in the Bootloader CLI:

```
[Device name]> show

sysname          Device              System Name
ipaddr           10.0.0.1            System IP Address
ipsubmask        255.0.0.0           System Subnet Mask
ipgw             10.0.0.1            System Default Gateway IP Address
ipaddrtype       DYNAMIC             IP Address type
tftpipaddr       10.0.0.2            TFTP Server IP Address
tftpfilename     FILENAME            Image or Binary File Name

[Device name]>
```

Figure A-2 Results of "show" bootloader CLI command

CLI Command Types

This guide divides CLI Commands into two categories: Operational and Parameter Controls.

Operational CLI Commands

These commands affect Access Point behavior, such as downloading, rebooting, and so on. After entering commands (and parameters, if any) press the **Enter** key to execute the Command Line.

Operational commands include:

- **?:** Typing a question mark lists CLI Commands or parameters, depending on usage (you do not need to type Enter after typing this command)
- **done, exit, quit:** Terminates the CLI session
- **download:** Uses a TFTP server to download "image" files, "config" files, "bootloader upgrade" files, a "license" file, "SSL certificates", "SSL private keys", "SSH public keys", "SSH private keys", or "CLI Batch Files" to the Access Point
- **help:** Displays general CLI help information or command help information, such as command usage and syntax
- **history:** Remembers commands to help avoid re-entering complex statements
- **passwd:** Sets the Access Point's CLI password
- **reboot:** Reboots the Access Point in the specified time
- **search:** Lists the parameters in a specified Table
- **upload:** Uses TFTP server to upload "config" files from Access Point to TFTP default directory or specified path

? (List Commands)

This command can be used in a number of ways to display available commands and parameters.

The following table lists each operation and provides a basic example. Following the table are detailed examples and display results for each operation.

Operation	Basic Example
Display the Command List (Example 1)	`[Device-Name]>`**?**
Display commands that start with specified letters (Example 2)	`[Device-Name]>`**s?**
Display parameters for set and show Commands (Examples 3a and 3b)	`[Device-Name]>`**set ?** `[Device-Name]>`**show ipa?**
Prompt to enter successive parameters for Commands (Example 4)	`[Device-Name]>`**download ?**

Example 1. Display Command list

To display the Command List, enter **?**.

`[Device-Name]>`**?**

```
[Device Name]>
show
set
download
upload
reboot
passwd
help
quit
done
exit
history
search
[Device Name]> _
```

Figure A-3 Result of "?" CLI command

Example 2. Display specific Commands

To show all commands that start with specified letters, enter one or more letters, then **?** with no space between letters and **?**.

[Device-Name]>**s?**

```
[Device Name]> s
show            set                search
```

Figure A-4 Result of "s?" CLI command

Example 3. Display parameters for set and show

Example 3a allows you to see every possible parameter for the set (or show) commands. Notice from example 3a that the list is very long. Example 3b shows how to display a subset of the parameters based on initial parameter letters.

Example 3a. Display every parameter that can be changed

[Device-Name]>**set ?**

```
[Device Name]> set
Command Description:
The set command modifies the value of a given scalar parameter or table entry.

Command Usage:
set <parameter> <parameter value> <CR>
set <table> <index> <arg1> <value1> ..... <argN> <valueN> <CR>

Example:
set sysname "My Wireless Device" <CR>
set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0 cmt "Test WorkStation"
 <CR>

[Device Name]> set
broadcastflttbl
dhcpgw
dhcpippooltbl
dhcppridnsipaddr
dhcpsecdnsipaddr
dhcpstatus
dnsdomainname
dnsprisvripaddr
dnssecsvripaddr
dnsstatus
etherfltifbitmask
.
.
.
.
telsessiontout
tftpfilename
tftpfiletype
tftpipaddr
vlanidtbl
vlanmgmtid
vlanstatus
wdstbl
wif
wifsec
[Device Name]> set _
```

Figure A-5 Result of "set ?" CLI command

Example 3b. Display parameters based on letter sequence

This example shows entries for parameters that start with the letter "i". The more letters you enter, the fewer the results returned. Notice that there is no space between the letters and the question mark.

[Device-Name]> **show ipa?**

```
[Device Name]> show ipa
ipaddr              ipaddrtype           iparp
iparpfltipaddr      iparpfltstatus       iparpfltsubmask
```

Figure A-6 Result of "show ipa?" CLI command

[Device-Name]> **show iparp?**

```
[Device Name]> show iparp
iparp              iparpfltipaddr        iparpfltstatus
iparpfltsubmask
[Device Name]> show iparp_
```

Figure A-7 Result of "show iparp?" CLI command

Example 4. Display Prompts for Successive Parameters

Enter the command, a space, and then **?**. Then, when the parameter prompt appears, enter the parameter value. The parameter is changed and a new CLI line is echoed with the new value (in the first part of the following example, the value is the IP Address of the TFTP server).

After entering one parameter, you may add another **?** to the new CLI line to see the next parameter prompt, and so on until you have entered all of the required parameters. The following example shows how this is used for the **download** Command. The last part of the example shows the completed **download** Command ready for execution.

```
[Device-Name]> download ?
<TFTP IP Address>

[Device-Name]> download 192.168.0.101 ?
<File Name>

[Device-Name]> download 192.168.0.101 apimage ?
<file type (config/img/bootloader)>

[Device-Name]> download 192.168.0.101 apimage img <CR>
```

done, exit, quit

Each of the following commands ends a CLI session:

```
[Device-Name]> done
[Device-Name]> exit
[Device-Name]> quit
```

download

Downloads the specified file from a TFTP server to the Access Point. Executing **download** in combination with the asterisks character ("*") will make use of the previously set TFTP parameters. Executing download without parameters will display command help and usage information.

1. Syntax to download a file:
   ```
   [Device-Name]>download <tftp server address> <path and filename> <file type>
   ```

   Example:
   ```
   [Device-Name]>download 192.168.1.100 APImage2 img
   ```

2. Syntax to display help and usage information:
   ```
   [Device-Name]>download
   ```

3. Syntax to execute the download Command using previously set (stored) TFTP Parameters:
   ```
   [Device-Name]>download *
   ```

help

Displays instructions on using control-key sequences for navigating a Command Line and displays command information and examples.

1. Using help as the only argument:
   [Device-Name]>**help**

```
[Device Name]> help
Type ? at the command prompt for a command list.

Complete command description and command usage can be provided by:
help <command name> <CR>
<command name> help <CR>

Special keys supported:
Arrow Keys
DEL, BS .... delete previous character
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W ..... delete previous word
Ctrl-T ..... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer

Tab     .... will attempt command completion
# .... Comment Character
?       .... will provide command listing

Examples:
'?'          list all the supported commands
'sh?'        list all commands that start with sh
'show ?'     list all arguments to the show command
'sh<TAB>'    complete the 'show' command

[Device Name]>
```

Figure A-8 Results of "help" CLI command

2. Complete command description and command usage can be provided by:
   [Device-Name]>**help <command name>**
   [Device-Name]>**<command name> help**

history

Shows content of Command History Buffer. The Command History Buffer stores command statements entered in the current session. To avoid re-entering long command statements, use the keyboard "up arrow" (Ctrl-P) and "down arrow" (Ctrl-N) keys to recall previous statements from the Command History Buffer. When the desired statement reappears, press the **Enter** key to execute, or you may edit the statement before executing it.

[Device-Name]> **history**

passwd

Changes the CLI Password.

[Device-Name]> **passwd oldpassword newpassword newpassword**

reboot

Reboots Access Point after specified number of seconds. Specify a value of 0 (zero) for immediate reboot.

[Device-Name]> **reboot 0**
[Device-Name]> **reboot 30**

search

Lists the parameters supported by the specified table. This list corresponds to the table information displayed in the HTTP interface. In this example, the CLI returns the list of parameters that make up an entry in the IP Access Table.

[Device-Name]> **search mgmtipaccesstbl**

```
[Device Name]> search mgmtipaccesstbl
The supported elements are:
index
ipaddr
ipmask
cmt
status
```

Figure A-9 Results of "search mgmtipaccesstbl" CLI command

upload

Uploads a text-based configuration file from the AP to the TFTP Server. Executing **upload** with the asterisk character ("*") will make use of the previously set/stored TFTP parameters. Executing **upload** without parameters will display command help and usage information.

1. Syntax to upload a file:
   [Device-Name]>**upload <tftp server address> <path and filename> <filetype>**

   Example:
   [Device-Name]>**upload 192.168.1.100 APconfig.sys config**

2. Syntax to display help and usage information:
   [Device-Name]>**help upload**

3. Syntax to execute the upload command using previously set (stored) TFTP Parameters:
   [Device-Name]>**upload ***

Parameter Control Commands

The following sections cover the two Parameter Control Commands (**show** and **set**) and include several tables showing parameter properties. These commands allow you to view (**show**) all parameters and statistics and to change (**set**) parameters.

- **show:** To see any Parameter or Statistic value, you can specify a single parameter, a Group, or a Table.
- **set:** Use this CLI Command to change parameter values. You can use a single CLI statement to modify Tables, or you can modify each parameter separately.

"show" CLI Command

Displays the value of the specified parameter, or displays all parameter values of a specified group (parameter table). Groups contain Parameters and Tables. Tables contain parameters for a series of similar entities.

To see a definition and syntax example, type only **show** and then press the **Enter** key. To see a list of available parameters, enter a question mark (**?**) after **show** (example: **show ?**).

Syntax:
[Device-Name]>**show <parameter>**
[Device-Name]>**show <group>**
[Device-Name]>**show <table>**

Examples:
[Device-Name]>**show ipaddr**

```
[Device-Name]>show network
[Device-Name]>show mgmtipaccesstbl
```

"set" CLI Command

Sets (modifies) the value of the specified parameter. To see a definition and syntax example, type only **set** and then press the **Enter** key. To see a list of available parameters, enter a space, then a question mark (**?**) after **set** (example: **set?**).

Syntax:
```
[Device-Name]>set <parameter> <value>
[Device-Name]>set <table> <index> <argument 1> <value 1> ... <argument N> <value N>
```

Example:

```
[Device-Name]>set sysloc "Main Lobby"
[Device-Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

Configuring Objects that Require Reboot

Certain objects supported by the Access Point require a device reboot in order for the changes to take effect. In order to inform the end-user of this behavior, the CLI provides informational messages when the user has configured an object that requires a reboot. The following messages are displayed as a result of the configuring such object or objects.

Example 1: Configuring objects that require the device to be rebooted

The following message is displayed every time the user has configured an object that requires the device to be rebooted.

```
[Device-Name]>set ipaddr 135.114.73.10
```
The following elements require reboot

ipaddr

Example 2: Executing the "exit", "quit", or "done" commands when an object that requires reboot has been configured

In addition to the above informational message, the CLI also provides a message as a result of the **exit**, **quit**, or **done** command if changes have been made to objects that require reboot. If you make changes to objects that require reboot and execute the exit command the following message is displayed:

```
[Device-Name]>exit<CR> OR quit<CR> OR done<CR>
```

Modifications have been made to parameters that require the device to be rebooted. These changes will only take effect after the next reboot.

"set" and "show" Command Examples

In general, you will use the CLI **show** Command to view current parameter values and use the CLI **set** Command to change parameter values. As shown in the following examples, parameters may be set individually or all parameters for a given table can be set with a single statement.

Example 1 - Set the Access Point IP Address Parameter

Syntax:
```
[Device-Name]>set <parameter name> <parameter value>
```

Example:
```
[Device-Name]> set ipaddr 10.0.0.12
```

IP Address will be changed when you reboot the Access Point. The CLI reminds you when rebooting is required for a change to take effect. To reboot immediately, enter **reboot 0** (zero) at the CLI prompt.

Example 2 - Create a table entry or row

Use 0 (zero) as the index to a table when creating an entry. When creating a table row, only the mandatory table elements are required (comment is usually an optional table element). For optional table elements, the default value is generally applied if you do not specify a value.

Syntax:
```
[Device-Name]>set <table name> <table index> <element 1> <value 1> …
        <element n> <value n>
```

Example:
```
[Device-Name]> set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

A new table entry is created for IP address 10.0.0.10 with a 255.255.0.0 subnet mask.

Example 3 - Modify a table entry or row

Use the index to be modified and the table elements you would like to modify. For example, suppose the IP Access Table has one entry and you wanted to modify the IP address:

```
[Device-Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.11
```

You can also modify several elements in the table entry. Enter the index number and specific table elements you would like to modify. (Hint: Use the search Command to see the elements that belong to the table.)

```
[Device-Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.12 ipmask 255.255.255.248
        cmt "First Row"
```

Example 4 - Enable, Disable, or Delete a table entry or row

The following example illustrates how to manage the second entry in a table.

Syntax:
```
[Device-Name]>set <Table> index status <enable, disable, delete>
[Device-Name]>set <Table> index status <1=enable, 2=disable, 3=delete>
```

Example:
```
[Device-Name]>set mgmtipaccesstbl 2 status enable
[Device-Name]>set mgmtipaccesstbl 2 status disable
[Device-Name]>set mgmtipaccesstbl 2 status delete
[Device-Name]>set mgmtipaccesstbl 2 status 2
```

NOTE: You may need to enable a disabled table entry before you can change the entry's elements.

Example 5 - Show the Group Parameters

This example illustrates how to view all elements of a group or table.

Syntax:
```
[Device-Name]> show <group name>
```

Example:
```
[Device-Name]>show network
```

The CLI displays network group parameters. Note `show network` and `show ip` return the same data.

```
[Device Name]> show network
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

Figure A-10 Results of "show network" and "show ip" CLI Commands

Example 6 - Show Individual and Table Parameters

1. View a single parameter.

   Syntax:
   [Device-Name]>**show <parameter name>**

   Example:
   [Device-Name]> **show ipaddr**

   Displays the Access Point IP address.

```
[Device Name]> show ipaddr
ipaddr

10.0.0.1

[Device Name]> _
```

Figure A-11 Result of "show ipaddr" CLI Command

2. View all parameters in a table.

   Syntax:
   [Device-Name]> **show <table name>**
   Example: [Device-Name]> **show mgmtipaccesstbl**

   The CLI displays the IP Access Table and its entries.

Using Tables and Strings

Working with Tables

Each table element (or parameter) must be specified, as in the example below.

```
[Device-Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

Below are the rules for creating, modifying, enabling/disabling, and deleting table entries.

• Creation
  – The table name is required.
  – The table index is required – for table entry/instance creation the index is always zero (0).
  – The order in which the table arguments or objects are entered in not important.
  – Parameters that are not required can be omitted, in which case they will be assigned the default value.
• Modification
  – The table name is required.
  – The table index is required – to modify the table, "index" must be the index of the entry to be modified.
  – Only the table objects that are to be modified need to be specified. Not all the table objects are required.
  – If multiple table objects are to be modified the order in which they are entered is not important.
  – If the entire table entry is to be modified, all the table objects have to be specified.
• Enabling/Disabling
  – The table name is required.
  – The table index is required – for table enabling/disabling the index should be the index of the entry to be enabled/disabled.
  – The entry's new state (either "enable" or "disable") is required.
• Deletion
  – The table name is required.
  – The table index is required – for table deletion the index should be the index of the entry to be deleted.
  – The word "delete" is required.

Using Strings

Since there are several string objects supported by the AP, a string delimiter is required for the strings to be interpreted correctly by the command line parser. For this CLI implementation, the single quote or double quote character can be used at the beginning and at the end of the string.

For example:
```
[Device-Name]> set sysloc Lobby    - Does not need quote marks
[Device-Name]> set sysloc "Front Lobby"   - Requires quote marks.
```

The scenarios supported by this CLI are:

"My Desk in the office"	Double Quotes
'My Desk in the office'	Single Quotes
"My 'Desk' in the office"	Single Quotes within Double Quotes
'My "Desk" in the office'	Double Quotes within Single Quotes
"Daniel's Desk in the office"	One Single Quote within Double Quotes
'Daniel"s Desk in the office'	One Double Quote within Single Quotes

The string delimiter does not have to be used for every string object. The single quote or double quote only has to be used for string objects that contain blank space characters. If the string object being used does not contain blank spaces, then the string delimiters, single or double quotes, mentioned in this section are not required.

Configuring the AP using CLI commands

Log into the AP using HyperTerminal

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
    - Com Port: <COM1, COM2, etc., depending on your computer>
    - Baud rate: 9600
    - Data Bits: 8
    - Stop bits: 1
    - Flow Control: None
    - Parity: None
2. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.
    HyperTerminal sends a line return at the end of each line of code.
3. Enter the CLI password (default is **public**).

NOTE: *Proxim recommends changing your default passwords immediately. To perform this operation using CLI commands, see* Change Passwords*.*

Log into the AP using Telnet

The CLI commands can be used to access, configure, and manage the AP using Telnet. Follow these steps:

1. Confirm that your computer's IP address is in the same IP subnet as the AP.

    NOTE: *If you have not previously configured the Access Point's IP address and do not have a DHCP server on the network, the Access Point will default to an IP address of 169.254.128.132.*

2. Go to the DOS command prompt on your computer.
3. Type **telnet <IP Address of the unit>**.
4. Enter the CLI password (default is **public**).

NOTE: *Proxim recommends changing your default passwords immediately. To perform this operation using CLI commands, see* Change Passwords*.*

Set Basic Configuration Parameters using CLI Commands

There are a few basic configuration parameters that you may want to setup right away when you receive the AP. For example:

- Set System Name, Location and Contact Information
- Set Static IP Address for the AP
- Download an AP Configuration File from your TFTP Server
- Set up Auto Configuration
- Set Network Names for the Wireless Interface
- Enable 802.11d Support and Set the Country Code
- Enable and Configure TX Power Control for the Wireless Interface
- Configure SSIDs (Network Names), VLANs, and Profiles
- Download an AP Configuration File from your TFTP Server
- Backup your AP Configuration File

Set System Name, Location and Contact Information

NOTE: *System name must:*
- *Contain only letters, numbers, and hyphens.*
- *Be limited to 31 characters.*
- *Not begin with a number or hyphen.*
- *Not contain blank spaces.*

```
[Device-Name]>set sysname <Name> sysloc <Unit Location>
[Device-Name]>set sysctname <Contact Name>
[Device-Name]>set sysctphone <Contact Phone Number> sysctemail <Contact E-mail address>
[Device-Name]>show system
```

```
[Device Name]> show system
System Parameters
=================

sysname                  :        Device
sysloc                   :        System Location
sysctname                :        Contact Name
sysctemail               :        name@Organization.com
sysctphone               :        Contact Phone Number
sysuptime (DD:HH:MM:SS) :         0:11: 6:40
sysoid                   :        1.3.6.1.4.1.11898.2.4.6
sysdescr                 :         AP v3.3.0  SN-02UT16570004 v3.1.0
sysservices              :        2
sysflashupdate           :        0
sysflashbckint           :        120
sysresettodefaults       :        0

[Device Name]> _
```

Figure A-12 Result of "show system" CLI Command

Set Static IP Address for the AP

NOTE: *The IP Subnet Mask of the AP must match your network's Subnet Mask.*

```
[Device-Name]>set ipaddrtype static
[Device-Name]>set ipaddr <fixed IP address of unit>
[Device-Name]>set ipsubmask <IP Mask>
[Device-Name]>set ipgw <gateway IP address>
[Device-Name]>show network
```

Change Passwords

```
[Device-Name]>passwd <Old Password> <New Password> <Confirm Password> (CLI password)
[Device-Name]>set httppasswd <New Password> (HTTP interface password)
```

```
[Device-Name]>set snmprpasswd <New Password> (SNMP read password)
[Device-Name]>set snmprwpasswd <New Password> (SNMP read/write)
[Device-Name]>set snmpv3authpasswd <New Password> (SNMPv3 authentication password)
[Device-Name]>set snmpv3privpasswd <New Password> (SNMPv3 privacy password)
[Device-Name]>reboot 0
```

CAUTION: *Proxim strongly urges you to change the default passwords to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the Soft Reset to Factory Defaults.*

Set Network Names for the Wireless Interface

```
[Device-Name]>set wif 3 netname <Network Name (SSID) for wireless interface>
[Device-Name]>show wif
```

```
[Device Name]> show wif
Wireless Interface Table
=========================


Index                         :     3
Network Name                  :     My Wireless Network A
Distance Between APs          :     large
Interference Robustness       :     disable
DTIM Period                   :     1
Automatic Channel Selection   :     enable
Frequency Channel             :     56
RTS/CTS Medium Reservation    :     2347
Multicast Rate                :     2 MBps
Closed System                 :     disable
Load Balancing                :     enable
Medium Density Distribution   :     disable
MAC Address                   :     00:30:F1:65:09:E9
Supported Data Rates          :     6 9 12 18 24 36 48 54
Supported Frequency Channels  :     52 56 60 64 36 40 44 48 149 153 157 161
Physical Layer Type           :     OFDM
Regulatory Domain List        :     USA (FCC)
Transmit Rate                 :     0
TurboMode                     :     disable
```

Figure A-13 Results of "show wif" CLI command for an AP

Enable 802.11d Support and Set the Country Code

NOTE: On APs with model numbers ending in -WD, these commands are not available.

Perform the following command to enable 802.11d IEEE 802.11d support for additional regulatory domains.

```
[Device-Name]>set wif 3 dot11dstatus <enable/disable>
```

Perform the following command to set a country code:

```
[Device-Name]>set syscountrycode <country code>
```

Select a country code from the following table, derived from ISO 3166. Available countries will vary based on regulatory domain. Refer to the **ISO/IEC 3166-1 CountryCode** drop-down menu on the **Configure > Interfaces > Operational Mode** page; this menu contains a list of all the available countries in your regulatory domain.

NOTE: If you select a country code that is not supported in your regulatory domain, clients may attempt to connect to a channel that is not supported by your AP.

Country	Code	Country	Code	Country	Code
Algeria	DZ	Honduras	HN	Panama	PA
Albania	AL	Hong Kong	HK	Papua New Guinea	PG
Argentina	AR	Hungary	HU	Peru	PE

Country	Code	Country	Code	Country	Code
Armenia	AM	Iceland	IS	Philippines	PH
Australia	AU	India	IN	Poland	PL
Austria	AT	Indonesia	ID	Portugal	PT
Azerbaijan	AZ	Ireland 5.8 GHz	I1	Puerto Rico	PR
Bahrain	BH	Israel	IL	Qatar	QA
Belarus	BY	Italy	IT	Romania	RO
Belgium	BE	Jamaica	JM	Russia	RU
Belize	BZ	Japan	JP	Samoa	WS
Bolivia	BO	Japan2	J2	Saudi Arabia	SA
Brazil	BR	Jordan	JO	Singapore	SG
Brunei Darussalam	BN	Kazakhstan	KZ	Slovak Republic	SK
Bulgaria	BG	North Korea	KP	Slovenia	SI
Canada	CA	Korea Republic	KR	South Africa	ZA
Chile	CL	Korea Republic2	K2	South Korea	KR
China	CN	Kuwait	KW	Spain	ES
Colombia	CO	Latvia	LV	Sweden	SE
Costa Rica	CR	Lebanon	LB	Switzerland	CH
Croatia	HR	Liechtenstein	LI	Syria	SY
Cyprus	CY	Lithuania	LT	Taiwan	TW
Czech Republic	CZ	Luxembourg	LU	Thailand	TH
Denmark	DK	Macau	MO	Turkey	TR
Dominican Republic	DO	Macedonia	MK	Ukraine	UA
Ecuador	EC	Malaysia	MY	United Arab Emirates	AE
Egypt	EG	Malta	MT	United Kingdom	GB
El Salvador	SV	Mexico	MX	United Kingdom 5.8 GHz	G1
Estonia	EE	Monaco	MC	United States	US
Finland	FI	Morocco	MA	United States World	UW
France	FR	Netherlands	NL	United States DFS	U1
Georgia	GE	New Zealand	NZ	Uruguay	UY
Germany	DE	Nicaragua	NI	Venezuela	VE
Greece	GR	Norway	NO	Vietnam	VN
Guam	GU	Oman	OM		
Guatemala	GT	Pakistan	PK		

Enable and Configure TX Power Control for the Wireless Interface

The TX Power Control feature lets the user configure the transmit power level of the card in the AP.

Perform the following commands to enable TX Power Control and set the transmit power level:

```
[Device-Name]>set txpowercontrol enable
```

```
[Device-Name]>set wif <interface number> currentbackofftpcvalue <0-9 dBm1-35 dBm>
```

Configure SSIDs (Network Names), VLANs, and Profiles

Perform the following command to configure SSIDs and VLANS, and to assign Security and RADIUS Profiles.

```
[Device-Name]>set wifssidtbl <Wireless Interface Index.SSID Index> ssid <Network Name>
vlanid <-1 to 1094> ssidauth <enable/disable> acctstatus <enable/disable> secprofile
<Security Profile Nmuber> radmacprofile <MAC Authentication Profile Name> radeapprofile
<EAP Authentication Profile Name> radacctprofile <Accounting Profile Name>
radmacauthstatus <enable/disable> aclstatus <enable/disable>
```

Example:
```
[Device-Name]>set wifssidtbl 3.1 ssid accesspt1 vlanid 22 ssidauth enable acctstatus
enable secprofile 1 radmacprofile "MAC Authentication" radeapprofile "EAP Authentication"
radacctprofile "Accounting" radmacauthstatus enable aclstatus enable
```

Download an AP Configuration File from your TFTP Server

Start the Solarwinds TFTP program (available on the installation CD), and click on the Security tab to verify that the TFTP server is configured to both transmit and receive files. (Note that TFTP programs other than Solarwinds may also require this setting.) Then enter the following commands:

```
[Device-Name]>set tftpfilename <file name> tftpfiletype config
         tftpipaddr <IP address of your TFTP server>
[Device-Name]>show tftp (to ensure the filename, file type, and the IP address are correct)
[Device-Name]>download *
[Device-Name]>reboot 0
```

After following the complete process (above) once, you can download a file of the same name (so long as all the other parameters are the same), with the following command:

```
[Device-Name]>download *
```

Backup your AP Configuration File

Start the Solarwinds TFTP program (available on the installation CD), and click on the Security tab to verify that the TFTP server is configured to both transmit and receive files. (Note that TFTP programs other than Solarwinds may also require this setting.) Then enter the following commands:

```
[Device-Name]>upload <TFTP Server IP address> <tftpfilename (such as "config.sys")> config
[Device-Name]>show tftp (to ensure the filename, file type, and the IP address are correct)
```

After setting the TFTP parameters, you can backup your current file (so long as all the other parameters are the same), with the following command:

```
[Device-Name]>upload *
```

Set up Auto Configuration

The Auto Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Perform the following commands to enable and set up automatic configuration:

NOTE: *The configuration filename and TFTP server IP address are configured only when the AP is configured for Static IP. If the AP is configured for Dynamic IP these parameters are not used and obtained from DHCP.*
The default filename is "config". The default TFTP IP address is "169.254.128.133".

```
[Device-Name]>set autoconfigstatus <enable/disable>
[Device-Name]>set autoconfigfilename <configuration file name>
[Device-Name]>set autoconfigTFTPaddr <TFTP IP address>
```

Other Network Settings

There are other configuration settings that you may want to set for the AP. Some of them are listed below.

- Configure the AP as a DHCP Server
- Configure the DNS Client
- Configure DHCP Relay and Configure DHCP Relay Servers
- Maintain Client Connections using Link Integrity
- Change Wireless Interface Settings
- Set Ethernet Speed and Transmission Mode
- Set Interface Management Services
- Configure Wireless Distribution System
- Configure MAC Access Control
- Set RADIUS Parameters
- Set Rogue Scan Parameters
- Set Hardware Configuration Reset Parameters
- Set VLAN/SSID Parameters
- Set Security Profile Parameters

NOTE: See Advanced Configuration *for more information on these settings.*

Configure the AP as a DHCP Server

NOTE: You must have at least one entry in the DHCP Server IP Address Pool Table before you can set the DHCP Server Status to Enable.

```
[Device-Name]>set dhcpstatus disable
[Device-Name]>set dhcpippooltbl 0 startipaddr <start ip address>
          endipaddr <end ip address>
[Device-Name]>set dhcpgw <gateway ip address>
[Device-Name]>set dhcppridnsipaddr <primary dns ip address>
[Device-Name]>set dhcpsecdnsipaddr <secondary dns ip address>
[Device-Name]>set dhcpstatus enable
[Device-Name]>reboot 0
```

CAUTION: Before enabling this feature, confirm that the IP address pools you have configured are valid addresses on the network and do not overlap the addresses assigned by any other DHCP server on the network. Enabling this feature with incorrect address pools will cause problems on your network.

Configure the DNS Client

```
[Device-Name]>set dnsstatus enable
[Device-Name]>set dnsprisvripaddr <IP address of primary DNS server>
[Device-Name]>set dnssecsvripaddr <IP address of secondary DNS server>
[Device-Name]>set dnsdomainname <default domain name>
[Device-Name]>show dns
```

```
[Device Name]> show dns
DNS Client Group
=================

dnsstatus       :      disable
dnsprisvripaddr :      0.0.0.0
dnssecsvripaddr :      0.0.0.0
dnsdomainname   :
```

Figure A-14 Results of "show dns" CLI command

Configure DHCP Relay

Perform the following command to enable or disable DHCP Relay Agent Status.

NOTE: *You must have at least one entry in the DHCP Relay Server Table before you can set the DHCP Relay Status to*
Enable.

```
[Device-Name]>set dhcprelaystatus enable
```

Configure DHCP Relay Servers

Perform the following command to configure and enable a DHCP Relay Server. The AP allows the configuration of a
maximum of 10 server settings in the DHCP Relay Agents server table.

```
[Device-Name]>set dhcprlyindex 1 dhcprlyipaddr <ip address> dhcprlycmt <comment>
dhcprlystatus 1 (1 to enable, 2 to disable, 3 to delete, 4 to create)
```

Maintain Client Connections using Link Integrity

```
[Device-Name]>show linkinttbl (this shows the current links)
[Device-Name]>set linkinttbl <1-5 (depending on what table row you wish to address)>
              ipaddr <ip address of the host computer you want to check>
[Device-Name]>set linkintpollint <the interval between link integrity checks>
[Device-Name]>set linkintpollretx <number of times to retransmit before considering the
link down>
[Device-Name]>set linkintstatus enable
[Device-Name]>show linkinttbl  (to confirm new settings)
[Device-Name]>reboot 0
```

Change Wireless Interface Settings

See Interfaces for information on the parameters listed below. The AP uses index 3.

Operational Mode

```
[Device-Name]>set wif 3 mode <see table>
```

Mode	Operational Mode
1	dot11b-only
2	dot11g-only
3	dot11bg
4	dot11a-only
5	dot11g-wifi

Autochannel Select (ACS)

ACS is enabled by default. Reboot after disabling or enabling ACS.

```
[Device-Name]>set wif 3 autochannel <enable/disable>
[Device-Name]>reboot 0
```

Enable/Disable Closed System

```
[Device-Name]>set wif 3 closedsys <enable/disable>
```

Shutdown/Resume Wireless Service

[Device-Name]>**set wif 3 wssstatus <1 (resume)/2 (shutdown)>**

Set Load Balancing Maximum Number of Clients

[Device-Name]>**set wif 3 lbmaxclients <1-63>**

Set the Multicast Rate (802.11a/b/g)

[Device-Name]>**set wif 3 multrate <6, 12, 24** (Mbits/sec)**>**

Enable/Disable Super Mode (802.11a/g only)

[Device-Name]>**set wif 3 supermode <enable/disable>**

Enable/Disable Turbo Mode (802.11a/g only)

[Device-Name]>**set wif 3 turbo <enable/disable>**

NOTE: Super mode must be enabled on the interface before Turbo mode can be enabled.

Configure Antenna Diversity

[Device-Name]>**set wif 3 atdiversity <1, 2, 5(auto)>** (see below)

[Device-Name]>**reboot 0**

Value	Corresponding Antenna Enabled
1	802.11a/b/g (connector 1)
2	802.11a/b/g (connector 2)
5 (auto)	Both antennas

NOTE: See Antennas for more information on internal and external antenna ports.

Set the Distance Between APs

[Device-Name]>**set wif 3 distaps <1-5>** (see below)

[Device-Name]>**reboot 0**

Value	Distance Between APs
1	Large
2	Medium
3	Small
4	Mini
5	Micro

Set Ethernet Speed and Transmission Mode

```
[Device-Name]>set etherspeed <value> (see below)
[Device-Name]>reboot 0
```

Ethernet Speed and Transmission Mode	Value
10 Mbits/sec - half duplex	10halfduplex
10 Mbits/sec - full duplex	10fullduplex
10 Mbits/sec - auto duplex	10autoduplex
100 Mbits/sec - half duplex	100halfduplex
100 Mbits/sec - full duplex	100fullduplex
Auto Speed - half duplex	autohalfduplex
Auto Speed - auto duplex	autoautoduplex (default)

Set Interface Management Services

Edit Management IP Access Table

```
[Device-Name]>set mgmtipaccesstbl <index> ipaddr <IP address> ipmask <subnet mask>
```

Configure Management Ports

```
[Device-Name]>set snmpifbitmask <(see below)>
[Device-Name]>set httpifbitmask <(see below)>
[Device-Name]>set telifbitmask <(see below)>
```

Choose from the following values:

Interface Bitmask	Description
0 or 2 = Disable (all interfaces)	All management channels disabled
1 or 3 = Ethernet only	Ethernet only enabled
4 or 6 = Wireless only	Wireless A only enabled
5 or 7 = Enable all interfaces	All management channels enabled

Set Communication Ports

```
[Device-Name]>set httpport <HTTP port number (default is 80)>
[Device-Name]>set telport <Telnet port number (default is 23)>
```

Configure Secure Socket Layer (HTTPS)

Enabling SSL and configuring a passphrase allows encrypted Secure Socket Layer communications to the AP through the HTTPS interface.

```
[Device-Name]>set sslstatus <enable/disable>
```

The user must change the SSL passphrase when uploading a new certificate/private key pair, which will have a corresponding passphrase.

```
[Device-Name]>set sslpassphrase <SSL certificate passphrase>
[Device-Name]>show http (to view all HTTP configuration information including SSL.)
```

Set Telnet Session Timeouts

```
[Device-Name]>set tellogintout <time in seconds between 1 and 300 (default is 30)>
[Device-Name]>set telsessiontout <time in seconds between 1 and 36000 (default is 900)>
```

Configure Serial Port Interface

NOTE: To avoid unexpected performance issues, leave Flow Control at the default setting (none) unless you are sure what this setting should be.

```
[Device-Name]>set serbaudrate <2400, 4800, 9600, 19200, 38400, 57600>
[Device-Name]>set serflowctrl <none, xonxoff>
[Device-Name]>show serial
```

```
[Device Name]> show serial
Serial Interface Group Parameters
=================================

serbaudrate          :     9600
serdatabits          :     8
serparity            :     none
serstopbits          :     1
serflowctrl          :     none
```

Figure A-15 Result of "show serial" CLI Command

Configure Syslog

```
[Device-Name]>set syslogpriority <1–7 (default is 6)>
[Device-Name]>set syslogstatus <enable/disable>
[Device-Name]>set sysloghbstatus <enable/disable> (default is disable)
[Device-Name]>set sysloghbinterval <1–604800> (default is 900 seconds)
[Device-Name]>set sysloghosttbl <index> ipaddr <ipaddress> cmt <comment> status
<enable/disable>
```

Configure Intra BSS

```
[Device-Name]>set intrabssoptype <passthru (default)/block)>
```

Configure Wireless Distribution System

Create/Enable WDS

```
[Device-Name]>set wdstbl <Index> partnermacaddr <MAC Address> status enable
```

Enable/Disable WDS

```
[Device-Name]>set wdstbl <Index> status <enable/disable>
```

NOTE: <Index> is 3.1–3.6. To determine the index, type show wdstbl at the prompt.

NOTE: When WDS is enabled, spanning tree protocol is automatically enabled. It may be manually disabled. If Spanning Tree protocol is enabled by WDS and WDS is subsequently disabled, Spanning tree will remain enabled until it is manually disabled. See Spanning Tree Parameters.

Configure MAC Access Control

Setup MAC (Address) Access Control

```
[Device-Name]>set wifssidtbl <index> aclstatus enable/disable
[Device-Name]>set macacloptype <passthru, block>
[Device-Name]>reboot 0
```

Add an Entry to the MAC Access Control Table

```
[Device-Name]>set macacltbl 0 macaddr <MAC Address> status enable
[Device-Name]>show macacltbl
```

Disable or Delete an Entry in the MAC Access Control Table

```
[Device-Name]>set macacltbl <index> status <disable/delete>
[Device-Name]>show macacltbl
```

NOTE: *For larger networks that include multiple Access Points, you may prefer to maintain this list on a centralized location using the RADIUS parameters (see* *).*

Set RADIUS Parameters

Configure RADIUS Authentication servers

Perform the following command to configure a RADIUS Server and assign it to a VLAN. The RADIUS Server Profile index is specified by the index parameter and the subindex parameter specifies whether you are configuring a primary or secondary RADIUS server.

```
[Device-Name]>set radiustbl <Index> profname <Profile Name> seraddrfmt <1 - IP Address 2
- Name> sernameorip <IP Address or Name> port <value> ssecret <value> responsetm <value>
maxretx <value> acctupdtintrvl <value> macaddrfmt <value> authlifetm <value>
radaccinactivetmr <value> vlanid <vlan id -1 to 4094> status enable
```

NOTE: *To create a new RADIUS profile, use 0 for* `<Index>`*.*

Examples of Configuring Primary and Secondary RADIUS Servers and Displaying the RADIUS Configuration

Primary server configuration:

```
[Device-Name]>set radiustbl 1.1 profname "MAC Authentication" seraddrfmt 1 sernameorip
20.0.0.20 port 1812 ssecret public responsetm 3 maxretx 3 acctupdtintrvl 0 macaddrfmt 1
authlifetm 900 radaccinactivetmr 5 vlanid 22 status enable
```

Secondary server configuration:

```
[Device-Name]>set radiustbl 1.2 profname "MAC Authentication" seraddrfmt 1 sernameorip
20.0.0.30 port 1812 ssecret public responsetm 3 maxretx 3 acctupdtintrvl 0 macaddrfmt 1
authlifetm 900 radaccinactivetmr 5 vlanid 33 status enable
```

```
[Device-Name]>show radiustbl

Index                         : 1
Primary/Backup                : Primary
Profile Name                  : MAC Authentication
Server Status                 : notReady
Server Addressing Format      : ipaddr
IP Address/Host Name          : 0.0.0.0
Destination Port              : 1812
VLAN Identifier               : -1
MAC Address Format            : dashdelimited
Response Time                 : 3
Maximum Retransmission        : 3
Authorization Lifetime        : 0
Accounting Update Interval    : 0
Accounting Inactivity Timer   : 5
```

```
Index                       : 1
Primary/Backup              : Backup
Profile Name                : MAC Authentication
Server Status               : notReady
Server Addressing Format    : ipaddr
IP Address/Host Name        : 0.0.0.0
Destination Port            : 1812
VLAN Identifier             : -1
MAC Address Format          : dashdelimited
Response Time               : 3
Maximum Retransmission      : 3
.

.

.

Index                       : 4
Primary/Backup              : Backup
Profile Name                : Management Access
Server Status               : notReady
Server Addressing Format    : ipaddr
IP Address/Host Name        : 0.0.0.0
Destination Port            : 1812
VLAN Identifier             : -1
MAC Address Format          : dashdelimited
Response Time               : 3
Maximum Retransmission      : 3
Authorization Lifetime      : 0
Accounting Update Interval  : 0
Accounting Inactivity Timer : 5
```

Figure A-16 Result of "showradiustbl" CLI Command

Set Rogue Scan Parameters

Perform the following command to enable or disable Rogue Scan on a wireless interface and configure the scanning parameters.

The **cycletime** parameter is only configured for background scanning mode.

```
[Device-Name]>set rscantbl 3 mode <1 for background scanning, 2 for continuous scanning>
cycletime <cycletime from 1–1440 minutes> status <enable/disable>
```

NOTE: Rogue Scan cannot be enabled on a wireless interface when the Wireless Service Status on that interface is shutdown. First, resume service on the wireless interface.

Set Hardware Configuration Reset Parameters

The Hardware Configuration Reset commands allows you to enable or disable the hardware reset functionality and to change the password to be used for configuration reset during boot up.

To disable hardware configuration reset, enter:

```
[Device-Name]>set hwconfigresetstatus disable
```

To enable hardware configuration reset, enter:

```
[Device-Name]>set hwconfigresetstatus enable
```

To define the Configuration Reset Password to be used for configuration reset during boot up, enter the following command

```
[Device-Name]>set configresetpasswd <password>
```

It is important to safely store the

NOTE: *It is important to safely store the configuration reset password. If a user forgets the configuration reset password, the user will be unable to reset the AP to factory default configuration if the AP becomes inaccessible and the hardware configuration reset functionality is disable.*

Set VLAN/SSID Parameters

Enable VLAN Management

```
[Device-Name]>set vlanstatus enable
[Device-Name]>set vlanmgmtid <1–4094>
```

```
[Device-Name]>show wifssidtbl (to review your settings)
[Device-Name]>reboot 0
```

Disable VLAN Management

```
[Device-Name]>set vlanstatus disable or
[Device-Name]>set vlanmgmtid -1
[Device-Name]>reboot 0
```

Add a Entry to the WIFSSID Table

```
[Device-Name]>set wifssidtbl <index> ssid <Network Name> vlanid <-1 (untagged) or 1–4094>
status enable
```

Set Security Profile Parameters

Configure a Security Profile with Non Secure Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode nonsecure status enable
```

Example:
```
[Device-Name]>set secprofiletbl 2 secmode nonsecure status enable
```

Configure a Security Profile with WEP Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode wep encryptkey<0-3> <value>
encryptkeylength <value> encryptkeytx <value> status enable
```

Example:
```
[Device-Name]>set secprofiletbl 3 secmode wep encryptkey0 12345 encryptkeylength 1
encryptkeytx 0 status enable
```

Configure a Security Profile with 802.1x Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode 802.1x encryptkeylength <value> status
enable
```

Example:
```
[Device-Name]>set secprofiletbl 4 secmode 802.1x encryptkeylength 1 status enable
```

Configure a Security Profile with WPA Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode wpa status enable
```

Example:
```
[Device-Name]>set secprofiletbl 5 secmode wpa status enable
```

Configure a Security Profile with WPA-PSK Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode wpa-psk passphrase <value> status enable
```

Example:
```
[Device-Name]>set secprofiletbl 6 secmode wpa-psk passphrase 12345678 status enable
```

Configure a Security Profile with 802.11i Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode 802.11i status enable
```

Example:
```
[Device-Name]>set secprofiletbl 7 secmode 802.11i status enable
```

Configure a Security Profile with 802.11i-PSK Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode 802.11i-psk passphrase <value> status enable
```

Example:
```
[Device-Name]>set secprofiletbl 8 secmode 802.11i-psk passphrase 12345678 status enable
```

CLI Monitoring Parameters

Using the **show** command with the following table parameters will display operating statistics for the AP (these are the same statistics that are described in the Monitoring section).

* **staticmp:** Displays the ICMP statistics.
* **statarptbl:** Displays the IP ARP Table statistics.
* **statbridgetbl:** Displays the Learn Table.
* **statiapp:** Displays the IAPP statistics.
* **statradius:** Displays the RADIUS Authentication statistics.
* **statif:** Displays information and statistics about the Ethernet and wireless interfaces.
* **stat802.11:** Displays additional statistics for the wireless interfaces.
* **statethernet:** Displays additional statistics for the Ethernet interface.
* **statmss:** Displays station statistics and Wireless Distribution System links.

Parameter Tables

Objects contain groups that contain both parameters and parameter tables. Use the following Tables to configure the Access Point. Columns used on the tables include:

• Name - Parameter, Group, or Table Name

• Type - Data type

• Value - Value range, and default value, if any

• Access = access type, R = Read Only (show), RW = Read-Write (can be "set"), W = Write Only

• CLI Parameter - Parameter name as used in the Access Point

Access Point network objects are associated with Groups. The network objects are listed below and associated parameters are described in the following Parameter Tables:

• System Parameters - Access Point system information
  – Inventory Management Information - Hardware, firmware, and software version information
• Network Parameters - IP and Network Settings
  – IP Configuration Parameters - Configure the Access Point's IP settings
    • DNS Client for RADIUS Name Resolution - Configure the Access Point as a DNS client
  – DHCP Server Parameters - Enable or disable dynamic host configuration
  – SNTP Parameters - Configure
  – Link Integrity Parameters - Monitor link status
• Interface Parameters - Configure Wireless and Ethernet settings
  – Wireless Interface Parameters
    • Wireless Distribution System (WDS) Parameters - Configure the WDS partnerships
  – Wireless Interface SSID/VLAN/Profile Parameters - Configure the SSIDs, VLANs, and security modes. Up to 16 SSIDs are supported; different security settings can be applied to each SSID, and a unique VLAN can be configured per SSID.
  – Ethernet Interface Parameters - Set the speed and duplex of the Ethernet port.
• Management Parameters - Control access to the AP's management interfaces
  – SNMP Parameters - Set read and read/write passwords
  – HTTP Parameters - Set up the graphical web browser interface. If required, enable SSL and configure the SSL certificate passphrase.
  – Telnet Parameters - Telnet Port setup
  – Serial Port Parameters - Serial Port setup
  – RADIUS Based Management Access Parameters - Configure RADIUS Based Management Access for HTTP and Telnet access.
  – SSH Parameters - Enable SSH and configure the host key.
  – TFTP Server Parameters - Set up for file transfers; specify IP Address, file name, and file type
  – IP Access Table Parameters - Configure range of IP addresses that can access the AP
  – Auto Configuration Parameters - Configure the Auto Configuration feature which allows an AP to be automatically configured by downloading a configuration file from a TFTP server during boot up.
• Filtering Parameters
  – Ethernet Protocol Filtering Parameters - Control network traffic based on protocol type
  – Static MAC Address Filter Table - Enable and disable specific addresses
  – Proxy ARP Parameters - Enable or disable proxy ARP for wireless clients
  – IP ARP Filtering Parameters - Control which ARP messages are sent to wireless clients based on IP settings
  – Broadcast Filtering Table - Control the type of broadcast packets forwarded to the wireless network

- – TCP/UDP Port Filtering - Filter IP packets based on TCP/UDP port
- Alarms Parameters
  - – SNMP Table Host Table Parameters - Enter the list of IP addresses that will receive alarms from the AP
  - – Syslog Parameters - Configure the AP to send Syslog information to network servers
- Bridge Parameters
  - – Spanning Tree Parameters - Used to help prevent network loops
  - – Storm Threshold Parameters - Set threshold for number of broadcast packets
  - – Intra BSS Subscriber Blocking - Enable or disable peer to peer traffic on the same AP
  - – Packet Forwarding Parameters - Redirect traffic from wireless clients to a specified MAC address
- RADIUS Parameters
  - – Set RADIUS Parameters - Configure RADIUS Servers and assign them to VLANs.
- Security Parameters - Access Point security settings
  - – MAC Access Control Parameters - Control wireless access based on MAC address
  - – Rogue Scan Configuration Table - Enable and configure Rogue Scan to detect Rogue APs and clients.
  - – 802.1x Parameters - Configure 802.1X Supplicant Timeout parameter
  - – Hardware Configuration Reset - Disable or enable hardware configuration reset and configure a configuration reset password.
  - – Other Parameters - Configure Security Profiles that define allowed security modes (wireless clients), and encryption and authentication mechanisms.
- VLAN/SSID Parameters - Enable the configuration of multiple subnetworks based on VLAN ID and SSID.
- Other Parameters
  - – IAPP Parameters - Enable or disable the Inter-Access Point Protocol
  - – Wireless Multimedia Enhancements (WME)/Quality of Service (QoS) parameters - Enable and configure Wireless Multimedia Enhancement/Quality of Service parameters, QoS policies, mapping priorities, and EDCA parameters. Apply a configured QoS policy to a particular SSID.

System Parameters

Name	Type	Value	Access	CLI Parameter
System	Group	N/A	R	system
Name	DisplayString	User Defined	RW	sysname
Location	DisplayString	User Defined	RW	sysloc
Country Identifier*	DisplayString	See Country Identifiers below	RW	sysworldcountrycode
Contact Name	DisplayString	User Defined	RW	sysctname
Contact E-mail	DisplayString	User Defined	RW	sysctemail
Contact Phone	DisplayString	User Defined max 254 characters	RW	sysctphone
FLASH Backup Interval	Integer	0 - 65535 seconds	RW	sysflashbckint
Flash Update		0 1	RW	sysflashupdate
System OID	DisplayString	N/A	R	sysoid
Descriptor	DisplayString	System Name, flash version, S/N, bootloader version	R	sysdescr
Up Time	Integer	dd:hh:mm:ss dd - days hh - hours mm - minutes ss - seconds	R	sysuptime
System Security ID	DisplayString	Retrieved from flash ID	R	sysinvmgmtsecurityid
Emergency Restore to defaults		Resets all parameters to default factory values	RW	sysresettodefaults Note: You must enter the following command twice to reset to defaults: **set sysresettodefaults 1**

* Available only on APs with model numbers ending in -WD. When available, this object must be configured before any interface parameters can be set.

Country Identifiers

NOTE: All countries may not be available on your AP.

Country	Indoor/Outdoor	Identifier
Austria	Indoor	AT1
	Outdoor	AT2
Belgium	Indoor	BE1
	Outdoor	BE2
Cyprus	Indoor	CY1
	Outdoor	CY2
Czech Republic	Indoor	CZ1
	Outdoor	CZ2
Denmark	Indoor	DK1
	Outdoor	DK2
Estonia	Indoor	EE1
	Outdoor	EE2

Country	Indoor/Outdoor	Identifier
Finland	Indoor	FI1
	Outdoor	FI2
France	Indoor	FR1
	Outdoor	FR2
Germany	Indoor	DE1
	Outdoor	DE2
Greece	Indoor	GR1
	Outdoor	GR2
Hungary	Indoor	HU1
	Outdoor	HU2
Ireland	Indoor	IE1
	Outdoor	IE2
Italy	Indoor	IT1
	Outdoor	IT2
Latvia	Indoor	LV1
	Outdoor	LV2
Lithuania	Indoor	LT1
	Outdoor	LT2
Luxembourg	Indoor	LU1
	Outdoor	LU2
Malta	Indoor	MT1
	Outdoor	MT2
Netherlands	Indoor	NL1
	Outdoor	NL2
Norway	Indoor	NO1
	Outdoor	NO2
Poland	Indoor	PL1
	Outdoor	PL2
Portugal	Indoor	PT1
	Outdoor	PT2
Puerto Rico	Indoor	PR1
	Outdoor	PR2
Russia	Indoor/Outdoor	RU
Spain	Indoor	ES1
	Outdoor	ES2
Sweden	Indoor	SE1
	Outdoor	SE2
Switzerland	Indoor	CH1
	Outdoor	CH2
United Kingdom/ Great Britain	Indoor	GB1
	Outdoor	GB2

Inventory Management Information

The inventory management commands display advanced information about the AP's installed components. You may be asked to report this information to a representative if you contact customer support.

Name	Type	Value	Access	CLI Parameter
System Inventory Management	Subgroup	N/A	R	sysinvmgmt
Component Table	Subgroup	N/A	R	sysinvmgmtcmptbl
Component Interface Table	Subgroup	N/A	R	sysinvmgmtcmpiftbl

Network Parameters

IP Configuration Parameters

Name	Type	Value	Access	CLI Parameter
Network	Group	N/A	R	network
IP Configuration	Group	N/A	R	ip (Note: The **network** and **ip** parameters display the same information)
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Default Router IP Address	IpAddress	User Defined	RW	ipgw
Default TTL	Integer	User Defined (seconds) 0 - 255, 64 (default)	RW	ipttl
Address Type	Integer	static dynamic (default)	RW	ipaddrtype

NOTE: *The IP Address Assignment Type (ipaddrtype) must be set to static before the IP Address (ipaddr), IP Mask (ipmask) or Default Gateway IP Address (ipgw) values can be entered.*

DNS Client for RADIUS Name Resolution

Name	Type	Value	Access	CLI Parameter
DNS Client	Group	N/A	R	dns
DNS Client status	Integer	enable disable (default)	RW	dnsstatus
Primary DNS Server IP Address	IpAddress	User Defined	RW	dnspridnsipaddr
Secondary DNS Server IP Address	IpAddress	User Defined	RW	dnssecdnsipaddr
Default Domain Name	Integer32	User Defined (up to 254 characters)	RW	dnsdomainname

DHCP Server Parameters

Name	Type	Value	Access	CLI Parameter
DHCP Server	Group	N/A	R	dhcp
DHCP Server Status*	Integer	enable (1) (default) disable (2) delete (3)	RW	dhcpstatus
Gateway IP Address	IpAddress	User Defined	RW	dhcpgw
Primary DNS IP Address	IpAddress	User Defined	RW	dhcppridnsipaddr
Secondary DNS IP Address	IpAddress	User Defined	RW	dhcpsecdnsipaddr
Number of IP Pool Table Entries	Integer32	N/A	R	dhcpippooltblent

* The DHCP Server (dhcpstatus) can only be enabled after a DHCP IP Pool table entry has been created.

DHCP Server table for IP pools

Name	Type	Value	Access	CLI Parameter
DHCP Server IP Address Pool Table	Table	N/A	R	dhcpippooltbl
Table Index	Integer	User Defined	N/A	index
Start IP Address*	IpAddress	User Defined	RW	startipaddr
End IP Address*†	IpAddress	User Defined	RW	endipaddr
Width†	Integer	User Defined	RW	width
Default Lease Time (optional)	Integer32	300 - 86400 sec (default)	RW	defleasetm
Maximum Lease Time (optional)	Integer32	300 - 86400 sec (default)	RW	maxleasetm
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

* IP addresses must be from within the same subnet as the AP.

† Set End IP Address or Width, but not both.

DHCP Relay Group

The DHCP Relay Group allows you to enable or disable DHCP Relay Agent Status.

Name	Type	Value	Access	CLI Parameter
DHCP Relay Group	Group	N/A	R	dhcprelay
Status	Integer	enable disable	RW	dhcprelaystatus
DHCP Relay Server Table	Table	N/A	R	dhcprelaytbl

DHCP Relay Server Table

The DHCP Relay Server Table contains the commands to set the table entries. The AP supports the configuration of a maximum of 10 server settings in the DHCP Relay Agents server table.

Name	Type	Value	Access	CLI Parameter
DHCP Relay Server Table	Table	N/A	R	dhcprelaytbl
DHCP Relay Server Table Entry Index	Integer32	1 - 10	R	dhcprlyindex
DHCP Relay Server Table Entry IP Address	IpAddress	User Defined	RW	dhcprlyipaddr
DHCP Relay Server Table Entry Comment	DisplayString	User Defined	RW	dhcprlycmt
DHCP Relay Server Table Entry Status	Integer	enable (1) disable (2) delete (3) create (4)	RW	dhcprlystatus

SNTP Parameters

Name	Type	Value	Access	CLI Parameter
SNTP Group	Group	N/A	R	sntp
SNTP Status	Integer	enable disable	RW	sntpstatus
Primary Server Name or IP Address	DisplayString	0 - 255 characters	RW	sntpprisvr
Secondary Server Name or IP Address	DisplayString	0 - 255 characters	RW	sntpsecsvr
Time Zone	Integer	See MIB for requirements	RW	sntptimezone
Daylight Savings Time	Integer	-2 -1 0 +1 +2	RW	sntpdaylightsaving
Year	Integer32	N/A	RW	sntpyear
Month	Integer32	1 - 12	RW	sntpmonth
Day	Integer32	1 - 31	RW	sntpday
Hour	Integer32	0 - 23	RW	sntphour
Minutes	Integer32	0 - 59	RW	sntpmins
Seconds	Integer32	0 - 59	RW	sntpsecs
Addressing Format	Integer	ipaddress name	RW	sntpaddrfmt

Link Integrity Parameters

Name	Type	Value	Access	CLI Parameter
Link Integrity	Group	N/A	R	linkint
Link Integrity Status	Integer	enable disable (default)	RW	linkintstatus
Link Integrity Poll Interval	Integer	500 - 15000 ms (in increments of 500ms) 500 ms (default)	RW	linkintpollint
Link Integrity Poll Retransmissions	Integer	0 - 255 5 (default)	RW	linkintpollretx

Link Integrity IP Target Table

Name	Type	Value	Access	CLI Parameter
Link Integrity IP Target Table	Table	N/A	R	linkinttbl
Table Index	Integer	1 - 5	N/A	index
Target IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined (up to 254 characters)	RW	cmt
Status (optional)	Integer	enable disable (default) delete	RW	status

Interface Parameters

Wireless Interface Parameters

The wireless interface group parameter is **wif**. The wireless interface uses table index 3.

Common Parameters to 802.11a and 802.11b/g

Name	Type	Value	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Table Index	Integer	3	R	index
Operational Mode	Integer	1 = dot11b-only 2 = dot11g-only 3 = dot11bg 4 = dot11a 5 = dot11g-wifi	RW	mode
Network Name	DisplayString	1 - 32 characters My Wireless Network (default)	RW	netname
Auto Channel Select (ACS)*	Integer	enable (default) disable	RW	autochannel
DTIM Period	Integer	1 - 255 1 = default	RW	dtimperiod
RTS/CTS Medium Reservation	Integer	0 - 2347 Default is 2347 (off)	RW	medres
MAC Address	PhyAddress	12 hex digits	R	macaddr
Wireless Service Status†	Integer	1 = resume 2 = shutdown	RW	wssstatus
Supported Frequency Channels	Octet String	Depends on Regulatory Domain	R	suppchannels
Load Balancing Max Clients	Integer	1 - 63	RW	lbmaxclients
Distance Between APs‡	Integer	1 (large) (default) 2 (medium) 3 (small) 4 (minicell) 5 (microcell)	RW	distaps
Transmit Power Control	Integer	enable disable	RW	txpowercontrol
Transmit Power Control Back-Off	Integer	0 - 35 (dBm)	RW	currentbackofftpcvalue
Antenna Diversity	Integer	1 (Antenna 1) 2 (Antenna 2) 5 (Auto; both antennas) (See Configure Antenna Diversity)	RW	atdiversity

* For 802.11a APs certified in the ETSI and TELEC regulatory domains and operating in the middle frequency band, disabling Auto Channel Select will limit the available channels to those in the lower frequency band.

† Wireless Service Status cannot be shut down on an interface where Rogue Scan is enabled.

‡ Distance Between APs allows the AP to perform better in high noise environments by increasing the receive sensitivity and transmit defer threshold, as follows:

Distance Between APs	Receive Sensitivity Threshold (dBm)	Transmit Defer Threshold (dBm)
Large	-96	-62

Distance Between APs	Receive Sensitivity Threshold (dBm)	Transmit Defer Threshold (dBm)
Medium	-86	-62
Small	-78	-52
Mini	-70	-42
Micro	-62	-36

802.11a Specific Parameters

Name	Type	Value	Access	CLI Parameter
Operating Frequency Channel	Integer	Varies by regulatory domain and country. See Available Channels	RW	channel
Supported Data Rates	Octet String	See Transmit Rate, below	R	suppdatarates
Transmit Rate	Integer32	0 (Auto Fallback) 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec	RW	txrate
Physical Layer Type	Integer	ofdm (orthogonal frequency division multiplexing)	R	phytype
Regulatory Domain List	DisplayString	Varies by regulatory domain: USA -- FCC Hong Kong -- HK Australia -- AU Europe -- ETSI Russia -- RU Japan -- TELEC Singapore -- IDA Taiwan -- TW China -- CN Asia Brazil Argentina Saudi Arabia World Mode -- WO Undefined	R	regdomain
Super Mode	Integer	enable disable (default)	RW	supermode
Turbo Mode*†	Integer	enable disable (default)	RW	turbo

* Available for the 5 GHz frequency band in the FCC regulatory domain only.

† Super mode must be enabled before Turbo mode can be enabled.

802.11b Specific Parameters

Name	Type	Value	Access	CLI Parameter
Operating Frequency Channel	Integer	1 - 14; available channels vary by regulatory domain/country; see Available Channels	RW	channel
Multicast Rate	Integer	1 Mbits/sec (1) 2 Mbits/sec (2) (default) 5.5 Mbits/sec (3) 11 Mbits/sec (4)	RW	multrate
Closed Wireless System	Integer	enable disable (default)	RW	closedsys
MAC Address	PhyAddress	12 hex digits	R	macaddr
Supported Data Rates	Octet String	1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	R	suppdatarates
Transmit Rate	Integer32	0 (auto fallback; default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	RW	txrate
Physical Layer Type	Integer	dsss (direct sequence spread spectrum) for 802.11b	R	phytype
Regulatory Domain List	DisplayString	Varies by regulatory domain: U.S./Canada -- FCC Europe -- ETSI Japan -- TELEC	R	regdomain

802.11b/g Specific Parameters

Name	Type	Value	Access	CLI Parameter
Operating Frequency Channel	Integer	1 - 14; available channels vary by regulatory domain/country; see Available Channels	RW	channel
Supported Data Rates	Octet String	See Transmit Rate, below	R	suppdatarates

Name	Type	Value	Access	CLI Parameter
Transmit Rate	Integer32	**For 802.11b-only mode:** 0 (auto fallback; default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec **For 802.11g-only mode:*** 0 (auto fallback; default) 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec **For 802.11b/g mode:** 0 (auto fallback; default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec	RW	txrate
Physical Layer Type	Integer	ERP (Extended Rate Protocol)	R	phytype
Regulatory Domain List	DisplayString	Varies by regulatory domain: USA -- FCC Europe -- ETSI Russia -- RU Japan -- TELEC Brazil Argentina Saudi Arabia Israel -- IL World Mode -- WO Undefined	R	regdomain
Super Mode†	Integer	enable disable (default)	RW	supermode

* Also for 802.11g-wifi mode. 802.11g-wifi has been defined for Wi-Fi testing purposes; it is not recommended for use in your wireless network environment.

† Available in 802.11b/g or 802.11g modes only.

Wireless Distribution System (WDS) Parameters

Name	Type	Value	Access	CLI Parameter
WDS Table	Table	N/A	R	wdstbl
Port Index	Integer	3.1 - 3.6 (Wireless)	R	portindex
Status	Integer	enable, disable	RW	status
Partner MAC Address	PhysAddress	User Defined	RW	partnermacaddr

Wireless Distribution System (WDS) Security Table Parameters

The WDS Security Table manages WDS related security objects.

Name	Type	Value	Access	CLI Parameter
WDS Security Table	Table	N/A	R	wdssectbl
Table Index	Integer	3	R	index
Security Mode	Integer	1 or none 2 or wep 3 or aes	RW	secmode
Shared Secret	DisplayString	6–32 characters	W	sharedsecret
Encryption Key 0	WEPKeyType	N/A	W	encryptkey0

Wireless Interface SSID/VLAN/Profile Parameters

The Wireless Interface SSID table manages the SSIDs, VLANs, Security Profiles, and RADIUS Profiles associated to each SSID.

For configuration examples, see Configure SSIDs (Network Names), VLANs, and Profiles.

Name	Type	Value	Access	CLI Parameter
Wireless Interface SSID Table	Table	N/A	R	wifssidtbl
Table Index	Integer	3	R	index
SSID Table Index	Integer32	1 - 16 (SSID index)	R	ssidindex
SSID	DisplayString	2 - 32 characters	RW	ssid
Broadcast Unique Beacon	Integer	enable disable	RW	bcastbeacon
Closed System	Integer	enable, disable	RW	denybcastprobereq
VLAN ID	VlanId	-1 - 4094 or untagged	RW	vlanid
Rekeying Interval	Integer32	0 (disabled) 300 - 65535 *Default = 900*	RW	reykeyint
Table Row Status	RowStatus	enable disable delete	RW	status
SSID Authorization Status per VLAN	Integer	enable disable	RW	ssidauth
RADIUS Accounting Status per VLAN	Integer	enable disable	RW	acctstatus
MAC ACL Status per VLAN	Integer	enable disable	RW	aclstatus
Security Profile	Integer32	User defined	RW	secprofile
RADIUS MAC Profile	DisplayString	User defined	RW	radmacprofile

Name	Type	Value	Access	CLI Parameter
RADIUS EAP Profile	DisplayString	User defined	RW	radeapprofile
RADIUS Accounting Profile	DisplayString	User defined	RW	radacctprofile
QoS Policy	Integer32	User defined	RW	qospolicy

Ethernet Interface Parameters

Name	Type	Value	Access	CLI Parameter
Ethernet Interface	Group	N/A	R	ethernet
Speed	Integer	1 (10halfduplex) 2 (10fullduplex) 3 (10autoduplex) 4 (100halfduplex) 5 (100fullduplex) 6 (autohalfduplex) 7 (autoautoduplex) (default)	RW	etherspeed
MAC Address	PhyAddress	N/A	R	ethermacaddr

Management Parameters

Secure Management Parameters

Name	Type	Value	Access	CLI Parameter
Secure Management	Integer	1 (enable) 2 (disable)	RW	securemgmtstatus

SNMP Parameters

Name	Type	Value	Access	CLI Parameter
SNMP	Group	N/A	R	snmp
SNMP Management Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless 5 or 7 = All interfaces (default is 7)	RW	snmpifbitmask
Read Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmprpasswd
Read/Write Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmprwpasswd
SNMPv3 Authentication Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmpv3authpasswd
SNMPv3 Privacy Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmpv3privpasswd

HTTP Parameters

Name	Type	Value	Access	CLI Parameter
HTTP	Group	N/A	R	http
HTTP Management Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless 5 or 7 = All interfaces (default is 7)	RW	httpifbitmask
HTTP Password	DisplayString	User Defined (6 - 32 characters)	W	httppasswd
HTTP Port	Integer	User Defined Default = 80	RW	httpport
Help Link*	DisplayString	User Defined	RW	httphelplink
SSL Status	Integer	enable/disable	RW	sslstatus
SSL Certificate Passphrase	DisplayString	User Defined	W	sslpassphrase

* The help link must be set to an HTTP address. Use the forward slash character ("/") rather than the backslash character ("\") when configuring the Help Link location.

Telnet Parameters

Name	Type	Value	Access	CLI Parameter
Telnet	Group	N/A	R	telnet
Telnet Management Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless 5 or 7 = All interfaces (default is 7)	RW	telifbitmask
Telnet Port	Integer	User Defined 23 (default)	RW	telport
Telnet Login Inactivity Time-out	Integer	30 - 300 seconds 60 sec (default)	RW	tellogintout
Telnet Session Idle Time-out	Integer	60 - 36000 seconds 900 sec (default)	RW	telsessiontout

Serial Port Parameters

Name	Type	Value	Access	CLI Parameter
Serial	Group	N/A	R	serial
Baud Rate	Integer	2400, 4800,9600 (default), 19200, 38400, 57600	RW	serbaudrate
Data Bits	Integer	8	R	serdatabits
Parity	Integer	none	R	serparity
Stop Bits	Integer	1	R	serstopbits
Flow Control	Value	none (default) xonxoff	RW	serflowctrl

RADIUS Based Management Access Parameters

The RADIUS Based Management Access parameters allow you to enable HTTP or Telnet Radius Management Access, enable or disable local user access, and configure the local user password.

The default local user ID is **root** and the default local user password is **public**. "Root" cannot be configured as a valid user for RADIUS based management access when local user access is enabled.

Name	Type	Value	Access	CLI Parameter
Radius Local User Status	Integer	enable disable	RW	radlocaluserstatus
Radius Local User Password	DisplayString	User Defined	RW	radlocaluserpasswd
HTTP Radius Management Access	Integer	enable disable	RW	httpradiusmgmtaccess
Telnet Radius Management Access	Integer	enable disable	RW	telradiusmgmtaccess

SSH Parameters

The following commands enable or disable SSH and set the SSH host key.

Name	Type	Value	Access	CLI Parameter
SSH Status	Integer	enable disable	RW	sshstatus

Name	Type	Value	Access	CLI Parameter
SSH Public Host Key Fingerprint	DisplayString	AP Generated	RW	sshkeyfprint
SSH Host Key Status	Integer	create delete	RW	sshkeystatus

The AP SSH feature, open-SSH, confirms to the SSH protocol, and supports SSH version 2. The following SSH clients have been verified to interoperate with the AP's server. The following table lists the clients, version number, and the website of the client.

Clients	Version	Website
OpenSSH	V3.4-2	http://www.openssh.com
Putty	Rel 0.53b	http://www.chiark.greenend.org.uk
Zoc	5.00	http://www.emtec.com
Axessh	V2.5	http://www.labf.com

For key generation, only the OpenSSH client has been verified.

Auto Configuration Parameters

These parameters relate to the Auto Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Name	Type	Value	Access	CLI Parameter
Auto Configuration	Group	N/A	R	autoconfig
Auto Configuration Status	Integer	enable (default) disable	RW	autoconfigstatus
Auto Config File Name	DisplayString	User Defined	RW	autoconfigfilename
Auto Config TFTP Server IP Address	IpAddress	User Defined	RW	autoconfigTFTPaddr

TFTP Server Parameters

These parameters relate to upload and download commands.

When you execute an upload and/or download Command, the specified arguments are stored in TFTP parameters for future use. If nothing is specified in the command line when issuing subsequent upload and/or download commands, the stored arguments are used.

Name	Type	Value	Access	CLI Parameter
TFTP	Group	N/A	R	tftp
TFTP Server IP Address	IpAddress	User Defined	RW	tftpipaddr
TFTP File Name	DisplayString	User Defined	RW	tftpfilename
TFTP File Type	Integer	img config bootloader sslcertificate sslprivatekey sshprivatekey sshpublickey clibatchfile (CLI Batch File) cbflog (CLI Batch Error Log)	RW	tftpfiletype

IP Access Table Parameters

When creating table entries, you may either specify the argument name followed by argument value or simply enter the argument value. When only the argument value is specified, then enter the values in the order depicted by the following table. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the "comment" argument.

Name	Type	Value	Access	CLI Parameter
IP Access Table	Table	N/A	R	mgmtipaccesstbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Filtering Parameters

Ethernet Protocol Filtering Parameters

Name	Type	Value	Access	CLI Parameter
Ethernet Filtering	Group	N/A	R	etherflt
Filtering Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless 5 or 7 = All interfaces (default is 7)	RW	etherfltifbitmask
Operation Type		passthru block	RW	etherfltoptype

Ethernet Filtering Table

Identify the different filters by using the table index.

Name	Type	Value	Access	CLI Parameter
Ethernet Filtering Table	Table	N/A	R	etherflttbl
Table Index	N/A	N/A	R	index
Protocol Number	Octet String	N/A	RW	protonumber
Protocol Name (optional)	DisplayString		RW	protoname
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

*NOTE: The filter Operation Type (passthru or block) applies **only** to the protocol filters that are **enabled** in this table.*

Static MAC Address Filter Table

Name	Type	Value	Access	CLI Parameter
Static MAC Address Filter Table	Table	N/A	R	staticmactbl
Table Index	N/A	N/A	R	index

Name	Type	Value	Access	CLI Parameter
Static MAC Address on Wired Network	PhysAddress	User Defined	RW	wiredmacaddr
Static MAC Address Mask on Wired Network	PhysAddress	User Defined	RW	wiredmask
Static MAC Address on Wireless Network	PhysAddress	User Defined	RW	wirelessmacaddr
Static MAC Address Mask on Wireless Network	PhysAddress	User Defined	RW	wirelessmask
Comment (optional)	DisplayString	max 255 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Proxy ARP Parameters

Name	Type	Value	Access	CLI Parameter
Proxy ARP	Group	N/A	R	parp
Status	Integer	enable disable (default)	RW	parpstatus

IP ARP Filtering Parameters

Name	Type	Value	Access	CLI Parameter
IP ARP Filtering	Group	N/A	R	iparp
Status	Integer	enable disable (default)	RW	iparpfltstatus
IP Address	IpAddress	User Defined	RW	iparpfltipaddr
Subnet Mask	IpAddress	User Defined	RW	iparpfltsubmask

Broadcast Filtering Table

Name	Type	Value	Access	CLI Parameter
Broadcast Filtering Table	Table	N/A	R	broadcastflttbl
Index	Integer	1 - 5	N/A	index
Protocol Name	DisplayString	N/A	R	protoname
Direction	Integer	ethertowireless wirelesstoether both (default)	RW	direction
Status	Integer	enable disable (default)	RW	status

TCP/UDP Port Filtering

The following parameters are used to enable/disable the Port filter feature.

Name	Type	Value	Access	CLI Parameter
Port Filtering	Group	N/A	R	portflt
Port Filter Status	Integer	enable (default) disable	RW	portfltstatus

TCP/UDP Port Filtering Table

The following parameters are used to configure TCP/UDP Port filters.

Name	Type	Value	Access	CLI Parameter
Port Filtering Table	Table	N/A	R	portflttbl
Table Index	N/A	User Defined (there are also 4 pre-defined indices, see Port Number below for more information)	R	index
Port Type	Octet String	tcp udp tcp/udp	RW	porttype
Port Number	Octet String	User Defined (there are also 4 pre-defined protocols: Index 1: NetBios Name Service - 137, Index 2: NetBios Datagram Service - 138, Index 3: NetBios Session Service - 139, Index 4: SNMP Service - 161)	RW	portnum
Protocol Name	DisplayString	User Defined (there are also 4 pre-defined protocols, see Port Number above)	RW	protoname
Interface Bitmask	Integer32	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless 5 or 7 = All interfaces (default is 7)	RW	ifbitmask
Status (optional)	Integer	enable (default for new entries) disable (default for pre-defined entries) delete	RW	status

Alarms Parameters

SNMP Table Host Table Parameters

When creating table entries, you may either specifying the argument name followed by argument value. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the "comment" argument.

Name	Type	Value	Access	CLI Parameter
SNMP Trap Host Table	Table	N/A	R	snmptraphosttbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr

Name	Type	Value	Access	CLI Parameter
Password	DisplayString	User Defined (up to 64 characters)	W	passwd
Comment (optional)	DisplayString	User Defined (up to 254 characters)	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Syslog Parameters

The following parameters configure the Syslog settings.

Name	Type	Value	Access	CLI Parameter
Syslog	Group	N/A	R	syslog
Syslog Status	Integer	enable disable (default)	RW	syslogstatus
Syslog Port	Octet String	514	R	syslogport
Syslog Lowest Priority Logged	Integer	1 = LOG_ALERT 2 = LOG_CRIT 3 = LOG_ERR 4 = LOG_WARNING 5 = LOG_NOTICE 6 = LOG_INFO (default) 7 = LOG_DEBUG	RW	syslogpritolog
Heartbeat Status	Integer	enable (1) disable (2) (default)	RW	sysloghbstatus
Heartbeat Interval (seconds)	Integer	1 - 604800 seconds; 900 sec. (default)	RW	sysloghbinterval

NOTE: *When Heartbeat is enabled, the AP periodically sends a message to the Syslog server to indicate that it is active. The frequency with which the heartbeat message is sent depends upon the setting of the Heartbeat Interval.*

Syslog Host Table

The table described below configures the Syslog hosts that will receive message from the AP. You can configure up to ten Syslog hosts.

Name	Type	Value	Access	CLI Parameter
Syslog Host Table	Table	N/A	R	sysloghosttbl
Table Index	Integer	1 - 10	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Bridge Parameters

Spanning Tree Parameters

Name	Type	Value	Access	CLI Parameter
Spanning Tree	Group	N/A	R	stp
Spanning Tree Status	Integer	enable disable (default)	RW	stpstatus
Bridge Priority	Integer	0 - 65535 32768 (default)	RW	stppriority
Maximum Age	Integer	600 - 4000 (in 0.01 sec intervals; i.e., 6 to 40 seconds) 2000 (default)	RW	stpmaxage
Hello Time	Integer	100 - 1000 (1/100 second; i.e., 1 to 10 seconds); enter values in increments of 100 200 (default)	RW	stphellotime
Forward Delay	Integer	400 - 3000 (in 0.01 sec intervals; i.e., 4 to 30 seconds) 1500 (default)	RW	stpfwddelay

Spanning Tree Priority and Path Cost Table

Name	Type	Value	Access	CLI Parameter
Spanning Tree Table	Table	N/A	R	stpbl
Table Index (Port)	N/A	1 - 15	R	index
Priority	Integer	0 - 255 128 (default)	RW	priority
Path Cost	Integer	1 - 65535 100 (default)	RW	pathcost
State	Integer	disable blocking listening learning forwarding broken	R	state
Status	Integer	enable disable	RW	status

Storm Threshold Parameters

Name	Type	Value	Access	CLI Parameter
Storm Threshold	Group	N/A (see below)	N/A	stmthres
Broadcast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	stmbrdthres
Multicast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	stmmultithres

Storm Threshold Table

Name	Type	Value	Access	CLI Parameter
Storm Threshold Table	Table	N/A	R	stmthrestbl
Table Index	Integer	1 = Ethernet 3 = Wireless	R	index
Broadcast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	bcast
Multicast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	mcast

Intra BSS Subscriber Blocking

The following parameters control the Intra BSS traffic feature, which prevent wireless clients that are associated with the same AP from communicating with each other:

Name	Type	Value	Access	CLI Parameter
Intra BSS Traffic	Group	N/A	R	intrabss
Intra BSS Traffic Operation	Integer	passthru (default) block	RW	intrabssoptype

Packet Forwarding Parameters

The following parameters control the Packet Forwarding feature, which redirects wireless traffic to a specific MAC address:

Name	Type	Value	Access	CLI Parameter
Packet Forwarding MAC Address	Group	N/A	R	pktfwd
Packet Forwarding MAC Address	MacAddress	User Defined	RW	pktfwdmacaddr
Packet Forwarding Status	Integer	enable disable (default)	RW	pktfwdstatus
Packet Forwarding Interface Port	Integer	0 (any) (default) 1 (Ethernet) 2 (WDS 1) 3 (WDS 2) 4 (WDS 3) 5 (WDS 4) 6 (WDS 5) 7 (WDS 6)	RW	pktfwdif

RADIUS Parameters

General RADIUS Parameters

Name	Type	Value	Access	CLI Parameter
RADIUS	Group	N/A	R	radius
Client Invalid Server Address	Counter32	N/A	R	radcliinvsvradd

RADIUS Server Configuration Parameters

NOTE: *Use a server name only if you have enabled the DNS Client functionality. See* DNS Client for RADIUS Name Resolution.

Name	Type	Value	Access	CLI Parameter
RADIUS Authentication	Table	N/A	R	radiustbl
Table Index (Profile Index)	Integer	N/A	R	index
Primary/Secondary Index	Integer	Primary (1) Secondary (2)	R	subindex
Status	Integer	enable disable	RW	status
Server Address Format	Integer	Ipaddr Name	RW	seraddrfmt
Server IP Address or Name	IpAddress DisplayString	User defined (enter an IP address if seraddrfmt is ipaddr or a name if set to name; up to 254 characters if using a name)	RW	ipaddr
Port (optional)	Integer	User Defined 1812 (default)	RW	port
Shared Secret	DisplayString	User Defined 6 - 32 characters	W	ssecret
Response Time (optional)	Integer	1 - 10 seconds 3 (default)	RW	responsetm
Maximum Retransmissions (optional)	Integer	0 - 4 3 (default)	RW	maxretx
RADIUS MAC Address Format	Integer	dashdelimited colondelimited singledashdelimited nodelimiter	RW	radmacaddrformat
RADIUS Accounting Inactivity Timer	Integer32	1 - 60 minutes	RW	radaccinactivetmr
Authorization Lifetime	Integer32	900 - 43200 seconds	W	radauthlifetm
RADIUS Accounting Update Interval	Integer32	10 - 3600 minutes	RW	radacctupdinterval
VLAN ID	vlanID	-1 (untagged) 1 - 4094	RW	radvlanid

Security Parameters

MAC Access Control Parameters

Name	Type	Value	Access	CLI Parameter
MAC Address Control	Group	N/A	R	macacl
Status	Integer	enable disable (default)	RW	aclstatus
Operation Type	Integer	passthru (default) block	RW	macacloptype

MAC Access Control Table

Name	Type	Value	Access	CLI Parameter
MAC Address Control Table	Table	N/A	R	macacltbl
Table Index	N/A	N/A	R	index
MAC Address	PhysAddress	User Defined	RW	macaddr
Comment (optional)	DisplayString	User Defined max 254 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Rogue Scan Configuration Table

The Rogue Scan Configuration Table allows you to enable or disable Rogue Scan and configure the scanning parameters.

Name	Type	Value	Access	CLI Parameter
Rogue Scan Configuration Table	Table	N/A	R	rscantbl
Rogue Scan Mode	Integer	Bkscan (1) Contscan (2)	RW	mode
Rogue Scan Cycle Time	Integer	1 - 1440	RW	cycletime
Rogue Scan Configuration Table Index	Integer	3 or 4	RW	index
Rogue Scan Status	Integer	enable disable	RW	status

802.1x Parameters

Name	Type	Value	Access	CLI Parameter
802.1x Group	Group	N/A	R	dot1xauthcfg
802.1x Supplicant Timeout	Integer32	3 - 60 seconds (recommended range)	RW	dot1xsupptimeout

Hardware Configuration Reset

The Hardware Configuration Reset commands allows you to enable or disable the feature and to change the password to be used for configuration reset during boot up.

Name	Type	Value	Access	CLI Parameter
Hardware Configuration Reset Status	Integer	enable (1) disable (2)	R	hwconfigresetstatus
Configuration Reset Password	DisplayString	User Defined	RW	configresetpasswd

Security Profile Table

The Security Profile Table allows you to configure security profiles. A maximum of 16 security profiles are supported.

Each security profile can contain one or more enabled security modes (Non-secure station, WEP station, 802.1x station, WPA station, WPA-PSK station, 802.11i, 802.11i-PSK). The WEP/PSK parameters are separately configurable for each security mode. See the command examples in Set Security Profile Parameters.

Name	Type	Value	Access	CLI Parameter
Security Profile Table	Table	N/A	R	secprofiletbl
Table Index	Integer	1 - 16	RW	index
Security Mode	Integer	nonsecure wep 802.1x wpa wpa-psk 802.11i 802.11i-psk	RW	secmode
Authentication Mode	Integer	none 802.1x psk	R	authmode
Cipher	Integer	none wep tkip aes	R	ciphersuite
Encryption Key 0	Integer	See Encryption Key Format	W	encryptkey0
Encryption Key 1	Integer	See Encryption Key Format	W	encryptkey1
Encryption Key 2	Integer	See Encryption Key Format	W	encryptkey2
Encryption Key 3	Integer	See Encryption Key Format	W	encryptkey3
Encryption Transmit Key	Integer	0 - 3	RW	encryptkeytx
Encryption Key Length	Integer	1 (64 bits) 2 (128 bits) 3 (152 bits)	RW	encryptkeylength
PSK Passphrase	Integer	8 - 64 characters	W	passphrase

Encryption Key Format

If WEP security mode is configured, then the appropriate key size must be configured. The AP supports 63-, 128-, and 152-bit encryption keys. Encryption keys may be configured using either hexadecimal or ASCII values, as described in the following table.

Key Length	Hexadecimal	ASCII
64-bit	10 characters (0 - F)	5 alphanumeric characters

Key Length	Hexadecimal	ASCII
128-bit	26 characters (0 - F)	13 alphanumeric characters
152-bit	32 characters (0 - F)	16 alphanumeric characters

Each ASCII character corresponds to two hexadecimal digits. See ASCII Character Chart for ASCII/Hexadecimal correspondence.

VLAN/SSID Parameters

Name	Type	Value	Access	CLI Parameter
VLAN	Group	N/A	R	vlan
Status	Integer	enable disable (default)	RW	vlanstatus
Management ID	VlanId	-1 (untagged) or 1 - 4094	RW	vlanmgmtid

Other Parameters

IAPP Parameters

Name	Type	Value	Access	CLI Parameter
IAPP	Group	N/A	R	iapp
IAPP Status	Integer	enable (default) disable	RW	iappstatus
Periodic Announce Interval (seconds)	Integer	80 120 (default) 160 200	RW	iappannint
Announce Response Time	Integer	2 seconds	R	iappannresp
Handover Time-out	Integer	410 ms 512 ms (default) 614 ms 717 ms 819 ms	RW	iapphandtout
Max. Handover Retransmissions	Integer	1 - 4 (default 4)	RW	iapphandretx
Send Announce Request on Startup	Integer	enable (default) disable	RW	iappannreqstart

NOTE: *These parameters configure the Inter Access Point Protocol (IAPP) for roaming. Leave these settings at their default value unless a technical representative asks you to change them.*

Wireless Multimedia Enhancements (WME)/Quality of Service (QoS) parameters

The Wireless Multimedia Enhancements commands enable and configure Wireless Multimedia Enhancement/Quality of Service parameters. The following two commands are part of the Wireless Interface Properties table.

Enabling QoS

Name	Type	Value	Access	CLI Parameter
QoS Status	Object Status	enable disable (default)	RW	qosstatus
QoS Maximum Medium Threshold	Integer	50 - 90	RW	qosmaximummediumthreshold

Configuring QoS Policies

The QoS group manages the QoS policies:

Name	Type	Value	Access	CLI Parameter
QoS Group	Group	N/A	N/A	qos
QoS Policy Table	Table	N/A	N/A	qospolicytbl
Table Primary Index	Integer	N/A	R	index
Table Secondary Index	Integer	N/A	R	secindex
Policy Name	Display String	0 - 32 characters	RW	policyname
Policy Type	Integer	inlayer2, inlayer3, outlayer2, outlayer3, spectralink*	RW	type
Priority Mapping Index†	Integer	See Note†.	RW	mapindex
Apply QoS Marking	Object Status	enable disable	RW	markstatus
Table Row Status	Row Status	enable disable delete	RW	status

* QoS must be enabled on the wireless interface before spectralink can be enabled.

† A priority mapping needs to be specified for a QoS Policy. The priority mapping depends on the type of policy configured. For Layer 2 policy types (inbound or outbound) a mapping index from the 802.1p to 802.1D table should be specified. For Layer 3 policy types (inbound or outbound) a mapping index from the IP DSCP to 802.1D table should be specified. The mapping index, in both cases, depends on the number of mappings configured by the user. For SpectraLink policy type a mapping is not required.

Specifying the Mapping between 802.1p and 802.1D Priorities

The QoS 802.1p to 802.1D Mapping Table specifies the mapping between 802.1P and 802.1D priorities.

Name	Type	Value	Access	CLI Parameter
QoS 802.1p to 802.1D Mapping Table	Table	N/A	N/A	qos1pto1dtbl
Table Index (Primary Index)	Integer	0 - 7	R	index
802.1D Priority (Secondary Index)	Integer	0 - 7	R	1dpriority
802.1p Priority	Integer	0 - 7	RW	1ppriority
Table Row Status	Row Status	enable disable delete	RW	status

Specifying the Mapping between IP Precedence/DSCP Ranges and 802.1D Priorities

The QoS IP DSCP to 802.1D Mapping Table specifies the mapping between IP Precedence/DSCP Ranges and 802.1D priorities.

Name	Type	Value	Access	CLI Parameter
QoS IP DSCP to 802.1D Mapping Table	Table	N/A	N/A	qosdscpto1dtbl
Table Index (Primary Index)	Integer	0 - 7	R	index
802.1D Priority	Integer	0 - 7	R	1dpriority
IP DSCP Lower Limit	Integer	0 - 62	RW	dscplower
IP DSCP Upper Limit	Integer	1 - 63	RW	dscpupper
Table Row Status	Row Status	enable disable delete	RW	status

QoS Enhanced Distributed Channel Access (EDCA) Parameters

The following commands configure the client (STA) and AP Enhanced Distributed Channel Access (EDCA) parameters.

The EDCA parameter set provides information needed by the client stations for proper QoS operation during the wireless contention period. These parameters are used by the QoS enabled AP to establish policy, to change policies when accepting new stations or new traffic, or to adapt to changes in the offered load. The EDCA parameters assign priorities to traffic types where higher priority packets gain access to the wireless medium more frequently than lower priority packets.

NOTE: We have defined default recommended values for EDCA parameters; we recommend not modifying EDCA parameters unless strictly necessary.

Name	Type	Value	Access	CLI Parameter
STA EDCA Table	Table	N/A	N/A	qosedcatbl
Table Index	Integer	3 (Wireless A) 4 (Wireless B)	R	—
QoS Access Category	Integer	1 (Best Effort) 2 (Background) 3 (Video) 4 (Voice)	R	—
CWmin	Integer	0 - 255	RW	cwmin
CWmax	Integer	0 - 65535	RW	cwmax
AIFSN	Integer	2 - 15	RW	aifsn
Tx OP Limit	Integer	0 - 65535	RW	txoplimit
MSDU Lifetime	Integer	0 - 500	RW	msdulifetime
AC Mandatory	Truth Value	1 (Enable) 2 (Disable)	RW	acmandatory
AP EDCA Table	Table	N/A	N/A	qosqapedcatbl
Table Index	Integer	3 (Wireless A) 4 (Wireless B)	R	—
QoS Access Category	Integer	1 (Best Effort) 2 (Background) 3 (Video) 4 (Voice)	R	—
CWmin	Integer	0 - 255	RW	cwmin

Name	Type	Value	Access	CLI Parameter
CWmax	Integer	0 - 65535	RW	cwmax
AIFSN	Integer	2 - 15	RW	aifsn
Tx OP Limit	Integer	0 - 65535	RW	txoplimit
MSDU Lifetime	Integer	0 - 500	RW	msdulifetime
AC Mandatory	Truth Value	true false	RW	acmandatory

Examples:

`show qosedcatbl` (or `qosqapedcatbl`)

`set qosedcatbl` (or `qosqapedcatbl`) `<Index>.<Access Category> <EDCA parameter> <value>`

For example: `set qosedcatbl 3.1 cwmin 15`

Defining the QoS Policy used for a Wireless Interface SSID

The QoS Policy object configures the QoS policy to be used per wireless interface SSID. This object is part of the Wireless Interface SSID Table; the CLI command for this table is "wifssidtbl."

Name	Type	Value	Access	CLI Parameter
QoS Policy	Integer	See Note*	RW	qospolicy

* A QoS Policy number needs to be specified in the SSID table. This depends on the QoS policies configured by the user. Once the user has configured QoS policies, the user should specify the policy to be used for that SSID.

CLI Batch File

A CLI Batch file is a user-editable file that lists a series of CLI set commands, that can be uploaded to the Access Point to change its configuration. The Access Point executes the CLI commands specified in the CLI Batch file after upload and the configuration gets changed accordingly. A CLI Batch file can also be used for Auto Configuration.

The CLI Batch file does not replace the existing LTV format configuration file, which continues to define the configuration of the AP.

The CLI Batch file contains a list of CLI commands that the AP will execute. The AP performs the commands in the file immediately after the file is uploaded to the AP manually or during Auto Configuration. The AP parses the file and executes the CLI commands. Commands that do not require a reboot take effect immediately, while commands that require a reboot (typically commands affecting a wireless interface) will take effect after reboot.

Auto Configuration and the CLI Batch File

The Auto Configuration feature allows download of the LTV format configuration file or the CLI Batch file. The AP detects whether the file uploaded is LTV format or a CLI Batch file. If the AP detects a CLI Batch file (a file with extension .cli), the AP executes the file immediately.

The AP will reboot after executing the CLI Batch file. Auto Configuration will not result in repeated reboots if the CLI Batch file contains rebootable parameters.

CLI Batch File Format and Syntax

The CLI Batch file must be named with a .cli extension to be recognized by the AP. The maximum file size allowed is 100 Kbytes, and files with larger sizes cannot be uploaded to the AP. The CLI commands supported in the CLI Batch File are a subset of the legal AP CLI commands.

The follow commands are supported:

- Set commands
- Reboot command (the reboot command ignores the argument (time)

Each command must be separated by a new line.

NOTE: The following commands are not supported: Show command, Debug command, Undebug command, Upload command, Download command, Passwd command, Kill command, and the Exit, Quit, and Done commands.

Sample CLI Batch File

The following is a sample CLI Batch File:

```
set sysname system1
set sysloc sunnyvale
set sysctname contact1
set sysctphone 1234567890
set sysctemail email@domain.com
set ipaddr 11.0.0.66
set ipaddrtype static
set ipsubmask 255.255.255.0
set ipgw 11.0.0.1
set wif 3 autochannel disable
set wif 3 mode 1
set syslogstatus enable
set sysloghbstatus enable
set sysloghbinterval 5
set wif 3 netname london
reboot
```

Reboot Behavior

When a CLI Batch file contains a reboot command, the reboot will occur only after the entire CLI Batch file has been executed.

There are two methods of uploading the CLI Batch File:

- Upload
- Upload and reboot (this option is to be used for a CLI Batch file containing the configuration parameters that require a reboot)

CLI Batch File Error Log

If there is any error during the execution of the CLI Batch file, the AP will stop executing the file. The AP generates traps for all errors and each trap contains the following information:

- Start of execution
- Original filename of the uploaded file
- End of execution (along with the status of execution)
- Line number and description of failures that occurred during execution

The AP logs all the errors during execution and stores them in the Flash memory in a CLI Batch File Error Log named "CBFERR.LOG". The CLI Batch File Error Log can be downloaded though TFTP, HTTP, or CLI file transfer to a specified host.

B

ASCII Character Chart

You can configure WEP Encryption Keys in either Hexadecimal or ASCII format. Hexadecimal digits are 0-9 and A-F (not case sensitive). ASCII characters are 0-9, A-F, a-f (case sensitive), and punctuation marks. Each ASCII character corresponds to two hexadecimal digits.

The table below lists the ASCII characters that you can use to configure WEP Encryption Keys. It also lists the Hexadecimal equivalent for each ASCII character.

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64			7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

C

Specifications

- Software Features
- Hardware Specifications
- Available Channels

Software Features

The tables below list the software features available on the AP-700.

- Number of Stations per BSS
- Management Functions
- Advanced Bridging Functions
- Medium Access Control (MAC) Functions
- Security Functions
- Network Functions

Number of Stations per BSS

Feature	Supported by AP-700
Without encryption	up to 63
With WEP encryption	up to 63
With 802.1x Authentication	up to 63
With WPA	up to 27
With 802.11i (WPA2)	up to 63

Management Functions

Feature	Supported by AP-700
Web User Interface	✓
Telnet / CLI	✓
SNMP Agent	✓
Serial CLI	✓
Secure Management	✓
SSH	✓
RADIUS Based Management Access	✓

Advanced Bridging Functions

Feature	Supported by AP-700
IEEE 802.1d Bridging	✓
WDS Relay	✓
Roaming	✓
Protocol Filtering	✓
Multicast/Broadcast Storm Filtering	✓
Proxy ARP	✓
TCP/UDP Port Filtering	✓
Blocking Intra BSS Clients	✓
Packet Forwarding	✓

Medium Access Control (MAC) Functions

Feature	Supported by AP-700
Automatic Channel Selection (ACS)	✓
Dynamic Frequency Selection (DFS)/Radar Detection (RD)*	✓
Wireless Service Shutdown	✓
802.11d Support	✓
TX Power Control	✓
Wireless Multimedia Enhancements/Quality of Service (QoS)	✓
Channel Blacklist	✓
Closed System	✓
Broadcast Unique Beacon	✓
Super and Turbo Mode Support	✓

* DFS is required for 802.11a APs certified in the ETSI, TELEC, FCC, and IC regulatory domains and operating in the middle frequency band. When ACS is disabled, available channels are limited to those in the lower frequency band. See Dynamic Frequency Selection/Radar Detection (DFS/RD).

Security Functions

Feature	Supported by AP-700
Security Profiles per VLAN	✓
RADIUS Profiles per VLAN	✓
IEEE 802.11 WEP*	✓
MAC Access Control	✓
RADIUS MAC-based Access Control	✓
IEEE 802.1x Authentication†	✓
Multiple Authentication Server Support per VLAN‡	✓
Rogue Scanning to Detect Rogue Access Points and Clients	✓
Per User Per Session (PUPS) Encryption §	✓
Wi-Fi Protected Access (WPA)/802.11i (WPA2)	✓
Hardware Configuration Reset Disable	✓

   * Key lengths supported by 802.11a: 64-bit, 128-bit, and 152-bit.
      Key lengths supported by 802.11b: 64-bit and 128-bit.
      Key lengths supported by 802.11b/g: 64-bit, 128-bit, and 152-bit.

   † EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP client supplicant supported.

   ‡ Support is provided for a primary and backup RADIUS authentication server for both MAC-based authentication and 802.1x authentication per VLAN.

   § Use in conjunction with WPA or 802.1x Authentication.

Network Functions

Feature	Supported by AP-700
DHCP Client	✓
DHCP Server	✓
DHCP Relay Agent and IP Lease Renewal	✓
Inter Access Point Protocol (IAPP)	✓
Link Integrity	✓
System Logging (Syslog)	✓
RADIUS Accounting Support*	✓
DNS Client	✓
TCP/IP Protocol Support	✓
Virtual LAN Support	Up to 16 SSID/VLAN pairs, with specific Security and RADIUS profiles. For more information, see the Advanced Configuration chapter.

   * Includes Fallback to Primary RADIUS Server, RADIUS Session Timeout, RADIUS Multiple MAC Address Formats, RADIUS DNS Host Name Support, RADIUS Start/Stop Accounting.

Hardware Specifications

Category	Specification
Physical	
Dimensions (H x W x L)	1 x 4.75 x 7.1 in (25 x 121 x 180 mm)
Weight	**Unit:** .65 lb (.295 kg) **Power Supply:** .45 lbs (.20 kg)
Electrical	
Voltage	100 to 240 VAC +/- 10% (50-60 Hz) (power supply)
Power Draw	<9 Watts (power supply)
Environmental	
Storage Temperature	-20°C to 85°C (-4°F to 185°F)
Operating Temperature	0°C to 55°C (32°F to 131°F)
Humidity	5 to 95% relative humidity, non-condensing
Interfaces	
Wired Ethernet	10/100 Base-T auto-sensing RJ45 Female Socket, Auto-sensing
Wireless Ethernet	1 integrated 802.11a/b/g radio
Serial Port	Standard RS-232 interface with DB-9 female connector
LEDs	
Types	Power Ethernet Link Wireless 802.11a/b/g Radio Link

Available Channels

Available channels vary based on operational mode and country. To verify which channels are available for your product:

1. Locate the product model number on the underside of your AP unit or on the unit's box.
2. Note the alphanumeric code following the number 8675. (e.g., 8675-**EU**)
3. See the following tables.
   - 802.11a/b/g Channels
   - WD SKU Channels by Country

802.11a/b/g Channels

Mode	Frequency Band	Channel	Product Model Number														
			AU	AU2	BR	CN	EU	EU2	HK	JP	SG	SK	TW	UK	US	US2	WD
802.11b/g	—	1	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		2	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		3	✓*		✓*	✓*	✓*	✓*		✓*	✓*	✓*	✓*		✓*	✓	
		4	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		5	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		6	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		7	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		8	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		9	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		10	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		11	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	
		12					✓	✓		✓			✓				
		13					✓	✓		✓			✓				
		14								✓†							
802.11a	Lower	34								✓*							
		36	✓	✓	✓		✓*	✓*						✓*		✓	
		38								✓							
		40	✓	✓	✓		✓	✓						✓		✓‡	
		42								✓							
		44	✓	✓	✓		✓	✓						✓		✓	
		46								✓							
		48	✓	✓	✓		✓	✓						✓		✓‡	
	Middle	52	✓*	✓*				✓						✓	✓*	✓*	
		56	✓	✓				✓					✓*	✓	✓‡	✓‡	
		58															
		60	✓	✓				✓					✓	✓	✓	✓	
		64	✓	✓				✓					✓	✓	✓	✓	
	High	100													✓	✓	
		104													✓	✓	
		108													✓	✓	
		112													✓	✓	
		116													✓	✓	
		120													✓	✓	
		124													✓	✓	
		128													✓	✓	
		132													✓	✓	
		136													✓	✓	
		140													✓	✓	
	Upper	149	✓	✓	✓	✓*			✓*		✓*	✓*	✓		✓	✓	
		153	✓	✓	✓	✓			✓		✓	✓	✓		✓‡	✓‡	
		157	✓	✓	✓	✓			✓		✓	✓	✓		✓	✓	
		161	✓	✓	✓	✓			✓		✓	✓	✓		✓‡	✓‡	
	ISM Band	165	✓	✓	✓						✓		✓		✓	✓	

WD column: See WD SKU Channels by Country

*   Default channel.
†   Available for use only in 802.11b mode.
‡   Also supports 40 MHz channel bandwidths.

WD SKU Channels by Country

Available channel bands depend on the selected country and mode of use (indoor/outdoor).

The typical channels available in each 802.11a frequency band are as follows:

Band	Supported Channels
Lower (L)	36, 40, 44, 48
Middle (M)	52, 56, 60, 64
High (H)	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Upper (U)	149, 153, 157, 161
ISM	165

Country	Indoor/Outdoor	802.11a	802.11b/g	Country Identifier	.11d Country Code
Austria	Indoor	L, M, H	1 - 13	AT1	AT
	Outdoor	H	1 - 13	AT2	AT
Belgium	Indoor	L, M, H	1 - 13	BE1	BE
	Outdoor	H	1 - 13	BE2	BE
Cyprus	Indoor	L, M, H	1 - 13	CY1	CY
	Outdoor	H	1 - 13	CY2	CY
Czech Republic	Indoor	L, M, H	1 - 13	CZ1	CZ
	Outdoor	H	1 - 13	CZ2	CZ
Denmark	Indoor	L, M, H	1 - 13	DK1	DK
	Outdoor	H	1 - 13	DK2	DK
Estonia	Indoor	L, M, H	1 - 13	EE1	EE
	Outdoor	H	1 - 13	EE2	EE
Finland	Indoor	L, M, H	1 - 13	FI1	FI
	Outdoor	H	1 - 13	FI2	FI
France	Indoor	L, M, H	1 - 13	FR1	FR
	Outdoor	H	1 - 13	FR2	FR
Germany	Indoor	L, M, H	1 - 13	DE1	DE
	Outdoor	H	1 - 13	DE2	DE
Greece	Indoor	L, M, H	1 - 13	GR1	GR
	Outdoor	H	1 - 13	GR2	GR
Hungary	Indoor	L, M, H	1 - 13	HU1	HU
	Outdoor	H	1 - 13	HU2	HU
Ireland	Indoor	L, M, H	1 - 13	IE1	IE
	Outdoor	H	1 - 13	IE2	IE
Italy	Indoor	L, M, H	1 - 13	IT1	IT
	Outdoor	H	1 - 13	IT2	IT
Latvia	Indoor	L, M, H	1 - 13	LV1	LV
	Outdoor	H	1 - 13	LV2	LV
Lithuania	Indoor	L, M, H	1 - 13	LT1	LT
	Outdoor	H	1 - 13	LT2	LT
Luxembourg	Indoor	L, M, H	1 - 13	LU1	LU
	Outdoor	H	1 - 13	LU2	LU

Country	Indoor/Outdoor	802.11a	802.11b/g	Country Identifier	.11d Country Code
Malta	Indoor	L, M, H	1 - 13	MT1	MT
	Outdoor	H	1 - 13	MT2	MT
Netherlands	Indoor	L, M, H	1 - 13	NL1	NL
	Outdoor	H	1 - 13	NL2	NL
Norway	Indoor	L, M, H	1 - 13	NO1	NO
	Outdoor	H	1 - 13	NO2	NO
Poland	Indoor	L, M, H	1 - 13	PL1	PL
	Outdoor	H	1 - 13	PL2	PL
Portugal	Indoor	L, M, H	1 - 13	PT1	PT
	Outdoor	H	1 - 13	PT2	PT
Russia	Indoor/Outdoor	L, M, H, U, ISM	1 - 13	RU	RU
Spain	Indoor	L, M, H	1 - 13	ES1	ES
	Outdoor	H	1 - 13	ES2	ES
Sweden	Indoor	L, M, H	1 - 13	SE1	SE
	Outdoor	H	1 - 13	SE2	SE
Switzerland	Indoor	L, M, H	1 - 13	CH1	CH
	Outdoor	H	1 - 13	CH2	CH
United Kingdom/ Great Britain	Indoor	L, M, H	1 - 13	GB1	GB
	Outdoor	H	1 - 13	GB2	GB

D

Technical Services and Support

See the following sections:

- Obtaining Technical Services and Support
- Support Options
    - Proxim eService Web Site Support
    - Telephone Support
    - ServPak Support

Obtaining Technical Services and Support

If you are having trouble utilizing your Proxim product, please review this manual and the additional documentation provided with your product.

If you require additional support and would like to use Proxim's free Technical Service to help resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services:

- Product information
    - Part number of suspected faulty unit
    - Serial number of suspected faulty unit
- Trouble/error information:
    - Trouble/symptom being experienced
    - Activities completed to confirm fault
    - Network information (what kind of network are you using?)
    - Circumstances that preceded or led up to the error
    - Message or alarms viewed
    - Steps taken to reproduce the problem
- Servpak information (if a Servpak customer):
    - Servpak account number
- Registration information:
    - If the product is not registered, date when you purchased the product
    - If the product is not registered, location where you purchased the product

    NOTE: If you would like to register your product now, visit the Proxim eService Web Site at http://support.proxim.com *and click on* **New Product Registration***.*

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at http://support.proxim.com.

On the Proxim eService Web Site, you can access the following services:

- **New Product Registration**: Register your product for free support.
- **Open a Ticket or RMA**: Open a ticket or RMA and receive an immediate reply.
- **Search Knowledgebase**: Locate white papers, software upgrades, and technical information.
- **ServPak (Service Packages)**: Receive Advanced Replacement, Extended Warranty, 7x24x365 Technical Support, Priority Queuing, and On-Site Support.
- **Your Stuff**: Track status of your tickets or RMAs and receive product update notifications.
- **Provide Feedback**: Submit suggestions or other types of feedback.
- **Customer Survey**: Submit an On-Line Customer Survey response.
- **Repair Tune-Up**: Have your existing Proxim equipment inspected, tested, and upgraded to current S/W and H/W revisions, and extend your warranty for another year.

Telephone Support

Contact technical support via telephone as follows:

- **Domestic**: 866-674-6626
- **International**: +1-408-542-5390

Hours of Operation
- **North America**: 8 a.m. to 5 p.m. PST, Monday through Friday
- **EMEA**: 8 a.m. to 5 p.m. GMT, Monday through Friday

ServPak Support

Proxim understands that service and support requirements vary from customer to customer. It is our mission to offer service and support options that go above-and-beyond normal warranties to allow you the flexibility to provide the quality of service that your networks demand.

In recognition of these varying requirements we have developed a support program called ServPak. ServPak is a program of Enhanced Service Options that can be purchased individually or in combinations to meet your needs.

- **Advanced Replacement**: This service offers customers an advance replacement of refurbished or new hardware. (Available in the U.S., Canada, and select countries. Please inquire with your authorized Proxim distributor for availability in your country.)
- **Extended Warranty**: This service provides unlimited repair of your Proxim hardware for the life of the service contract.
- **7x24x365 Technical Support**: This service provides unlimited, direct access to Proxim's world-class technical support 24 hours a day, 7 days a week, 365 days a year.
- **Priority Queuing**: This service allows your product issue to be routed to the next available Customer Service Engineer.

To purchase ServPak support services, please contact your authorized Proxim distributor.   To receive more information or for questions on any of the available ServPak support options, please call Proxim Support at +1-408-542-5390 or send an email to servpak@proxim.com.

E

Statement of Warranty

Warranty Coverage

Proxim Wireless Corporation warrants that its Products are manufactured solely from new parts, conform substantially to specifications, and will be free of defects in material and workmanship for a Warranty Period of **1 year** from the date of purchase.

Repair or Replacement

In the event a Product fails to perform in accordance with its specification during the Warranty Period, Proxim offers return-to-factory repair or replacement, with a thirty (30) business-day turnaround from the date of receipt of the defective Product at a Proxim Wireless Corporation Repair Center. When Proxim Wireless has reasonably determined that a returned Product is defective and is still under Warranty, Proxim Wireless shall, at its option, either: (a) repair the defective Product; (b) replace the defective Product with a refurbished Product that is equivalent to the original; or (c) where repair or replacement cannot be accomplished, refund the price paid for the defective Product. The Warranty Period for repaired or replacement Products shall be ninety (90) days or the remainder of the original Warranty Period, whichever is longer. This constitutes Buyer's sole and exclusive remedy and Proxim Wireless's sole and exclusive liability under this Warranty.

Limitations of Warranty

The express warranties set forth in this Agreement will not apply to defects in a Product caused; (i) through no fault of Proxim Wireless during shipment to or from Buyer, (ii) by the use of software other than that provided with or installed in the Product, (iii) by the use or operation of the Product in an application or environment other than that intended or recommended by Proxim Wireless, (iv) by modifications, alterations, or repairs made to the Product by any party other than Proxim Wireless or Proxim Wireless's authorized repair partners, (v) by the Product being subjected to unusual physical or electrical stress, or (vii) by failure of Buyer to comply with any of the return procedures specified in this Statement of Warranty.

Support Procedures

Buyer should return defective LAN Products within the first 30 days to the merchant from which the Products were purchased. Buyer can contact a Proxim Wireless Customer Service Center either by telephone or via web. Calls for support for Products that are near the end of their warranty period should be made not longer than seven (7) days after expiration of warranty. Repair of Products that are out of warranty will be subject to a repair fee. Contact information is shown below. Additional support information can be found at Proxim Wireless's web site at http://support.proxim.com.

- **Domestic**: 866-674-6626
- **International**: +1-408-542-5390

Hours of Operation

- **North America:** 8 a.m. to 5 p.m. PST, Monday through Friday
- **EMEA:** 8 a.m. to 5 p.m. GMT, Monday through Friday

When contacting the Customer Service for support, Buyer should be prepared to provide the Product description and serial number and a description of the problem. The serial number should be on the product.

In the event the Customer Service Center determines that the problem can be corrected with a software update, Buyer might be instructed to download the update from Proxim Wireless's web site or, if that's not possible, the update will be sent to Buyer. In the event the Customer Service Center instructs Buyer to return the Product to Proxim Wireless for repair or replacement, the Customer Service Center will provide Buyer a Return Material Authorization ("RMA") number

and shipping instructions. Buyer must return the defective Product to Proxim Wireless, properly packaged to prevent damage, shipping prepaid, with the RMA number prominently displayed on the outside of the container.

Calls to the Customer Service Center for reasons other than Product failure will not be accepted unless Buyer has purchased a Proxim Wireless Service Contract or the call is made within the first thirty (30) days of the Product's invoice date. Calls that are outside of the 30-day free support time will be charged a fee of $25.00 (US Dollars) per Support Call.

If Proxim Wireless reasonably determines that a returned Product is not defective or is not covered by the terms of this Warranty, Buyer shall be charged a service charge and return shipping charges.

Other Information

Search Knowledgebase

Proxim Wireless stores all resolved problems in a solution database at the following URL: http://support.proxim.com.

Ask a Question or Open an Issue

Submit a question or open an issue to Proxim Wireless technical support staff at the following URL: http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/ask.php.

Other Adapter Cards

Proxim Wireless does not support internal mini-PCI devices that are built into laptop computers, even if identified as "ORiNOCO" devices. Customers having such devices should contact the laptop vendor's technical support for assistance.

For support for a PCMCIA card carrying a brand name other than Proxim, ORiNOCO, Lucent, Wavelan, or Skyline, Customer should contact the brand vendor's technical support for assistance.