About This Guide

Introduction .................................................. vii
Document Conventions ...................................... vii
Notational Conventions ..................................... viii
Service Information ......................................... viii

Chapter 1. AP-5131 Introduction

Feature Overview ............................................. 1-2
  Single or Dual Mode Radio Options .................... 1-2
  Separate LAN and WAN Ports ............................ 1-3
  Multiple Mounting Options ............................. 1-3
  Antenna Support for 2.4 GHz and 5.2 GHz Radios .... 1-3
  Sixteen Configurable WLANs ........................... 1-4
  Support for 4 BSSID per Radio ........................ 1-4
  Quality of Service (QoS) Support ..................... 1-4
  Industry Leading Data Security ....................... 1-5
Available Product Configurations ............................................. 2-2
Requirements ........................................................................... 2-4
Placement of the AP-5131 ....................................................... 2-4
Site Surveys .............................................................................. 2-5
Antenna Options ....................................................................... 2-5
Power Options .......................................................................... 2-7
Symbol Power Injector System ............................................... 2-7
Installing the Power Injector .................................................... 2-9
Preparing for Site Installation .................................................. 2-9
Cabling the Power Injector ...................................................... 2-9
Power Injector LED Indicators .................................................. 2-10
Mounting the AP-5131 ............................................................. 2-11
Desk Mounted Installations ...................................................... 2-11
Wall Mounted Installations ....................................................... 2-13
Suspended Ceiling T-Bar Installations ................................. 2-15
Above the Ceiling (Plenum) Installations................................. 2-17
LED Indicators .......................................................................... 2-20
Setting Up MUs ......................................................................... 2-22

Chapter 3. Getting Started
Installing the AP-5131 ............................................................. 3-1
Configuration Options ............................................................. 3-2
Basic Device Configuration ...................................................... 3-3
Configuring Device Settings .................................................... 3-4
Configuring WLAN Security Settings ..................................... 3-9
Testing Connectivity ............................................................... 3-11
Where to Go from Here? ........................................................ 3-12

Chapter 4. System Configuration
Configuring System Settings .................................................... 4-2
Configuring Data Access .......................................................... 4-5
Managing Certificate Authority (CA) Certificates ................. 4-8
Importing a CA Certificate ...................................................... 4-8
Creating Self Certificates ......................................................... 4-9
Configuring SNMP Settings .................................................... 4-11
Configuring SNMP Access Control ........................................ 4-17
Enabling SNMP Traps ........................................ 4-19
Configuring Specific SNMP Traps ....................... 4-22
Configuring SNMP RF Trap Thresholds ............... 4-24
Configuring Network Time Protocol (NTP) .......... 4-26
Logging Configuration ...................................... 4-28
Importing/Exporting Configurations ................. 4-30
Updating Device Firmware ................................. 4-34

Chapter 5. Network Management
Configuring the LAN Interface ......................... 5-1
Configuring VLAN Support ............................... 5-5
Configuring Advanced DHCP Server Settings ...... 5-10
Configuring Advanced DHCP Server Settings ...... 5-11
Configuring WAN Settings ............................... 5-13
Configuring Network Address Translation (NAT) Settings .... 5-18
Setting the Type Filter Configuration ............... 5-11
Configuring Port Forwarding ............................ 5-20
Enabling Wireless LANs (WLANs) ..................... 5-22
Creating/Editing Individual WLANs ................. 5-24
Configuring WLAN Security Policies ................. 5-27
Configuring a WLAN Access Control List (ACL) .. 5-29
Setting the WLAN Quality of Service (QoS) Policy . 5-31
Setting the WLAN’s Radio Configuration .......... 5-36
Configuring the 802.11a or 802.11b/g Radio ........ 5-38
Configuring Bandwidth Management Settings .... 5-45
Configuring Router Settings ............................ 5-47

Chapter 6. Configuring Access Point Security
Configuring Security Options ......................... 6-2
Setting Passwords ......................................... 6-3
Resetting the AP-5131 Password ...................... 6-4
Enabling Authentication and Encryption Schemes .... 6-5
Configuring Kerberos Authentication ................. 6-9
Configuring 802.1x EAP Authentication ............. 6-11
Configuring WEP Encryption ........................... 6-15
Configuring KeyGuard Encryption .................... 6-17
Configuring WPA Using TKIP ......................... 6-19
Configuring WPA2-CCMP (802.11i) ........................................... 6-22
Configuring Firewall Settings ........................................... 6-25
  Configuring LAN to WAN Access ..................................... 6-27
    Available Protocols ............................................. 6-30
  Configuring Advanced LAN Access .................................. 6-30
Configuring VPN Tunnels .................................................. 6-33
  Configuring Manual Key Settings ................................... 6-36
  Configuring Auto Key Settings ..................................... 6-40
  Configuring IKE Key Settings ...................................... 6-42
    Viewing VPN Status ............................................ 6-46
Configuring Content Filtering Settings .................................. 6-48
Configuring Rogue AP Detection ........................................ 6-51
  Moving Rogue APs to the Allowed AP List ......................... 6-54
    Displaying Rogue AP Details ................................... 6-56
    Using MUs to Detect Rogue Devices ........................... 6-58

Chapter 7. Monitoring Statistics

Viewing WAN Statistics .................................................. 7-2
Viewing LAN Statistics .................................................. 7-5
Viewing Wireless Statistics ............................................ 7-8
  Viewing WLAN Statistics ........................................... 7-10
Viewing Radio Statistics Summary ....................................... 7-14
  Viewing Radio Statistics ........................................... 7-15
    Retry Histogram ................................................ 7-19
Viewing MU Statistics Summary .......................................... 7-20
  Viewing MU Details ................................................ 7-22
  Pinging Individual MUs ............................................ 7-24
  MU Authentication Statistics ....................................... 7-25
Viewing Known Access Point Statistics ................................. 7-26

Chapter 8.
Command Line Interface Reference

Connecting to the CLI ..................................................... 8-1
  Accessing the CLI through the Serial Port ......................... 8-1
  Accessing the CLI via Telnet ...................................... 8-2
Admin and Common Commands .......................................... 8-3
<table>
<thead>
<tr>
<th>Command Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Commands</td>
<td>8-12</td>
</tr>
<tr>
<td>Network LAN Commands</td>
<td>8-13</td>
</tr>
<tr>
<td>Network LAN, VLAN Commands</td>
<td>8-16</td>
</tr>
<tr>
<td>Network LAN, DHCP Commands</td>
<td>8-23</td>
</tr>
<tr>
<td>Network Type Filter Commands</td>
<td>8-29</td>
</tr>
<tr>
<td>Network WAN Commands</td>
<td>8-34</td>
</tr>
<tr>
<td>Network WAN NAT Commands</td>
<td>8-37</td>
</tr>
<tr>
<td>Network WAN, VLAN Commands</td>
<td>8-43</td>
</tr>
<tr>
<td>Network WAN App Commands</td>
<td>8-52</td>
</tr>
<tr>
<td>Network Wireless Commands</td>
<td>8-56</td>
</tr>
<tr>
<td>Network WLAN Commands</td>
<td>8-57</td>
</tr>
<tr>
<td>Network Security Commands</td>
<td>8-62</td>
</tr>
<tr>
<td>Network ACL Commands</td>
<td>8-71</td>
</tr>
<tr>
<td>Network Radio Configuration Commands</td>
<td>8-76</td>
</tr>
<tr>
<td>Network Quality of Service (QoS) Commands</td>
<td>8-93</td>
</tr>
<tr>
<td>Network Bandwith Management Commands</td>
<td>8-98</td>
</tr>
<tr>
<td>Network Rogue-AP Commands</td>
<td>8-101</td>
</tr>
<tr>
<td>Network Firewall Commands</td>
<td>8-111</td>
</tr>
<tr>
<td>Network Router Commands</td>
<td>8-116</td>
</tr>
<tr>
<td>System Commands</td>
<td>8-121</td>
</tr>
<tr>
<td>System Debug and Last Password Commands</td>
<td>8-125</td>
</tr>
<tr>
<td>System Access Commands</td>
<td>8-126</td>
</tr>
<tr>
<td>System Certificate Management Commands</td>
<td>8-129</td>
</tr>
<tr>
<td>System SNMP Commands</td>
<td>8-140</td>
</tr>
<tr>
<td>System SNMP Access Commands</td>
<td>8-141</td>
</tr>
<tr>
<td>System SNMP Traps Commands</td>
<td>8-146</td>
</tr>
<tr>
<td>System Network Time Protocol (NTP) Commands</td>
<td>8-152</td>
</tr>
<tr>
<td>System Log Commands</td>
<td>8-155</td>
</tr>
<tr>
<td>System Configuration-Update Commands</td>
<td>8-161</td>
</tr>
<tr>
<td>Firmware Update Commands</td>
<td>8-168</td>
</tr>
<tr>
<td>System Test Commands</td>
<td>8-172</td>
</tr>
<tr>
<td>Statistics Commands</td>
<td>8-175</td>
</tr>
</tbody>
</table>
Appendix A. Technical Specifications

Physical Characteristics .................................................. A-1
Electrical Characteristics ................................................ A-2
Radio Characteristics ...................................................... A-3
Antenna Specifications ..................................................... A-3
  2.4 GHz Antenna Matrix ................................................. A-4
    ML-2499-11PNA2 .......................................................... A-4
    ML-2499-APA2-0 .......................................................... A-5
    ML-2499-APA3-01 ......................................................... A-5
    ML-2499-BYGA2-01 ....................................................... A-6
  5.2 GHz Antenna Matrix ............................................... A-6
    ML-5299-APA1-01 .......................................................... A-7
    ML-5299-HPA1-01 .......................................................... A-9
    ML-5299-WPNA1-01 ....................................................... A-12
  Additional Antenna Components ........................................ A-14
  Antenna Accessory Connectors, Cable Type and Length .......... A-15
Country Codes .............................................................. A-15

Appendix B. Customer Support
Introduction

This guide provides configuration and setup information for the AP-5131 model access point.

Document Conventions

The following document conventions are used in this document:

<table>
<thead>
<tr>
<th>NOTE</th>
<th>Indicate tips or special requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAUTION</td>
<td>Indicates conditions that can cause equipment damage or data loss.</td>
</tr>
</tbody>
</table>
Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (*) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Service Information

If a problem is encountered with the AP-5131, contact the Symbol Customer Support. Refer to Appendix C for contact information. Before calling, have the model number and serial number at hand.

If the problem cannot be solved over the phone, you may need to return your equipment for servicing. If that is necessary, you will be given specific instructions.

Symbol Technologies is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty. If the original shipping container was not kept, contact Symbol to have another sent to you.
AP-5131 Introduction

The Symbol AP-5131 Access Point (AP) provides a bridge between Ethernet wired LANs or WANs and wireless networks. It provides connectivity between Ethernet wired networks and radio-equipped mobile units (MUs). MUs include the full line of Symbol terminals, bar-code scanners, adapters (PC cards, Compact Flash cards and PCI adapters) and other devices.

The AP-5131 provides a maximum 54Mbps data transfer rate via each radio. It monitors Ethernet traffic and forwards appropriate Ethernet messages to MUs over the network. It also monitors MU radio traffic and forwards MU packets to the Ethernet LAN.

The AP-5131 is available in two models:

- A single-radio version (Part No. AP-5131-4002X-WW), that can be configured as either an 802.11a access point or an 802.11b/g access point.
- A dual-radio version (Part No. AP-5131-1304X-WW), allowing both the 802.11a radio and the 802.11b/g radio to function simultaneously.

If you are new to using an access point for managing your network, refer to Theory of Operations on page 1-14 for an overview on wireless networking fundamentals.
1.1 Feature Overview

The Symbol AP-5131 has the following features:

- Single or Dual Mode Radio Options
- Separate LAN and WAN Ports
- Multiple Mounting Options
- Antenna Support for 2.4 GHz and 5.2 GHz Radios
- Sixteen Configurable WLANs
- Support for 4 BSSIDs per Radio
- Quality of Service (QoS) Support
- Industry Leading Data Security
- VLAN Support
- Multiple Management Accessibility Options
- Updatable Firmware
- Programmable SNMP v1/v2/v3 Trap Support
- Power-over-Ethernet Support
- MU-MU Transmission Disallow
- Voice Prioritization
- Support for CAM and PSP MUs
- Statistical Displays
- Transmit Power Control
- Advanced Event Logging Capability
- Configuration File Import/Export Functionality
- Default Configuration Restoration
- DHCP Support
- Multi Function LEDs

1.1.1 Single or Dual Mode Radio Options

One or two possible configurations are available on the AP-5131 depending on which model is purchased. If the AP-5131 is manufactured as a single radio access point, the AP-5131 enables you to configure the single radio for either 802.11a or 802.11b/g.
If the AP-5131 is manufactured as a dual-radio access point, the AP-5131 enables you to configure one radio for 802.11a, and the other 802.11b/g. For more information on configuring your AP-5131, see Setting the WLAN's Radio Configuration on page 5-36.

1.1.2 Separate LAN and WAN Ports

The AP-5131 has one LAN port and one WAN port, each with their own MAC address. The AP-5131 must manage all data traffic over the LAN connection carefully as either a DHCP client, BOOTP client, DHCP server or using a static IP address. The AP-5131 can only use a Power-over-Ethernet device when connected to the LAN port. For more information on configuring the AP-5131 LAN port, see Configuring the LAN Interface on page 5-1.

A Wide Area Network (WAN) is a widely dispersed telecommunications network. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet. Regardless, network address information must be configured for the AP-5131’s intended mode of operation. For information on configuring the AP-5131’s WAN port, see Configuring WAN Settings on page 5-13.

The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens. For information on locating the AP-5131 MAC addresses, see Viewing WAN Statistics on page 7-2 and Viewing LAN Statistics on page 7-5.

1.1.3 Multiple Mounting Options

The AP-5131 rests on a flat surface, attaches to a wall, mounts under a ceiling or above a ceiling (attic). Choose a mounting option based on the physical environment of the coverage area. Do not mount the AP-5131 in a location that has not been approved in an AP-5131 radio coverage site survey. For detailed information on the mounting options available for the AP-5131, see Mounting the AP-5131 on page 2-11.

1.1.4 Antenna Support for 2.4 GHz and 5.2 GHz Radios

The AP-5131 supports several 802.11a and 802.11b/g radio antennas. Select the antenna best suited to the radio transmission requirements of your coverage area. For an overview of the Radio 1 (2.4 GHz) and Radio 2 (5.2 GHz) antennas supported on the AP-5131’s Reverse SMA (RSMA) connectors, see Technical Specifications on page A-1.
1.1.5 Sixteen Configurable WLANs

A Wireless Local Area Network (WLAN) is a data-communications system that flexibly extends the functionalities of a wired LAN. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one AP-5131 to another like a cellular phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity. Sixteen WLANs are configurable on each AP-5131. To enable and configure WLANs on an AP-5131 radio, see Enabling Wireless LANs (WLANs) on page 5-22.

1.1.6 Support for 4 BSSIDs per Radio

The AP-5131 supports four BSSIDs per radio. Each BSSID has a corresponding MAC address. The first MAC address corresponds to BSSID #1. The MAC addresses for the other three BSSIDs (BSSIDs #2, #3, #4) are derived by adding 1, 2, 3, respectively, to the radio MAC address.

If the radio MAC address displayed on the Radio Settings screen is 00:A0:F8:72:20:DC, then the BSSIDs for that radio will have the following MAC addresses:

<table>
<thead>
<tr>
<th>BSSID</th>
<th>MAC Address</th>
<th>Hexadecimal Addition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID #1</td>
<td>00:A0:F8:72:20:DC</td>
<td>Same as Radio MAC address</td>
</tr>
<tr>
<td>BSSID #2</td>
<td>00:A0:F8:72:20:DD</td>
<td>Radio MAC address +1</td>
</tr>
<tr>
<td>BSSID #3</td>
<td>00:A0:F8:72:20:DE</td>
<td>Radio MAC address +2</td>
</tr>
<tr>
<td>BSSID #4</td>
<td>00:A0:F8:72:20:DF</td>
<td>Radio MAC address +3</td>
</tr>
</tbody>
</table>

For information on strategically mapping BSSIDs to WLANs, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.

1.1.7 Quality of Service (QoS) Support

The AP-5131 QoS implementation provides applications running on different wireless devices a variety of priority levels to transmit data to and from the AP-5131. Equal data transmission priority is fine for data traffic from applications such as Web browsers, file transfers or email, but is inadequate for multimedia applications. Voice over Internet Protocol (VoIP), video streaming and interactive gaming are highly sensitive to latency increases and throughput reductions. These forms of higher priority data traffic can significantly benefit from the AP-5131 QoS implementation. The WiFi Multimedia QOS Extensions (WMM) implementation used by the AP-5131 shortens the time between transmitting higher priority data traffic and is thus desirable for multimedia applications.
WMM defines four access categories (voice, video, best effort and background) to prioritize traffic to provide enhanced multimedia support. For information on configuring QoS support for the AP-5131, see Setting the WLAN Quality of Service (QoS) Policy on page 5-31.

1.1.8 Industry Leading Data Security

The AP-5131 supports numerous encryption and authentication techniques to protect the data transmitting on the WLAN.

The following authentication techniques are supported on the AP-5131:

- Kerberos Authentication
- EAP Authentication

The following encryption techniques are supported on the AP-5131:

- WEP Encryption
- KeyGuard Encryption
- Wi-Fi Protected Access (WPA) Using TKIP Encryption
- WPA2-CCMP (802.11i) Encryption

In addition, the AP-5131 supports the following additional security features:

- Firewall Security
- VPN Tunnels
- Content Filtering

For an overview on the encryption and authentication schemes available on the AP-5131, refer to Configuring Access Point Security on page 6-1.

1.1.8.1 Kerberos Authentication

Authentication is a means of verifying information that is transmitted from a secure source. If information is authentic, you know who created it and you know that it has not been altered in any way since it was originated. Authentication entails a network administrator employing a software “supplicant” on their computer or wireless device.

Authentication is critical for the security of any wireless LAN device. Traditional authentication methods are not suitable for use in wireless networks where an unauthorized user can monitor network traffic and intercept passwords. The use of strong authentication methods that do not disclose passwords is necessary. Symbol uses the Kerberos authentication service protocol (specified
in RFC 1510), to authenticate users/clients in a wireless network environment and to securely distribute the encryption keys used for both encrypting and decrypting.

A basic understanding of *RFC 1510 Kerberos Network Authentication Service (V5)* is helpful in understanding how Kerberos functions. By default, WLAN devices operate in an open system network where any wireless device can associate with an AP without authorization. Kerberos requires device authentication before access to the wired network is permitted. For additional information on configuring Kerberos, see Configuring Kerberos Authentication on page 6-9.

**1.1.8.2 EAP Authentication**

The *Extensible Authentication Protocol (EAP)* feature provides access points and their associated MU's an additional measure of security for data transmitted over the wireless network. Using EAP, authentication between devices is achieved through the exchange and verification of certificates. EAP can be used in mixed mode security with Kerberos and WEP.

EAP is a mutual authentication method whereby both the MU and AP are required to prove their identities. Like Kerberos, the user loses device authentication if the server cannot provide proof of device identification.

Using EAP, a user requests connection to a WLAN through the AP-5131. The AP-5131 then requests the identity of the user and transmits that identity to an authentication server. The server prompts the AP for proof of identity (supplied to the AP-5131 by the user) and then transmits the user data back to the server to complete the authentication.

An MU is not able to access the network if not authenticated. When configured for EAP support, the access point displays the MU as an EAP station.

EAP is only supported on mobile devices running Windows XP, Windows 2000 (using Service Pack #4) and Windows Mobile 2003. Refer to the system administrator for information on configuring a RADIUS Server for EAP (802.1x) support. For additional information on configuring EAP, see Configuring 802.1x EAP Authentication on page 6-11.

**1.1.8.3 WEP Encryption**

All WLAN devices face possible information theft. Theft occurs when an unauthorized user eavesdrops to obtain information illegally. The absence of a physical connection makes wireless links particularly vulnerable to this form of theft. Most forms of WLAN security rely on encryption to various extents. Encryption entails scrambling and coding information, typically with mathematical formulas called *algorithms*, before the information is transmitted. An algorithm is a set of instructions
or formula for scrambling the data. A \textit{key} is the specific code used by the algorithm to encrypt or decrypt the data. \textit{Decryption} is the decoding and unscrambling of received encrypted data.

The same device, host computer or front-end processor, usually performs both encryption and decryption. The data transmit or receive direction determines whether the encryption or decryption function is performed. The device takes plain text, encrypts or scrambles the text typically by mathematically combining the key with the plain text as instructed by the algorithm, then transmits the data over the network. At the receiving end, another device takes the encrypted text and decrypts, or unscrambles, the text revealing the original message. An unauthorized user can know the algorithm, but cannot interpret the encrypted data without the appropriate key. Only the sender and receiver of the transmitted data know the key.

\textit{Wired Equivalent Privacy (WEP)} is an encryption security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b and supported by the AP-5131 AP. WEP encryption is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. The level of protection provided by WEP encryption is determined by the encryption key length and algorithm. An encryption key is a string of case sensitive characters used to encrypt and decrypt data packets transmitted between a mobile unit (MU) and the AP-5131. An AP-5131 and associated wireless clients must use the same encryption key (typically 1 through 4) to interoperate. For additional information on configuring WEP, see \textit{Configuring WEP Encryption on page 6-15}.

1.1.8.4 \textbf{KeyGuard Encryption}

Use KeyGuard to shield the master encryption keys from being discovered through hacking. KeyGuard negotiation takes place between the access point and MU upon association. The access point can use KeyGuard with Symbol MUs. KeyGuard is only supported on Symbol MUs making it a Symbol proprietary security mechanism. For additional information on configuring KeyGuard on the AP-5131, see \textit{Configuring KeyGuard Encryption on page 6-17}.

1.1.8.5 \textbf{Wi-Fi Protected Access (WPA) Using TKIP Encryption}

Wi-Fi Protected Access (WPA) is a security standard for systems operating with a Wi-Fi wireless connection. WEP’s lack of user authentication mechanisms is addressed by WPA. Compared to WEP, WPA provides superior data encryption and user authentication.

WPA addresses the weaknesses of WEP by including:

- a per-packet key mixing function
- a message integrity check
- an extended initialization vector with sequencing rules
WPA uses an encryption method called Temporal Key Integrity Protocol (TKIP). WPA employs 802.1X and Extensible Authentication Protocol (EAP). For additional information on configuring WPA, see Configuring WPA Using TKIP on page 6-19.

### 1.1.8.6 WPA2-CCMP (802.11i) Encryption

WPA2 is a newer 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. Counter-mode/CBC-MAC Protocol (CCMP) is the security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Message Authentication Code (CBC-MAC) technique. Changing just one bit in a message produces a totally different result.

WPA2-CCMP is based on the concept of a Robust Security Network (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. the end result is an encryption scheme as secure as any the AP-5131 provides. For additional information on configuring WPA2-CCMP, see Configuring WPA-CCMP (802.11i) on page 6-22.

### 1.1.8.7 Firewall Security

A firewall keeps personal data in and hackers out. The AP-5131 firewall prevents suspicious Internet traffic from proliferating the AP-5131 managed network. The AP-5131 performs network address translation (NAT) on packets passing to and from the WAN port. This combination provides enhanced security by monitoring communication with the wired network. For instructions on setting the AP-5131 firewall, see Configuring Firewall Settings on page 6-25.

### 1.1.8.8 VPN Tunnels

Virtual Private Networks (VPNs) are IP-based networks using encryption and tunneling providing users remote access to a secure LAN. In essence, the trust relationship is extended from one LAN across the public network to another LAN, without sacrificing security. A VPN behaves like a private network; however, because the data travels through the public network, it needs several layers of security. The AP-5131 can function as a robust VPN gateway. For additional information on configuring VPN security on the AP-5131, see Configuring VPN Tunnels on page 6-33.
1.1.8.9 Content Filtering

Content filtering allows system administrators to block specific commands and URL extensions from going out through the AP-5131 WAN port only. Therefore, content filtering affords system administrators selective control on the content proliferating the network and is a powerful screening tool. Content filtering allows the blocking of up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

For instructions on configuring content filtering on the AP-5131, see Configuring Content Filtering Settings on page 6-48.

1.1.9 VLAN Support

A Virtual Local Area Network (VLAN) is a means to electronically separate data on the same AP-5131 from a single broadcast domain into separate broadcast domains. By using a VLAN, you can group by logical function instead of physical location. There are 16 VLANs supported on the AP-5131. An administrator can map up to 16 WLANs to 16 VLANs and enable or disable dynamic VLAN assignment. In addition to these 16 VLANs, the AP-5131 supports dynamic, user-based, VLANs when using EAP authentication.

VLANs enable organizations to share network resources in various network segments within large areas (airports, shopping malls, etc.). A VLAN is a group of clients with a common set of requirements independent of their physical location. VLANs have the same attributes as physical LANs, but they enable administrators to group clients even when they are not members of the same network segment. For more information, see Configuring VLAN Support on page 5-5.

1.1.10 Multiple Management Accessibility Options

The AP-5131 can be accessed and configured using one of the following methods:

- Java-Based Web UI
- Human readable config file (imported via FTP or TFTP)
- MIB (Management Information Base)
- Command Line Interface (CLI) accessed via RS-232 or Telnet. Use the AP-5131 DB-9 serial port for direct access to the command-line interface from a PC. Use Symbol’s Null-Modem cable (Part No. 25-632878-0) for the best fitting connection.
1.1.11 Updatable Firmware

Symbol periodically releases updated versions of the AP-5131 device firmware to the Symbol Web site. If the AP-5131 firmware version displayed on the System Settings page (see Configuring System Settings on page 4-2) is older than the version on the Web site, Symbol recommends updating the AP-5131 to the latest firmware version for full feature functionality. For instructions on updating the AP-5131 firmware using FTP or TFTP, see Updating Device Firmware on page 4-34.

1.1.12 Programmable SNMP v1/v2/v3 Trap Support

Simple Network Management Protocol (SNMP) facilitates the exchange of management information between network devices. SNMP uses Management Information Bases (MIBs) to manage the device configuration and monitor Internet devices in remote locations. MIB information accessed via SNMP is defined by a set of managed objects called object identifiers (OIDs). An object identifier (OID) is used to uniquely identify each object variable of a MIB.

SNMP allows a network administrator to configure the AP-5131, manage network performance, find and solve network problems, and plan for network growth. The AP-5131 supports SNMP management functions for gathering information from its network components. The AP-5131 CDROM and the (AP-5131 downloads site) contains the following 2 MIB files:

- Symbol-CC-WS2000-MIB-2.0 (standard Symbol MIB file)
- Symbol-AP-5131-MIB (AP-5131 specific MIB file)

The AP-5131 SNMP agent functions as a command responder and is a multilingual agent responding to SNMPv1, v2c and v3 managers (command generators). The factory default configuration maintains SNMPv1/2c support of the community names, hence providing backward compatibility. For information on configuring SNMP traps, see Configuring SNMP Settings on page 4-11.

1.1.13 Power-over-Ethernet Support

When users purchase a Symbol WLAN solution, they often need to place access points in obscure locations. In the past, a dedicated power source was required for each access point in addition to the Ethernet infrastructure. This often required an electrical contractor to install power drops at each access point location. An approved power injector solution merges power and Ethernet into one cable, reducing the burden of installation and allows optimal AP-5131 placement in respect to the intended radio coverage area. The AP-5131 can only use a Power-over-Ethernet device when connected to the LAN port.
The Symbol Power Injector (Part No. AP-PSBIAS-T-1P-AF) is a single-port, 802.3af compliant Power over Ethernet hub combining low-voltage DC with Ethernet data in a single cable connecting to the AP-5131. The Power Injector’s single DC and Ethernet data cable creates a modified Ethernet cabling environment on the AP-5131’s LAN port eliminating the need for separate Ethernet and power cables. For more information on the Symbol Power Injector, see Symbol Power Injector System on page 2-7.

1.1.14 MU-MU Transmission Disallow

The AP-5131’s MU-MU Disallow feature prohibits MUs from communicating with each other even if they are on different WLANs, assuming one of the WLAN’s is configured to disallow MU-MU communication. Therefore, if an MU’s WLAN is configured for MU-MU disallow, it will not be able to communicate with any other MUs connected to this AP-5131.

For information on configuring an AP-5131 WLAN to disallow MU to MU communications, see Creating/Editing Individual WLANs on page 5-24.

1.1.15 Voice Prioritization

Each AP-5131 WLAN has the capability of having its QoS policy configured to prioritize the network traffic requirements for associated MUs. A WLAN QoS page is available for each enabled WLAN on either the AP-5131 802.11a or 802.11b/g radio.

Use the QoS page to enable voice prioritization for devices to receive the transmission priority they may not normally receive over other data traffic. Voice prioritization allows the AP-5131 to assign priority to voice traffic over data traffic, and (if necessary) assign legacy voice supported devices (non WMM supported voice devices) additional priority. For information on configuring voice prioritization over other voice enabled devices, see Setting the WLAN Quality of Service (QoS) Policy on page 5-31.
1.1.16 Support for CAM and PSP MUs

The AP-5131 supports both CAM and PSP powered MUs. CAM (Continuously Aware Mode) MUs leave their radios on continuously to hear every beacon and message transmitted. These systems operate without any adjustments by the AP-5131. A beacon is a uniframe system packet broadcast by the AP to keep the network synchronized. A beacon includes the ESSID, AP-5131 MAC address, Broadcast destination addresses, a time stamp, a DTIM (Delivery Traffic Indication Message) and the TIM (Traffic Indication Map).

PSP (Power Save Polling) MUs power off their radios for short periods. When a Symbol MU in PSP mode associates with an AP-5131, it notifies the AP-5131 of its activity status. The AP-5131 responds by buffering packets received for the MU. PSP mode is used to extend an MU's battery life by enabling the MU to "sleep" during periods of inactivity.

1.1.17 Statistical Displays

The AP-5131 can display robust transmit and receive statistics for the WAN and LAN ports. WLAN stats can be displayed collectively and individually for enabled WLANs. Transmit and receive statistics are available for the AP-5131’s 802.11a and 802.11b/g radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated MU stats can be displayed collectively and individually for specific MUs. An echo (ping) test is also available to ping specific MUs to assess association strength. Finally, the AP-5131 can detect and display the properties of other APs detected within the AP-5131’s radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs. For information on available AP-5131 statistical displays and the values they represent, see Monitoring Statistics on page 7-1.

1.1.18 Transmit Power Control

The AP-5131 has a configurable power level for each radio. This enables the network administrator to define the antenna’s transmission power level in respect to the AP-5131’s placement or network requirements as defined in the AP-5131 site survey. For detailed instructions on setting the radio transmit power level, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.

1.1.19 Advanced Event Logging Capability

The AP-5131 provides the capability for periodically logging system events. Logging events is useful in assessing the throughput and performance of the AP-5131 or troubleshooting problems on the
AP-5131 managed Local Area Network (LAN). For more information, see *Logging Configuration on page 4-28.*

### 1.1.20 Configuration File Import/Export Functionality

Configuration settings for an AP-5131 can be downloaded from the current configuration of another AP-5131. This affords the administrator the opportunity to save the current configuration before making significant changes or restoring the default configuration. For information on importing or exporting configuration files, see *Importing/Exporting Configurations on page 4-30.*

### 1.1.21 Default Configuration Restoration

The AP-5131 has the ability to restore its default configuration or a partial default configuration with the exception of current WAN and SNMP settings. Restoring the default configuration is a good way to create new WLANs if the MUs the AP-5131 supports have been moved to different radio coverage areas. For information on restoring a default or partial default configuration, see *Configuring System Settings on page 4-2.*

### 1.1.22 DHCP Support

The AP-5131 can use *Dynamic Host Configuration Protocol (DHCP)* to obtain a leased IP address and configuration information from a remote server. DHCP is based on the BOOTP protocol and can coexist or interoperate with BOOTP. Configure the AP-5131 to send out a *DHCP request* searching for a DHCP/BOOTP server to acquire HTML, firmware or network configuration files when the AP-5131 boots. Because BOOTP and DHCP interoperate, whichever responds first becomes the server that allocates information.

The AP-5131 can be set to only accept replies from DHCP or BOOTP servers or both (this is the default setting). Disabling DHCP disables BOOTP and DHCP and requires network settings to be set manually. If running both DHCP and BOOTP, do not select BOOTP Only. BOOTP should only be used when the server is running BOOTP exclusively.

The DHCP client automatically sends a DHCP request at an interval specified by the DHCP server to renew the IP address lease as long as the AP-5131 is running (this parameter is programmed at the DHCP server). For example: Windows 2000 servers typically are set for 3 days.
1.1.23 Multi Function LEDs

The AP-5131 houses seven LED indicators. Four LEDs exist on the top of the AP-5131 and are visible from wall, ceiling and table-top orientations. Three of these four LEDs are single color activity LEDs, and one is a multi-function red and white status LED. Two LEDs exist on the rear of the AP-5131 and are viewable using a single (customer installed) extended light pipe, adjusted as required to suit above the ceiling installations. For detailed descriptions of the AP-5131 LEDs and their functionality, see LED Indicators on page 2-20.

1.2 Theory of Operations

To understand AP-5131 management and performance alternatives, users need familiarity with AP-5131 functionality and configuration options. The AP-5131 includes features for different interface connections and network management.

The AP-5131 uses electromagnetic waves to transmit and receive electric signals without wires. Users communicate with the network by establishing radio links between mobile units (MUs) and access points.

The AP-5131 uses DSSS (direct sequence spread spectrum) to transmit digital data from one device to another. A radio signal begins with a carrier signal that provides the base or center frequency. The digital data signal is encoded onto the carriers using a DSSS chipping algorithm. The AP-5131 radio signal propagates into the air as electromagnetic waves. A receiving antenna (on the MU) in the path of the waves absorbs the waves as electrical signals. The receiving MU interprets (demodulates) the signal by reapplying the direct sequence chipping code. This demodulation results in the original digital data.

The AP-5131 uses its environment (the air and certain objects) as the transmission medium. The AP-5131 can either transmit in the 2.4 to 2.5-GHz frequency range (802.11b/g radio) or the 5.2 GHz frequency range (802.11a radio), the actual range is country-dependent. Symbol devices, like other Ethernet devices, have unique, hardware encoded Media Access Control (MAC) or IEEE addresses. MAC addresses determine the device sending or receiving data. A MAC address is a 48-bit number written as six hexadecimal bytes separated by colons.

For example: 00:A0:F8:24:9A:C8

Also see the following sections:

- Cellular Coverage
- Network Topology
1.2.1 Cellular Coverage

An AP-5131 establishes an average communication range with MUs called a Basic Service Set (BSS) or cell. When in a particular cell, the MU associates and communicates with the AP-5131 supporting the radio coverage area of that cell. Adding AP-5131’s to a single LAN establishes more cells to extend the range of the network. Configuring the same ESSID (Extended Service Set Identifier) on all AP-5131’s makes them part of the same Wireless LAN.

AP-5131’s with the same ESSID defines a coverage area. A valid ESSID is an alphanumeric, case-sensitive identifier up to 32 characters. An MU searches for an AP-5131 with a matching ESSID and synchronizes (associates) to establish communications. This device association allows MUs within the coverage area to move about or roam. As the MU roams from cell to cell, it associates with a different AP-5131. The roam occurs when the MU analyzes the reception quality at a location and determines a different AP-5131 provides better signal strength and lower MU load distribution.

If the MU does not find an AP-5131 with a workable signal, it can perform a scan to find any AP. As MUs switch APs, the AP updates its association statistics.

The user can configure the ESSID to correspond to up to 16 WLANs on each 802.11a or 802.11b/g radio. A Wireless Local Area Network (WLAN) is a data-communications system that flexibly extends the functionalities of a wired LAN. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable. Within the WLAN, roaming users can be handed off from one AP-5131 to another like a cellular phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity.
1.2.2 Network Topology

The following are sample topologies:

- A single AP-5131 without a wired network establishing a single-cell wireless network for peer-to-peer MUs.
- A single AP-5131 bridging the Ethernet and radio networks.
- Two or more AP-5131s coexisting as separate, individual networks (WLANs) at the same site without interference using different ESSIDs. These separate WLANs can be configured to use different channel assignments to avoid RF interference.
Multiple AP-5131’s wired together provide a network with better coverage area and performance when using the same ESSID.

1.2.3 MAC Layer Bridging

The AP-5131 provides MAC layer bridging between its interfaces. The AP-5131 monitors traffic from its interfaces and, based on frame address, forwards the frames to the proper destination. The AP-5131 tracks source and destination addresses to provide intelligent bridging as MUs roam or network topologies change. The AP-5131 also handles broadcast and multicast messages and responds to MU association requests.

The AP-5131 listens to all packets on its LAN and WAN interfaces and builds an address database using MAC addresses. An address in the database includes the interface media that the device uses to associate with the AP-5131. The AP-5131 uses the database to forward packets from one interface
to another. The bridge forwards packets addressed to unknown systems to the Default Interface (Ethernet).

The AP-5131 internal stack interface handles all messages directed to the AP-5131. Each AP-5131 stores information on destinations and their interfaces to facilitate forwarding. When a user sends an ARP (Address Resolution Protocol) request packet, the AP-5131 forwards it over all enabled interfaces except over the interface the ARP request packet was received.

On receiving the ARP response packet, the AP-5131 database keeps a record of the destination address along with the receiving interface. With this information, the AP-5131 forwards any directed packet to the correct destination. Transmitted ARP request packets echo back to other MUs. The AP-5131 removes from its database the destination or interface information that is not used for a specified time. The AP refreshes its database when it transmits or receives data from these destinations and interfaces.

### 1.2.4 Media Types

The AP-5131 radio interface conforms to IEEE 802.11a/b/g specifications. The interface operates at a maximum 54Mbps (802.11a radio) using direct-sequence radio technology. The AP-5131 supports multiple-cell operations with fast roaming between cells. Within a direct-sequence system, each cell can operate independently. Adding cells to the network provides increased coverage area and total system capacity.

The RS-232 serial port provides a Command Line Interface (CLI) connection. The serial link supports a direct serial connection. The AP-5131 is a Data Terminal Equipment (DTE) device with male pin connectors for the RS-232 port. Connecting the AP-5131 to a PC requires a null modem serial cable.

### 1.2.5 Direct-Sequene Spread Spectrum

Spread spectrum (broadband) uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range. The Symbol AP-5131 uses Direct-Sequence Spread Spectrum (DSSS) for radio communication.

Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a chipping sequence. Each bit of transmitted data is mapped into chips by the AP-5131 and rearranged into a pseudorandom spreading code to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the AP-5131’s output signal.

MUs receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the AP-5131.
Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting AP-5131 to the receiving MU. This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving MU to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference.

The ratio of chips per bit is called the spreading ratio. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The AP-5131 uses different modulation schemes to encode more bits per chip at higher data rates. The AP-5131 is capable of a maximum 54Mbps data transmission rate (802.11a radio), but the coverage area is less than AP-5131’s operating at lower data rates since coverage area decreases as bandwidth increases.

1.2.6 MU Association Process

An AP-5131 recognizes MUs as they begin the association process with the AP-5131. An AP-5131 keeps a list of the MUs it services. MUs associate with an AP-5131 based on the following conditions:

- signal strength between the AP-5131 and MU
- number of MUs currently associated with the AP-5131
- MUs encryption and authentication capabilities
- MUs supported data rate

MUs perform pre-emptive roaming by intermittently scanning for AP-5131’s and associating with the best available AP-5131. Before roaming and associating, MUs perform full or partial scans to collect AP-5131 statistics and determine the direct-sequence channel used by the AP-5131.

Scanning is a periodic process where the MU sends out probe messages on all channels defined by the country code. The statistics enable an MU to reassociate by synchronizing its channel to the AP-5131. The MU continues communicating with that AP-5131 until it needs to switch cells or roam.

MUs perform partial scans at programmed intervals, when missing expected beacons or after excessive transmission retries. In a partial scan, the MU scans AP-5131’s classified as proximate on the AP-5131 table. For each channel, the MU tests for Clear Channel Assessment (CCA). The MU broadcasts a probe with the ESSID and broadcast BSS_ID when the channel is transmission-free. It sends an ACK to a directed probe response from the AP-5131 and updates the table.

An MU can roam within a coverage area by switching AP-5131s. Roaming occurs when:

- Unassociated MU attempts to associate or reassociate with an available AP-5131
• Supported rate changes or the MU finds a better transmit rate with another AP-5131
• \textit{RSSI} (received signal strength indicator) of a potential AP-5131 exceeds the current AP-5131
• Ratio of good-transmitted packets to attempted-transmitted packets falls below a threshold.

An MU selects the best available AP-5131 and adjusts itself to the AP-5131 direct-sequence channel to begin association. Once associated, the AP-5131 begins forwarding frames addressed to the target MU. Each frame contains fields for the current direct-sequence channel. The MU uses these fields to resynchronize to the AP-5131.

The scanning and association process continues for active MUs. This process allows the MUs to find new AP-5131’s and discard out-of-range or deactivated AP-5131’s. By testing the airwaves, the MUs can choose the best network connection available.

\textbf{1.2.7 Operating Modes}

The AP-5131 can operate in a couple of configurations.

• \textbf{Access Point} - As an Access Point, the AP-5131 functions as a layer 2 bridge (similar to Symbol’s existing AP-4131 access point). The wired uplink can operate as a trunk and support multiple VLANs. Up to 16 WLANs can be defined and mapped to AP-5131 WLANs. Each WLAN can be configured to be broadcast by one or both AP-5131 radios (unlike the AP-4131). The AP-5131 can operate in both an Access Point mode and Wireless Gateway/Router mode simultaneously. The network architecture and AP-5131 configuration define how the Access Point and Wireless Gateway/Router mode are negotiated.

• \textbf{Wireless Gateway/Router} - If operating as a Wireless Gateway/Router, the AP-5131 functions as a router between two layer 2 networks: the WAN uplink (the ethernet port) and the Wireless side. A number of options are available providing a solution for single-cell deployment:
  • \textbf{PPPoE} - The WAN interface can terminate a PPPoE connection, thus enabling the AP-5131 to operate in conjunction with a DSL or Cable modem to provide WAN connectivity.
  • \textbf{NAT} - (Network Address Translation) on the Wireless interface. Using NAT, the AP-5131 router is able to manage a private IP scheme. NAT allows translation of private addresses to the WAN IP address.
  • \textbf{DHCP} - On the Wireless side, the AP-5131 can assign private IP addresses.
  • \textbf{Firewall} - In between the WAN and Wireless interfaces, a Firewall protects against a number of known attacks.
1.2.8 Management Access Options

Managing the AP-5131 includes viewing network statistics and setting configuration options. Statistics track the network activity of associated MUs and data transfers on the AP interfaces.

The AP-5131 requires one of the following connection methods to perform a custom installation and manage the network:

- **Secure Java-Based WEB UI** - (use Sun Microsystems’ JRE 1.5 or higher available from Sun’s Web site and be sure to disable Microsoft’s Java Virtual Machine if installed)
- **Command Line Interface (CLI)** via Serial, Telnet and SSH
- **Config file** - Human-readable; Importable/Exportable via FTP and TFTP
- **MIB (Management Information Base)** accessing the AP-5131 SNMP function using a MIB Browser. The AP-5131 CDROM contains the following 2 MIB files:
  - Symbol-CC-WS2000-MIB-2.0 (standard Symbol MIB file)
  - Symbol-AP-5131-MIB (AP-5131 specific MIB file)

Make configuration changes to AP-5131’s individually. Optionally, use the AP-5131 import/export configuration function to download AP-5131’s settings to other AP-5131s. For more information, see *Importing/Exporting Configurations on page 4-30.*
An AP-5131 installation includes mounting the AP-5131 on a table-top, wall, ceiling T-bar or above the ceiling (attic or plenum), connecting the AP-5131 to the network (LAN or WAN port connection), connecting antennae and applying power. Installation procedures vary for different environments.

2.1 Precautions

Before installing the AP-5131 verify the following:

- Do not install in wet or dusty areas without additional protection. Contact a Symbol representative for more information.
- Verify the environment has a continuous temperature range between -20° C to 50° C.
2.2 Package Contents

Check package contents for the correct model AP-5131 and applicable AP-5131 accessories. Each available configuration (at a minimum), contains the following:

- AP-5131 (two models available)
- Single 802.11a/g radio, external antenna (Part No. AP-5131-4002X-WW)
- Dual 802.11a+g radios, external antenna (Part No. AP-5131-1304X-WW)
- Software and Documentation CD-ROM
- AP-5131 Install Guide (Part No. 72-70931-01)
- Accessories Bag (4 rubber feet for desk mounting and a LED light pipe, badge and label for above the ceiling installations).

2.2.1 Available Product Configurations

An AP-5131 can be ordered in the following access point and accessory combinations:

<table>
<thead>
<tr>
<th>Symbol Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP-5131-13040-WW</td>
<td>AP-5131 802.11a+g Dual Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
<tr>
<td>AP-5131-13041-WW</td>
<td>AP-5131 802.11a+g Dual Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Power Injector (Part No. AP-PSBIAS-T-1P-AF)</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
<tr>
<td>AP-5131-13042-WW</td>
<td>AP-5131 802.11a+g Dual Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>(4) Dual-Band Antennae (Part No. ML-2452-APA2-01)</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
<tr>
<td>AP-5131-13043-WW</td>
<td>AP-5131 802.11a+g Dual Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>Power Injector (Part No. AP-PSBIAS-T-1P-AF)</td>
</tr>
<tr>
<td></td>
<td>(4) Dual-Band Antennae (Part No. ML-2452-APA2-01)</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
</tbody>
</table>
Verify the model indicated on the bottom of the AP-5131 is correct. Contact the Symbol Support Center to report missing or improperly functioning items.

The Symbol power injector (Part No. AP-PSBIAS-T-1P-AF) is included in certain orderable configurations, but can be added to any configuration. For more information on the Symbol power injector, see *Symbol Power Injector System on page 2-7.*

**NOTE**

A standard Symbol 48 Volt Power Adapter (Part No. 50-24000-050) is recommended with AP-5131 product SKUs that do not include the Symbol power injector.

For an overview on the optional antennae available for the AP-5131, see *Antenna Options on page 2-5.* For detailed specifications on the 2.4 GHz and 5.2 GHz antenna suite, see *2.4 GHz Antenna Matrix on page A-4* and *5.2 GHz Antenna Matrix on page A-4.*

<table>
<thead>
<tr>
<th>Symbol Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP-5131-40020-WW</td>
<td>AP-5131 802.11a/g Single Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
<tr>
<td>AP-5131-40021-WW</td>
<td>AP-5131 802.11a/g Single Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>Power Injector (Part No. AP-PSBIAS-T-1P-AF)</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
<tr>
<td>AP-5131-40022-WW</td>
<td>AP-5131 802.11a/g Single Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>(2) Dual-Band Antennae (Part No. ML-2452-APA2-01)</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
<tr>
<td>AP-5131-40023-WW</td>
<td>AP-5131 802.11a/g Single Radio Access Point</td>
</tr>
<tr>
<td></td>
<td>AP-5131 Install Guide</td>
</tr>
<tr>
<td></td>
<td>Software and Documentation CD-ROM</td>
</tr>
<tr>
<td></td>
<td>Power Injector (Part No. AP-PSBIAS-T-1P-AF)</td>
</tr>
<tr>
<td></td>
<td>(2) Dual-Band Antennae (Part No. ML-2452-APA2-01)</td>
</tr>
<tr>
<td></td>
<td>Accessories Bag</td>
</tr>
</tbody>
</table>
2.3 Requirements

The minimum installation requirements for a single-cell, peer-to-peer network:

- AP-5131 (either the dual or single radio model)
- AP-5131 48 Volt Power Supply (Part No. 50-24000-050) or Symbol power injector (Part No. AP-PSBIAS-T-1P-AF)
- a power outlet
- Dual-Band Antennae (Part No. ML-2452-APA2-01).

2.4 Placement of the AP-5131

For optimal performance, install the AP-5131 away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators and other industrial equipment. Signal loss can occur when metal, concrete, walls or floors block transmission. Install the AP-5131 in open areas or add access points as needed to improve coverage.

Antenna coverage is analogous to lighting. Users might find an area lit from far away to be not bright enough. An area lit sharply might minimize coverage and create dark areas. Uniform antenna placement in an area (like even placement of a light bulb) provides even, efficient coverage.

Place the AP-5131 using the following guidelines:

- Install the AP-5131 at an ideal height of 10 feet from the ground.
- Orient the AP-5131 antennae vertically for best reception.
- Point the AP-5131 antenna(s) downward if attaching to the ceiling.
Symbol recommends conducting a site survey to define and document radio interference obstacles before installing the AP-5131 to maximize its radio coverage area.

### 2.4.1 Site Surveys

A site survey analyzes the installation environment and provides users with recommendations for equipment and placement. The optimum placement of 802.11a access points differs from 802.11b/g access points, because the locations and number of access points required are different to support the radio coverage area.

Symbol recommends conducting a new site survey and developing a new coverage area floor plan when switching from 2 or 11Mbps access points (AP-3021 or AP-4131 models) to 54Mbps access points (AP-5131 models), as the device placement requirements are significantly different.

### 2.4.2 Antenna Options

Both Radio 1 and Radio 2 require one antenna and can optimally use two antennae per radio (4 antennae total for dual-radio models). Two antennae per radio provides diversity that can improve performance and signal reception. Symbol supports two antenna suites for the AP-5131. One antenna suite supporting the 2.4 GHz band and another antenna suite supporting the 5.2 GHz band. Select an antenna model best suited to the intended operational environment of your AP-5131.

| NOTE | On a single-radio AP-5131, Radio 1 can be configured to be either a 2.4 GHz or 5.2 GHz radio. On a dual-radio model, Radio 1 refers to the AP-5131’s 2.4 GHz radio and Radio 2 refers to the AP-5131 5.2 GHz radio. However, there could be some cases where a dual-radio AP-5131 is performing a Rogue AP detector function. In this scenario, the AP-5131 is receiving in either 2.4 GHz or 5.2 GHz over the Radio 1 or Radio 2 antennae depending on which radio is selected for the scan. |

Antenna connectors for Radio 1 are located in a different location from the Radio 2 antenna connectors. On single radio versions, the R-SMA connectors can support both bands and should be connected to a R-SMA dual-band antenna or an appropriate single band antenna. If necessary a R-SMA to R-BNC adapter (Part No. 25-72178-01) can be purchased separately from Symbol.

The 2.4 GHz antenna suite includes the following models:

<table>
<thead>
<tr>
<th>Symbol Part Number</th>
<th>Antenna Type</th>
<th>Nominal Net Gain (dBi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML-2499-11PNA2-01</td>
<td>Wide Angle Directional</td>
<td>8.5</td>
</tr>
<tr>
<td>ML-2499-HPA3-01</td>
<td>Omni-Directional Antenna</td>
<td>3.3</td>
</tr>
</tbody>
</table>
The 5.2 GHz antenna suite includes the following models:

<table>
<thead>
<tr>
<th>Symbol Part Number</th>
<th>Antenna Type</th>
<th>Nominal Net Gain (dBi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML-2499-BYGA2-01</td>
<td>Yagi Antenna</td>
<td>13.9</td>
</tr>
<tr>
<td>ML-2452-APA2-01</td>
<td>Dual-Band</td>
<td>3.0</td>
</tr>
</tbody>
</table>

**NOTE** An additional adapter is required to use ML-2499-11PNA2-01 and ML-2499-BYGA2-01 model antennae. Please contact Symbol for more information.
For detailed specifications on the 2.4 GHz and 5.2 GHz antennae mentioned in this section, see section \textit{2.4 GHz Antenna Matrix on page A-4} and section \textit{5.2 GHz Antenna Matrix on page A-4}.

\subsection*{2.5 Power Options}

The power options for the AP-5131 include:

- Symbol Power Injector (Part No. AP-PSBIAS-T-1P-AF)
- Symbol 48-Volt Power Supply (Part No. 50-24000-050)
- Any standard 802.3af compliant device.

\subsection*{2.6 Symbol Power Injector System}

The AP-5131 can receive power either directly from a Symbol 48V AC-DC power supply (Part No. 50-24000-050) or via an Ethernet cable connected to the LAN port (using the 802.3af standard).

When users purchase a Symbol WLAN solution, they often need to place access points in obscure locations. In the past, a dedicated power source was required for each access point in addition to the Ethernet infrastructure. This often required an electrical contractor to install power drops at each access point location. An approved power injector solution merges power and Ethernet into one cable, reducing the burden of installation and allowing optimal AP-5131 placement in respect to the intended radio coverage area.

The Symbol Power Injector is included in certain AP-5131 kits. The Symbol Power Injector (Part No. AP-PSBIAS-T-1P-AF) is an integrated AC-DC converter and 802.3af power injector which requires 110-220V AC power to combine low-voltage DC with Ethernet data in a single cable.
connecting to the AP-5131. The AP-5131 can only use a Power Injector when connected to the LAN port.

The Symbol AP-5131 Power Supply (Part No. 50-24000-050) is not included in the kit and is orderable separately as an accessory.

**CAUTION** The AP-5131 supports any standards-based 802.3af compliant power source (including non-Symbol power sources). However, using the wrong solution (including a POE system used on a legacy Symbol access point) could severely damage the AP-5131 and void the product warranty.

A separate power injector is required for each AP-5131 comprising the network.
2.6.1 Installing the Power Injector

Refer to the following sections for information on planning, installing, and validating the power injector installation:

- Preparing for Site Installation
- Cabling the Power Injector
- Power Injector LED Indicators

2.6.1.1 Preparing for Site Installation

The power injector can be installed free standing, on an even horizontal surface or wall mounted using the power injector’s wall mounting key holes. The following guidelines should be adhered to before cabling the power injector to an Ethernet source and an AP-5131:

- Do not block or cover airflow to the power injector.
- Keep the power injector away from excessive heat, humidity, vibration and dust.
- The power injector is not a repeater, and does not amplify the Ethernet data signal. For optimal performance, ensure the power injector is placed as close as possible to the network data port.

2.6.1.2 Cabling the Power Injector

To install the power injector to an Ethernet data source and AP-5131:

<table>
<thead>
<tr>
<th>CAUTION</th>
<th>Ensure AC power is supplied to the power injector using an AC cable with an appropriate ground connection approved for the country of operation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Connect the power injector to an AC outlet (110VAC to 220VAC).</td>
</tr>
<tr>
<td>2.</td>
<td>Connect an RJ-45 Ethernet cable between the network data supply (host) and the power injector <strong>Data In</strong> connector.</td>
</tr>
<tr>
<td>3.</td>
<td>Connect an RJ-45 Ethernet cable between the power injector <strong>Data &amp; Power Out</strong> connector and the Symbol AP-5131 LAN port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAUTION</th>
<th>Cabling the power injector to the AP-5131’s WAN port renders the AP-5131 non-operational. Only use a AP-PSBIAS-T-1P-AF model power injector with the AP-5131’s LAN port.</th>
</tr>
</thead>
</table>
Ensure the cable length from the Ethernet source (host) to the power injector and AP-5131 does not exceed 100 meters (333 ft.)

The power injector has no On/Off power switch. The power injector receives power and is ready for AP-5131 device connection and operation as soon as AC power is applied.

### 2.6.1.3 Power Injector LED Indicators

The power injector demonstrates the following LED behavior under normal and/or problematic operating conditions:

<table>
<thead>
<tr>
<th>LED</th>
<th>AC (Main)</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green (Steady)</td>
<td>Power injector is receiving power from AC outlet.</td>
<td>Indicates a device is connected to the power injector’s outgoing Data &amp; Power cable.</td>
</tr>
<tr>
<td>Green (Blinking)</td>
<td>Output voltage source is out of range.</td>
<td>The power injector is overloaded or has a short circuit.</td>
</tr>
</tbody>
</table>
For more information and device specifications for the Symbol power injector, refer to the *Power Injector Quick Install Guide* (Part No. 72-66153-01) available from the Symbol Web site or the AP-5131 Software and documentation CDROM.

### 2.7 Mounting the AP-5131

The AP-5131 can rest on a flat surface, attach to a wall, mount under a suspended T-Bar or above a ceiling (plenum or attic). Choose one of the following mounting options based on the physical environment of the coverage area. Do not mount the AP-5131 in a location that has not been approved in a site survey.

Refer to the following, depending on how you intend to mount the AP-5131:

- Desk Mounted Installations
- Wall Mounted Installations
- Suspended Ceiling T-Bar Installations
- Above the Ceiling (Plenum) Installations

#### 2.7.1 Desk Mounted Installations

The desk mount option uses rubber feet allowing the unit to sit on most flat surfaces. The four (4) round rubber feet can be found in the AP-5131 (main) box in a separate plastic bag.

To install the AP-5131 in a desk mount orientation:

1. Turn the AP-5131 upside down.
2. Attach the radio antennae to their correct connectors.
3. Remove the backings from the four (4) rubber feet and attach them to the four rubber feet recess areas on the AP-5131.

**CAUTION** Both the Dual and Single Radio model AP-5131’s use RSMA type antenna connectors. On the Dual Radio AP-5131, a single dot on the antenna connector indicates the primary antenna for both Radio 1 (2.4 GHz) and Radio 2 (5.2 GHz). Two dots designate the secondary antenna for both Radio 1 and Radio 2. On Single Radio models, a single dot on the antenna connector indicates the primary antenna for Radio 1, and two dots designate the secondary antenna for Radio 1.
4. Cable the AP-5131 using either the Symbol power injector solution or an approved line cord and power supply.

**CAUTION** Do not supply power to the AP-5131 until the cabling of the unit is complete.

For Symbol power injector installations:

a. Connect a RJ-45 Ethernet cable between the network data supply (host) and the power injector **Data In** connector.

b. Connect a RJ-45 Ethernet cable between the power injector **Data & Power Out** connector and the Symbol AP-5131 LAN port.

c. Ensure the cable length from the Ethernet source (host) to the power injector and AP-5131 does not exceed 100 meters (333 ft). The power injector has no On/Off power switch. The power injector receives power as soon as AC power is applied. For more information on using the power injector, see *Symbol Power Injector System on page 2-7*.

For standard Symbol 48-Volt power adapter (Part No. 50-24000-050) and line cord installations:

a. Connect RJ-45 Ethernet cable between the network data supply (host) and the AP-5131 LAN port.

b. Verify the power adapter is correctly rated according the country of operation.

c. Connect the power supply line cord to the power adapter.

d. Attach the power adapter cable into the power connector on the AP-5131.

e. Plug the power adapter into an outlet.
5. Verify the behavior of the AP-5131 LEDs. For more information, see *LED Indicators on page 2-20*.

6. Return the AP-5131 to an upright position and place it in the location you wish it to operate. Ensure the AP-5131 is sitting evenly on all four rubber feet.

The AP-5131 is ready to configure. For information on an AP-5131 default configuration, see *Getting Started on page 3-1*. For specific details on AP-5131 system configurations, see *System Configuration on page 4-1*.

### 2.7.2 Wall Mounted Installations

Wall mounting requires hanging the AP-5131 along its width (or length) using the pair of slots on the bottom of the unit and using the AP-5131 itself as a mounting template for the screws. The AP-5131 can be mounted onto any plaster or wood wall surface.

The mounting hardware and tools (customer provided) required to install the AP-5131 on a wall consists of:

- Two Phillips pan head self-tapping screws (ANSI Standard) #6-18 X 0.875in. Type A or AB Self-Tapping screw, or (ANSI Standard Metric) M3.5 X 0.6 X 20mm Type D Self-Tapping screw
- Two wall anchors
- Security cable (optional)

To mount the AP-5131 on a wall:

1. Orient the AP-5131 on the wall by its width or length.
2. Using the arrows on one edge of the case as guides, move the edge to the midline of the mounting area and mark points on the midline for the screws.
3. At each point, drill a hole in the wall, insert an anchor, screw into the anchor the wall mounting screw and stop when there is 1mm between the screw head and the wall. If pre-drilling a hole, the recommended hole size is 2.8mm (0.11in.) if the screws are going directly into the wall and 6mm (0.23in.) if wall anchors are being used.
4. If required, install and attach a security cable to the AP-5131 lock port.
5. Place the large corner of each of the mount slots over the screw heads.
6. Slide the AP-5131 down along the mounting surface to hang the mount slots on the screw heads.
7. Attach the radio antennae to their correct connectors.
8. Cable the AP-5131 using either the Symbol power injector solution or an approved line cord and power supply.

**CAUTION** Both the Dual and Single Radio model AP-5131s use RSMA type antenna connectors. On the Dual Radio AP-5131, a single dot on the antenna connector indicates the primary antenna for both Radio 1 (2.4 GHz) and Radio 2 (5.2 GHz). Two dots designate the secondary antenna for both Radio 1 and Radio 2. On Single Radio models, a single dot on the antenna connector indicates the primary antenna for Radio 1, and two dots designate the secondary antenna for Radio 1.

**NOTE** The AP-5131 must be mounted with the RJ45 cable connector oriented upwards to ensure proper operation.

**CAUTION** Do not supply power to the AP-5131 until the cabling of the unit is complete.

For Symbol power injector installations:

a. Connect a RJ-45 Ethernet cable between the network data supply (host) and the Power Injector Data In connector.

b. Connect a RJ-45 Ethernet cable between the power injector Data & Power Out connector and the AP-5131 LAN port.

c. Ensure the cable length from the Ethernet source (host) to the power injector and AP-5131 does not exceed 100 meters (333 ft). The power injector has no On/Off power switch. The power injector receives power as soon as AC power is applied. For more information on using the power injector, see Symbol Power Injector System on page 2-7.

For standard Symbol 48-Volt Power Adapter (Part No. 50-24000-050) and line cord installations:

a. Connect RJ-45 Ethernet cable between the network data supply (host) and the AP-5131 LAN port.

b. Verify the power adapter is correctly rated according the country of operation.

c. Connect the power supply line cord to the power adapter.

d. Attach the power adapter cable into the power connector on the AP-5131.
e. Plug the power adapter into an outlet.

**NOTE** If the AP-5131 is utilizing remote management antennae, a wire cover can be used to provide a clean finished look to the installation. Contact Symbol for more information.

9. Verify the behavior of the AP-5131 LEDs. For more information, see *LED Indicators on page 2-20*.

   The AP-5131 is ready to configure. For information on an AP-5131 default configuration, see *Getting Started on page 3-1*. For specific details on AP-5131 system configurations, see *System Configuration on page 4-1*.

### 2.7.3 Suspended Ceiling T-Bar Installations

A suspended ceiling mount requires holding the AP-5131 up against the T-bar of a suspended ceiling grid and twisting the AP-5131 chassis onto the T-bar.

The mounting hardware and tools (customer provided) required to install the AP-5131 on a ceiling T-bar consists of:

- Safety wire (recommended)
- Security cable (optional)

To install the AP-5131 on a ceiling T-bar:

1. If required, loop a safety wire —with a diameter of at least 1.01 mm (.04 in.), but no more than 0.158 mm (.0625 in.) —through the tie post (above the AP-5131’s console connector) and secure the loop.
2. If required, install and attach a security cable to the AP-5131 lock port.
3. Attach the radio antennae to their correct connectors.

**CAUTION** Both the Dual and Single Radio model AP-5131s use RSMA type antenna connectors. On the Dual Radio AP-5131, a single dot on the antenna connector indicates the primary antenna for both Radio 1 (2.4 GHz) and Radio 2 (5.2 GHz). Two dots designate the secondary antenna for both Radio 1 and Radio 2. On Single Radio models, a single dot on the antenna connector indicates the primary antenna for Radio 1, and two dots designate the secondary antenna for Radio 1.
4. Cable the AP-5131 using either the Symbol power injector solution or an approved line cord and power supply.

**CAUTION** Do not supply power to the AP-5131 until the cabling of the unit is complete.

For Symbol power injector installations:
- a. Connect a RJ-45 Ethernet cable between the network data supply (host) and the Power Injector **Data In** connector.
- b. Connect a RJ-45 Ethernet cable between the power injector **Data & Power Out** connector and the AP-5131 LAN port.
- c. Ensure the cable length from the Ethernet source (host) to the power injector and AP-5131 does not exceed 100 meters (333 ft). The power injector has no On/Off power switch. The power injector receives power as soon as AC power is applied. For more information on using the power injector, see *Symbol Power Injector System on page 2-7*.

For standard Symbol 48-Volt Power Adapter (Part No. 50-24000-050) and line cord installations:
- a. Connect RJ-45 Ethernet cable between the network data supply (host) and the AP-5131 LAN port.
- b. Verify the power adapter is correctly rated according the country of operation.
- c. Connect the power supply line cord to the power adapter.
- d. Attach the power adapter cable into the power connector on the AP-5131.
- e. Plug the power adapter into an outlet.

5. Verify the behavior of the AP-5131 LEDs. For more information, see *LED Indicators on page 2-20*.

6. Align the bottom of the ceiling T-bar with the back of the AP-5131.

7. Orient the AP-5131 chassis by its length and the length of the ceiling T-bar.

8. Rotate the AP-5131 chassis 45 degrees clockwise, or about 10 o’clock.

9. Push the back of the AP-5131 chassis on to the bottom of the ceiling T-bar.

**CAUTION** Ensure the safety wire and cabling used in the T-Bar AP-5131 installation is securely fastened to the building structure in order to provide a safe operating environment.
10. Rotate the AP-5131 chassis 45 degrees counter-clockwise. The clips click as they fasten to the T-bar.

11. The AP-5131 is ready to configure. For information on an AP-5131 default configuration, see Getting Started on page 3-1. For specific details on AP-5131 system configurations, see System Configuration on page 4-1.

**NOTE** If the AP-5131 is utilizing remote management antennae, a wire cover can be used to provide a clean finished look to the installation. Contact Symbol for more information.

2.7.4 Above the Ceiling (Plenum) Installations

An AP-5131 above the ceiling installation requires placing the AP-5131 above a suspended ceiling and installing the provided light pipe under the ceiling tile for viewing the rear panel status LEDs of the unit. An above the ceiling AP-5131 installation enables installations compliant with drop ceilings, suspended ceilings and industry standard tiles from .625 to .75 inches thick.

**NOTE** The AP-5131 is Plenum rated to UL2043 and NEC1999 to support above the ceiling installations.
The mounting hardware required to install the AP-5131 above a ceiling consists of:

- Light pipe
- Badge for light pipe
- Decal for badge
- Safety wire (strongly recommended)
- Security cable (optional)

To install the AP-5131 above a ceiling:

1. If possible, remove the adjacent ceiling tile from its frame and place it aside.
2. Install a safety wire, between 1.5mm (.06in.) and 2.5mm (.10in.) in diameter, in the ceiling space.
3. If required, install and attach a security cable to the AP-5131's lock port.
4. Mark a point on the finished side of the tile where the light pipe is to be located.
5. Create a light pipe path hole in the target position on the ceiling tile.
6. Use a drill to make a hole in the tile the approximate size of the AP-5131 LED light pipe.

**CAUTION** Symbol recommends care be taken not to damage the finished surface of the ceiling tile when creating the light pipe hole and installing the light pipe.

7. Remove the light pipe's rubber stopper before installing the light pipe.
8. Connect the light pipe to the bottom of the AP-5131. Align the tabs and rotate approximately 90 degrees. Do not over tighten.

**CAUTION** Symbol does not recommend mounting the AP-5131 directly to any suspended ceiling tile with a thickness less than 12.7mm (0.5in.) or a suspended ceiling tile with an unsupported span greater than 660mm (26in.). Symbol strongly recommends fitting the AP-5131 with a safety wire suitable for supporting the weight of the device. The safety wire should be a standard ceiling suspension cable or equivalent steel wire between 1.59mm (.062in.) and 2.5mm (.10in.) in diameter.
9. Snap the clips of the light pipe into the bottom of the AP-5131.
10. Fit the light pipe into hole in the tile from its unfinished side.
11. Place the decal on the back of the badge and slide the badge onto the light pipe from the finished side of the tile.
12. Attach the radio antennae to their correct connectors.

**CAUTION** Both the Dual and Single Radio model AP-5131s use RSMA type antenna connectors. On the Dual Radio AP-5131, a single dot on the antenna connector indicates the primary antenna for both Radio 1 (2.4 GHz) and Radio 2 (5.2 GHz). Two dots designate the secondary antenna for both Radio 1 and Radio 2. On Single Radio models, a single dot on the antenna connector indicates the primary antenna for Radio 1, and two dots designate the secondary antenna for Radio 1.

13. Attach safety wire (if used) to the AP-5131 safety wire tie point or security cable (if used) to the AP-5131’s lock port.
14. Align the ceiling tile into its former ceiling space.
15. Cable the AP-5131 using either the Symbol power injector solution or an approved line cord and power supply.

**CAUTION** Do not supply power to the AP-5131 until the cabling of the unit is complete.
For Symbol power injector installations:

a. Connect a RJ-45 Ethernet cable between the network data supply (host) and the Power Injector **Data In** connector.

b. Connect a RJ-45 Ethernet cable between the power injector **Data & Power Out** connector and the AP-5131 LAN port.

c. Ensure the cable length from the Ethernet source (host) to the power injector and AP-5131 does not exceed 100 meters (333 ft). The power injector has no On/Off power switch. The power injector receives power as soon as AC power is applied. For more information on using the power injector, see *Symbol Power Injector System on page 2-7*.

For standard Symbol 48-Volt Power Adapter (Part No. 50-24000-050) and line cord installations:

a. Connect RJ-45 Ethernet cable between the network data supply (host) and the AP-5131 LAN port.

b. Verify the power adapter is correctly rated according the country of operation.

c. Connect the power supply line cord to the power adapter.

d. Attach the power adapter cable into the power connector on the AP-5131.

e. Plug the power adapter into an outlet.

16. Verify the behavior of the AP-5131 LED lightpipe. For more information, see *LED Indicators on page 2-20*.

17. Place the ceiling tile back in its frame and verify it is secure.

The AP-5131 is ready to configure. For information on an AP-5131 default configuration, see *Getting Started on page 3-1*. For specific details on AP-5131 system configurations, see *System Configuration on page 4-1*.

### 2.8 LED Indicators

The AP-5131 utilizes seven LED indicators. Five LEDs display within four LED slots on the front of the AP-5131 (on top of the AP-5131 housing) and two LEDs (for above the ceiling installations) are located on the back of the device (the side containing the LAN, WAN and antenna connectors).
The five LEDs on the top housing of the AP-5131 are clearly visible in table-top, wall and below ceiling installations. The five AP-5131 top housing LEDs have the following display and functionality:

**Power Status**

Solid **white** indicates the AP-5131 is adequately powered.

**Error Conditions**

Solid **red** indicates the AP-5131 is experiencing a problem condition requiring immediate attention.

**Ethernet Activity**

Flashing **white** indicates data transfers and Ethernet activity.

**802.11a Radio Activity**

Flickering **amber** indicates beacons and data transfers over the AP-5131 802.11a radio.

**802.11b/g Radio Activity**

Flickering **green** indicates beacons and data transfers over the AP-5131 802.11b/g radio.

The LEDs on the rear of the AP-5131 are viewed using a single (customer installed) extended lightpipe, adjusted as required to suit above the ceiling installations. The LEDs displayed using the lightpipe have the following color display and functionality:
2.9 Setting Up MUs

For a discussion of how to initially test the AP-5131 to ensure it can interoperate with the MUs intended for its operational environment, see Basic Device Configuration on page 3-3 and specifically Testing Connectivity on page 3-11.

Refer to the LA-5030 & LA-5033 Wireless Networker PC Card and PCI Adapter Users Guide, available from the Symbol Web site, for installing drivers and client software if operating in an 802.11a/g network environment.


Use the default values for the ESSID and other configuration parameters until the network connection is verified. MUs attach to the network and interact with the AP transparently.
The AP-5131 should be installed in an area tested for radio coverage using one of the site survey tools available to the Symbol field service technician. Once an installation site has been identified, the installer should carefully follow the hardware precautions, requirements, mounting guidelines and power options outlined in Hardware Installation on page 2-1.

3.1 Installing the AP-5131

Make the required cable and power connections before mounting the AP-5131 in its final operating position. Test the AP-5131 with an associated MU before mounting and securing the AP-5131. Carefully follow the mounting instructions in one of the following sections to ensure the AP-5131 is installed correctly:

- For instructions on installing the AP-5131 on a table top, see Desk Mounted Installations on page 2-11.
- For instructions on mounting an AP-5131 to a wall, see Wall Mounted Installations on page 2-13.
3.2 Configuration Options

Once installed and powered, the AP-5131 can be configured using one of several connection techniques. Managing the AP-5131 includes viewing network statistics and setting configuration options. The AP-5131 requires one of the following connection methods to manage the network:

- **Secure Java-Based WEB UI** - (use Sun Microsystems’ JRE 1.5 or higher available from Sun’s Web site. Disable Microsoft’s Java Virtual Machine if installed). For information on using the Web UI to set AP-5131 default configuration values, see Basic Device Configuration on page 3-3 or chapters 4 through 7 of this guide.

- **Command Line Interface (CLI)** via Serial, Telnet and SSH. The AP-5131 CLI is accessed through the AP-5131 RS232 port, via Telnet or SSH. The CLI follows the same configuration conventions as the device user interface with a few documented exceptions. For details on using the CLI to manage the AP-5131, see Command Line Interface Reference on page 8-1.

- **Config file** - Readable text file; Importable/Exportable via FTP, TFTP and HTTP. Configuration settings for an AP-5131 can be downloaded from the current configuration of another AP-5131 meeting the import/export requirements. For information on importing or exporting configuration files, see Importing/Exporting Configurations on page 4-30.

- **MIB (Management Information Base)** accessing the AP-5131 SNMP functions using a MIB Browser. The AP-5131 CDROM contains the following 2 MIB files:
  - Symbol-CC-WS2000-MIB-2.0 (standard Symbol MIB file)
  - Symbol-AP-5131-MIB (AP-5131 specific MIB file)
3.3 Basic Device Configuration

For the basic setup described in this section, the Java-based Web UI will be used to configure the AP-5131. Use the AP-5131’s LAN interface for establishing a link with the AP-5131. Configure the AP-5131 as a DHCP client. For optimal screen resolution, set your screen resolution to 1024 x 768 pixels or greater.

1. Start Internet Explorer and enter the following IP address in the address field: 192.168.0.1

   ![AP-5131 login screen](image)

   **NOTE** DNS names are not supported as a valid IP address for the AP-5131. The user is required to enter a numerical IP address.

   **NOTE** For optimum compatibility, use Sun Microsystems’ JRE 1.5 or higher (available from Sun’s Website), and be sure to disable Microsoft’s Java Virtual Machine if installed.

   The AP-5131 login screen displays.

2. Log in using `admin` as the default User ID and `symbol` as the default Password.
3. If the default login is successful, the Change Admin Password window displays. Change the password.

![Change Admin Password Window](image)

Enter the current password and a new admin password in fields provided, and click Apply. Once the admin password has been updated, a warning message displays stating the AP-5131 must be set to a country.

**NOTE**

Though the AP-5131 can have its basic settings defined using a number of different screens, Symbol recommends using the AP-5131 Quick Setup screen to set the correct country of operation and define its minimum required configuration from one convenient location.

### 3.3.1 Configuring Device Settings

Configure a set of minimum required device settings within the AP-5131 Quick Setup screen. The values defined within the Quick Setup screen are also configurable in numerous other locations within the AP-5131 menu tree. When you change the settings in the Quick Setup screen, the values also change within the screen where these parameters also exist. Additionally, if the values are updated in these other screens, the values initially set within the Quick Setup screen will be updated.

To define a basic AP-5131 configuration:

1. Select **System Configuration -> Quick Setup** from the AP-5131 menu tree, if the Quick Setup screen is not already displayed.
2. Enter a **System Name** for the AP-5131.

   The System Name is useful if multiple Symbol devices are being administered.

3. Select the **Country** for the AP-5131’s country of operation from the drop-down menu.

   The AP-5131 prompts the user for the correct country code on the first login. A warning message also displays stating that an incorrect country settings may result in illegal radio operation. Selecting the correct country is central to legally operating the AP-5131. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. To ensure compliance with national and local laws, be sure to set the Country accurately. CLI and MIB users cannot configure their AP-5131 until a two character country code (for example, United States - us) is set. Refer to **Country Codes on page A-5** for the two character country codes.

**NOTE**  
The System Name and Country are also configurable within the **System Settings** screen. Refer to **Configuring System Settings on page 4-2** (if necessary) to set a system location and admin email address for the AP-5131 or to view other default settings.
4. Optionally enter the IP address of the server used to provide system time to the AP-5131 within the Time Server field.

**NOTE** DNS names are not supported as a valid IP address. The user is required to enter a numerical IP address.

Once the IP address is entered, the AP-5131’s Network Time Protocol (NTP) functionality is engaged automatically. Refer to the AP-5131 Product Reference Guide for information on defining alternate time servers and setting a synchronization interval for the AP-5131 to adjust its displayed time. Refer to Configuring Network Time Protocol (NTP) on page 4-26 (if necessary) for information on setting alternate time servers and setting a synchronization interval for the AP-5131 to adjust its displayed time.

5. Click the **WAN** tab to set a minimum set of parameters for using the WAN interface.
   a. Select the **Enable WAN Interface** checkbox to enable a connection between the AP-5131 and a larger network or outside world through the WAN port. Disable this option to effectively isolate the AP-5131’s WAN connection. No connections to a larger network or the Internet will be possible. MUs cannot communicate beyond the configured subnets.
   b. Select the **This Interface is a DHCP Client** checkbox to enable DHCP for the AP-5131 WAN connection. This is useful, if the larger corporate network or Internet Service Provider (ISP) uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway.

**NOTE** Symbol recommends that the WAN and LAN ports should not both be configured as DHCP clients.

c. Specify an **IP address** for the AP-5131’s WAN connection. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1 (no DNS names supported).

d. Specify a **Subnet Mask** for the AP-5131’s WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the AP-5131 connects to a larger network. A subnet mask uses a series of four numbers expressed in dot notation. For example, 255.255.255.0 is a valid subnet mask.

e. Define a **Default Gateway** address for the AP-5131’s WAN connection. The ISP or a network administrator provides this address.
f. Specify the address of a **Primary DNS Server**. The ISP or a network administrator provides this address.

6. Optionally, use the **Enable PPP over Ethernet** checkbox to enable **Point-to-Point over Ethernet (PPPoE)** for a high-speed connection that supports this protocol. Most DSL providers are currently using or deploying this protocol. PPPoE is a data-link protocol for dialup connections. PPPoE will allow the AP-5131 to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data networks.

   a. Select the **Keep Alive** checkbox to enable occasional communications over the WAN port even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive maintains the WAN connection, even when there is no traffic. If the ISP drops the connection after the idle time, the AP-5131 automatically reestablishes the connection to the ISP.

   b. Specify a **Username** entered when connecting to the ISP. When the Internet session begins, the ISP authenticates the username.

   c. Specify a **Password** entered when connecting to the ISP. When the Internet session starts, the ISP authenticates the password.

   For additional AP-5131 WAN port configuration options, see *Configuring WAN Settings on page 5-13*.

7. Click the **LAN** tab to set a minimum set of parameters to use the AP-5131 LAN interface.

   a. Select the **Enable LAN Interface** checkbox to forward data traffic over the AP-5131 LAN connection. The LAN connection is enabled by default.

   b. Use the **This Interface** drop-down menu to specify how network address information is defined over the AP-5131’s LAN connection. Select **DHCP Client** if the larger corporate network uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. Select **DHCP Server** to use the AP-5131 as a DHCP server over the LAN connection. Select the **Bootp client** option to enable a diskless system to discover its own IP address.

   **NOTE**  Symbol recommends that the WAN and LAN ports should not both be configured as DHCP clients.
c. If using the static or DHCP Server option, enter the network-assigned IP Address of the AP-5131.

| NOTE | DNS names are not supported as a valid IP address for the AP-5131. The user is required to enter a numerical IP address. |

| NOTE | The Subnet Mask defines the size of the subnet. The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission. |

d. If using the static or DHCP Server option, enter a Default Gateway to define the numerical IP address of a router the AP-5131 uses on the Ethernet as its default gateway.

e. If using the static or DHCP Server option, enter the Primary DNS Server numerical IP address.

g. If using the DHCP Server option, use the Address Assignment Range parameter to specify a range of IP address reserved for mapping clients to IP addresses. If a manually (static) mapped IP address is within the IP address range specified, that IP address could still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

For additional AP-5131 LAN port configuration options, see Configuring the LAN Interface on page 5-1.

8. Enable the radio(s) using the Radio Enable checkbox(es). If using a single radio AP-5131, enable the radio, then select either 2.4 GHz or 5.2 GHz from the RF Band of Operation field. Only one RF band option at a time is permissible in a single-radio AP-5131. If using a dual-radio AP-5131, the user can enable both RF bands. For additional AP-5131 radio configuration options, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.

9. Select the WLAN #1 tab (WLANs 1 - 4 are available within the Quick Setup screen) to define its ESSID and security scheme for basic operation.

| NOTE | A maximum of 16 WLANs are configurable within the AP-5131 Wireless Configuration screen. The limitation of 16 WLANs exists regardless of whether the AP-5131 is a single or dual-radio model. |

a. Enter the Extended Services Set Identification (ESSID) and name associated with the WLAN. For additional information on creating and editing up to 16 WLANs per AP-5131, see Creating/Editing Individual WLANs on page 5-24.
b. Use the **Available On** checkboxes to define whether the target WLAN is operating over the 802.11a or 802.11b/g radio. Ensure the radio selected has been enabled (see step 8).

c. Even an AP-5131 configured with minimal values must protect its data against theft and corruption. A security policy should be configured for WLAN1 as part of the basic configuration outlined in this guide. A security policy can be configured for the WLAN from within the **Quick Setup** screen. Policies can be defined over time and saved to be used as needed as the AP-5131’s security requirements change. Symbol recommends you familiarize yourself with the security options available on the AP-5131 before defining a security policy. Refer to [Configuring WLAN Security Settings on page 3-9](#).

10. Click **Apply** to save any changes to the AP-5131 Quick Setup screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

11. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the AP-5131 Quick Setup screen to the last saved configuration.

### 3.3.1.1 Configuring WLAN Security Settings

To configure a basic security policy for a WLAN:

1. From the AP-5131 Quick Setup screen, click the **Create** button to the right of the Security Policy item.

   The **New Security Policy** screen displays with the **Manually Pre-shared key/No authentication** and **No Encryption** options selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a guest network wherein no sensitive data is either transmitted or received. Consequently, at a minimum, a basic security scheme (in this case WEP 128) is recommended in a network environment wherein sensitive data is transmitted.

   **NOTE** For information on configuring the other encryption and authentication options available to the AP-5131, see [Configuring Security Options on page 6-2](#).

2. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.

   Multiple WLANs can share the same security policy, so be careful not to name security policies after specific WLANs or risk defining a WLAN to single policy. Symbol recommends naming the policy after the attributes of the authentication or encryption type selected.

3. Select the **WEP 128 (104 bit key)** checkbox.
The **WEP 128 Settings** field displays within the New Security Policy screen.

4. Configure the **WEP 128 Settings** field as required to define the Pass Key used to generate the WEP keys.

   **Pass Key** Specify a 4 to 32 character pass key and click the **Generate** button. The AP-5131, other proprietary routers and Symbol MUs use the same algorithm to convert an ASCII string to the same hexadecimal number. Non-Symbol clients and devices need to enter WEP keys manually as hexadecimal numbers. The AP-5131 and its target client(s) must use the same pass key to interoperate.
5. Click the **Apply** button to save the security policy and return to the AP-5131 Quick Setup screen.

At this point, you can test the AP-5131 for MU interoperability.

### 3.3.2 Testing Connectivity

Verify the AP-5131’s link with an MU by sending *Wireless Network Management Protocol (WNMP)* ping packets to the associated MU. Use the Echo Test screen to specify a target MU and configure the parameters of the test. The WNMP ping test only works with Symbol MUs. Only use a Symbol MU to test AP-5131 connectivity using WNMP.

To ping a specific MU to assess its connection with an AP-5131:

<table>
<thead>
<tr>
<th><strong>NOTE</strong></th>
<th>Before testing for connectivity, the target MU needs to be set to the same ESSID as the AP-5131. Since WEP 128 has been configured for the AP-5131, the MU also needs to be configured for WEP 128 and use the same WEP keys. Ensure the MU is associated with the AP-5131 before testing for connectivity.</th>
</tr>
</thead>
</table>

1. Select **Status and Statistics** -> **MU Stats** from the AP-5131 menu tree.
2. Select the **Echo Test** button from within the **MU Stats Summary** screen.
3. Define the following parameters for the test.

| **Station Address** | The station address is the IP address of the target MU. Refer to the MU Stats Summary screen for associated MU IP address information. |
| **Number of pings** | Defines the number of packets to be transmitted to the MU. The default is 100. |
3.3.3 Where to Go from Here?

Once basic connectivity has been verified, the AP-5131 can be fully configured to meet the needs of the network and the users it supports. Refer to the following:

- For detailed information on AP-5131 device access, SNMP settings, network time, importing/exporting device configurations and device firmware updates, see Chapter 4, System Configuration on page 4-1.
- For detailed information on configuring AP-5131 LAN interface (subnet) and WAN interface see, Chapter 5, Network Management on page 5-1.
- For detailed information on configuring specific encryption and authentication security schemes for individual AP-5131 WLANs, see Chapter 6, Configuring Access Point Security on page 6-1.
- To view detailed statistics on the AP-5131 and its associated MUs, see Monitoring Statistics on page 7-1.

Packet Length

Specifies the length of each packet transmitted to the MU during the test. The default length is 100 bytes.

4. Click the Ping button to begin transmitting packets to the specified MU address.

Refer to the Number of Responses value to assess the number of responses from the MU versus the number of ping packets transmitted by the AP-5131. Use the ratio of packets sent versus the number of packets received the link quality between the MU and the AP-5131.

Click the OK button to exit the Echo Test screen and return to the MU Stats Summary screen.
The Symbol AP-5131 contains a built-in browser interface for system configuration and remote management using a standard Web browser such as Microsoft Internet Explorer, Netscape Navigator or Mozilla Firefox. The browser interface also allows for system monitoring of the AP.

Web management of the AP-5131 requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

To connect to the AP, the AP-5131 IP is required. Enter 192.168.0.1 for the default IP address. The password is “symbol.”

---

**NOTE**

For optimum compatibility, use Sun Microsystems’ JRE 1.5 or higher (available from Sun’s Web site), and be sure to disable Microsoft’s Java Virtual Machine if installed.

---

**NOTE**

DNS names are not supported as a valid IP address for the AP-5131. The user is required to enter a numerical IP address.
System configuration topics include:

- Configuring System Settings
- Configuring Data Access
- Managing Certificate Authority (CA) Certificates
- Configuring SNMP Settings
- Configuring Network Time Protocol (NTP)
- Logging Configuration
- Importing/Exporting Configurations
- Updating Device Firmware

4.1 Configuring System Settings

Use the System Settings screen to specify the name and location of the AP-5131, assign an email address for the network administrator, restore the AP’s default configuration or restart the AP.

To configure System Settings for the AP-5131:

1. Select System Configuration -> System Settings from the AP-5131 menu tree.
2. Configure the AP-5131 **System Settings** field to assign a system name and location, set the country of operation and view device version information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Name</strong></td>
<td>Specify a device name for the AP-5131. Symbol recommends selecting a name serving as a reminder of the user base the AP-5131 supports (engineering, retail, etc.).</td>
</tr>
<tr>
<td><strong>System Location</strong></td>
<td>Enter the location of the AP-5131. The <strong>System Location</strong> parameter acts as a reminder of where the AP can be found. Use the System Name field as a specific identifier of device location. Use the System Name and System Location fields together to optionally define the AP name by the radio coverage it supports and specific physical location. For example, &quot;second floor engineering&quot;</td>
</tr>
<tr>
<td><strong>Admin Email Address</strong></td>
<td>Specify the AP administrator’s email address.</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>The AP-5131 prompts the user for the correct country code after the first login. A warning message also displays stating that an incorrect country setting will lead to an illegal use of the AP-5131. Use the pull-down menu to select the country of operation. Selecting the correct country is extremely important. Each country has its own regulatory restrictions concerning electromagnetic emissions (channel range) and the maximum RF signal strength transmitted. To ensure compliance with national and local laws, be sure to set the <strong>Country</strong> field correctly. If using the AP-5131 configuration file, CLI or MIB to configure the AP-5131’s country code, see <a href="#">Country Codes on page A-5</a>.</td>
</tr>
<tr>
<td><strong>AP-5131 Version</strong></td>
<td>The displayed number is the current version of the AP-5131 device firmware. Use this information to determine if the AP is running the most recent firmware available from Symbol. Use the <strong>Firmware Update</strong> screen to keep the AP’s firmware up to date. For more information, see <a href="#">Updating Device Firmware on page 4-34</a>.</td>
</tr>
<tr>
<td><strong>System Uptime</strong></td>
<td>Displays the current uptime of the AP-5131 defined in the System Name field. <strong>System Uptime</strong> is the cumulative time since the AP-5131 was last rebooted or lost power.</td>
</tr>
</tbody>
</table>
3. Refer to the **Factory Defaults** field to restore either a full or partial default configuration.

   **Serial Number**: Displays the AP-5131 Media Access Control (MAC) address. The AP-5131 MAC address is hard coded at the factory and cannot be modified. The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens. For information on locating the AP-5131 MAC addresses, see Viewing WAN Statistics on page 7-2 and Viewing LAN Statistics on page 7-5.

4. Use the **Restart** AP-5131 field to restart the AP (if necessary).

   **Restart AP-5131**: Click the **Restart** AP-5131 button to reboot the AP. Restarting the AP-5131 resets all data collection values to zero. Symbol does not recommend restarting the AP during significant system uptime or data collection activities.

5. Click **Apply** to save any changes to the System Settings screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

---

**NOTE**

The **Apply** button is not needed for restoring the AP-5131 default configuration or restarting the AP-5131.
6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the System Settings screen to the last saved configuration.

7. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 4.2 Configuring Data Access

Use the AP-5131 **Access** screen to enable/disable data throughput to the AP-5131’s LAN and WAN interfaces and display screens for changing administrator passwords.

Use the AP-5131 Access screen checkboxes to enable or disable LAN and/or WAN access using the protocols and ports listed. If access is disabled, this effectively locks out the AP administrator from configuring the AP-5131 using that interface. To avoid jeopardizing the network data managed by the AP-5131, Symbol recommends enabling only those interfaces used in the routine (daily) management of the network, and disabling all other interfaces until they are required.

To configure access for the AP-5131:

1. Select **System Configuration** -> **AP-5131 Access** from the AP-5131 menu tree.
2. Use the AP-5131 **Access** field checkboxes to enable/disable the following AP-5131 interfaces:

- **Applet HTTP (port 80)**: Select the LAN and/or WAN checkboxes to enable access to the AP-5131 configuration applet using a Web browser.
- **Applet HTTPS (port 443)**: Select the LAN and/or WAN checkboxes to enable access to the AP-5131 configuration applet using a Secure Sockets Layer (SSL) for encrypted HTTP sessions.
- **CLI TELNET (port 23)**: Select the LAN and/or WAN checkboxes to enable access to the AP-5131 CLI via the TELNET terminal emulation TCP/IP protocol.
- **CLI SSH (port 22)**: Select the LAN and/or WAN checkboxes to enable access to the AP-5131 CLI using the SSH (Secure Shell) protocol.
- **SNMP (port 161)**: Select the LAN and/or WAN checkboxes to enable access to the AP-5131 configuration settings from an SNMP-capable client.

3. Refer to the **Applet Timeout** field to set an HTTPS timeout interval.

- **HTTP/S Timeout**: Disables access to the AP-5131 if no data activity is detected over Applet HTTPS (port 443) after the user defined interval. Default is 0 Mins.

4. Configure the **Secure Shell** field to set timeout values to reduce network inactivity.

- **Authentication Timeout**: Defines the maximum time (0–120 seconds) allowed for SSH authentication to occur before executing a timeout. The default is 120 seconds.
- **SSH Keepalive Interval**: The SSH Keepalive Interval defines a period (in minutes) after which if no data has been received from a client, SSH sends a message through the encrypted channel to request a response from the client. The default is 0, and no messages will be sent to the client until a non-zero value is set. Defining a Keepalive interval is important, otherwise programs running on a server may never notice if the other end of a connection is rebooted.

5. Use the **Admin Authentication** buttons to specify the authentication server connection method.

- **Local**: The AP-5131 verifies the authentication connection.
6. Use the Radius Server if a Radius server has been selected as the authentication server, enter the required network address information.

Radius Server IP Specify the numerical (non DNS name) IP address of the Remote Authentication Dial-In User Service (Radius) server. Radius is a client/server protocol and software enabling remote-access servers to communicate with a server used to authenticate users and authorize access to the requested system or service.

Port Specify the port on which the server is listening. The Radius server typically listens on ports 1812 (default port).

Shared Secret Define a shared secret for authentication on the server. The shared secret is required to be the same as the shared secret defined on the Radius server. Use shared secrets to verify Radius messages (with the exception of the Access-Request message) sent by a Radius-enabled device configured with the same shared secret. Apply the qualifications of a well-chosen password to the generation of a shared secret. Generate a random, case-sensitive string using letters, numbers and symbols. The default is symbol.

7. Update the Administrator Access field to change the administrative password used to access the AP-5131 configuration settings.

Change Admin Password Click the Change Admin Password button to display a screen for updating the AP administrator password. Enter and confirm a new administrator password as required.

8. Click Apply to save any changes to the AP-5131 Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

9. Click Undo Changes (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the AP-5131 Access screen to the last saved configuration.

10. Click Logout to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.
4.3 Managing Certificate Authority (CA) Certificates

Certificate management includes the following sections:

- Importing a CA Certificate
- Creating Self Certificates

4.3.1 Importing a CA Certificate

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates that it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so that it can trust certificates “signed” by the CA’s private key.

Depending on the public key infrastructure, the digital certificate includes the owner’s public key, the certificate expiration date, the owner’s name and other public key owner information.

The AP-5131 can import and maintain a set of CA certificates to use as an authentication option for Virtual Private Network (VPN) access. To use the certificate for a VPN tunnel, define a tunnel and select the IKE settings to use either RSA or DES certificates. For additional information on configuring VPN tunnels, see Configuring VPN Tunnels on page 6-33.

Refer to your AP-5131 network administrator to obtain a CA certificate to import into the AP-5131.

---

**NOTE**

Verify the AP-5131 device time is synchronized with an NTP server before importing a certificate to avoid issues with conflicting date/time stamps. For more information, see Configuring Network Time Protocol (NTP) on page 4-26.

---

To import a CA certificate:

1. Select System Configuration -> Certificate Mgmt -> CA Certificates from the AP-5131 menu tree.
2. Copy the content of the CA Certificate message (using a text editor such as notepad) and then click on Paste from Clipboard.

The content of the certificate displays in the Import a root CA Certificate field.

3. Click the Import root CA Certificate button to import it into the CA Certificate list.

4. Once in the list, select the certificate ID within the View Imported root CA Certificates field to view the certificate issuer name, subject, and certificate expiration data.

5. To delete a certificate, select the Id from the drop-down menu and click the Del button.

**4.3.2 Creating Self Certificates**

The AP-5131 requires two kinds of certificates for accessing the VPN, CA certificates and self certificates. Self certificates are certificate requests you create, send to a Certificate Authority (CA) to be signed, then import the signed certificate into the management system.

To create a self certificate:

1. Select System Configuration -> Certificate Mgmt -> Self Certificates from the AP-5131 menu tree.
2. Click on the **Add** button to create the certificate request. The **Certificate Request** screen displays.

3. Complete the request form with the pertinent information. Only 4 values are required, the others optional:

   - **Key ID**: Enter a logical name for the certificate to help distinguish between certificates. The name can be up to 7 characters in length.
   - **Subject**: The required **Subject** value contains important information about the certificate. Contact the CA signing the certificate to determine the content of the Subject parameter.
   - **Signature Algorithm**: Use the drop-down menu to select the signature algorithm used for the certificate. Options include:
     - **MD5-RSA** - Message Digest 5 algorithm in combination with RSA encryption.
     - **SHA1-RSA** - Secure Hash Algorithm 1 in combination with RSA encryption.
Complete as many of the optional values within the **Certificate Request** screen as possible.

4. When the form is completed, click the **Generate** button.
   - The Certificate Request screen disappears and the ID of the generated certificate request displays in the drop-down list of certificates.

5. Click the **Export Request** button.
   - The generated certificate request displays in Self Certificates screen text box.

6. Click the **Copy to Clipboard** button.
   - The content of certificate request is copied to the clipboard.
   - Create an email to your CA, paste the content of the request into the body of the message and send it to the CA.
   - The CA signs the certificate and will send it back. Once received, copy the content from the email into the clipboard.

7. Click the **Paste from clipboard** button.
   - The content of the email displays in the window.

8. Click the **Import Certificate** button to import the certificate and make it available for use as a VPN authentication option.

   - The certificate ID displays in the Signed list.

9. To use the certificate for a VPN tunnel, first define a tunnel and select the IKE settings to use either RSA or DES certificates. For additional information on configuring VPN tunnels, see *Configuring VPN Tunnels on page 6-33*.

**NOTE**

If the AP-5131 is restarted after a certificate request has been generated but before the signed certificate is imported, the import will not execute properly. Do not restart the AP-5131 during this process.

---

### 4.4 Configuring SNMP Settings

*Simple Network Management Protocol (SNMP)* facilitates the exchange of management information between network devices. SNMP uses *Management Information Bases (MIBs)* to manage the device.
configuration and monitor Internet devices in potentially remote locations. MIB information accessed via SNMP is defined by a set of managed objects called *object identifiers (OIDs)*. An object identifier (OID) is used to uniquely identify each object variable of a MIB. The AP-5131 CDROM contains the following 2 MIB files:

- Symbol-CC-WS2000-MIB-2.0 (common Symbol MIB file)
- Symbol-AP-5131-MIB (AP-5131 specific MIB file)

**NOTE** The Symbol-AP-5131-MIB contains the majority of the information contained within the Symbol-CC-WS2000-MIB-2.0 file. This feature rich information has been validated with the Symbol WS2000 and proven reliable. The remaining portion of the Symbol-AP-5131-MIB contains supplemental information unique to the AP-5131 feature set.

If using the Symbol-CC-WS2000-MIB-2.0 and/or Symbol-AP-5131-MIB to configure the AP-5131, use the table below to locate the MIB where the feature can be configured.

<table>
<thead>
<tr>
<th>Feature</th>
<th>MIB</th>
<th>Feature</th>
<th>MIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x Port Authentication</td>
<td>Symbol-AP-5131-MIB</td>
<td>Advanced DHCP Server configuration</td>
<td>Symbol-CC-WS2000-MIB-2.0</td>
</tr>
<tr>
<td>Ethernet Type Filter</td>
<td>Symbol-AP-5131-MIB</td>
<td>WAN IP Configuration</td>
<td>Symbol-CC-WS2000-MIB-2.0</td>
</tr>
<tr>
<td>MU ACL Configuration</td>
<td>Symbol-AP-5131-MIB</td>
<td>VPN Tunnel</td>
<td>Symbol-CC-WS2000-MIB-2.0</td>
</tr>
<tr>
<td>QOS Configuration</td>
<td>Symbol-AP-5131-MIB</td>
<td>VPN Tunnel status</td>
<td>Symbol-CC-WS2000-MIB-2.0</td>
</tr>
<tr>
<td>Radio Configuration</td>
<td>Symbol-AP-5131-MIB</td>
<td>Content Filtering</td>
<td>Symbol-CC-WS2000-MIB-2.0</td>
</tr>
<tr>
<td>SNMP Trap Selection</td>
<td>Symbol-AP-5131-MIB</td>
<td>Firewall Configuration</td>
<td>Symbol-CC-WS2000-MIB-2.0</td>
</tr>
</tbody>
</table>
SNMP allows a network administrator to manage network performance, find and solve network problems, and plan for network growth. The AP-5131 supports SNMP management functions for gathering information from its network components, communicating that information to specified users and configuring the AP-5131. All the fields available within the AP-5131 are also configurable within the MIB.

The AP-5131 SNMP agent functions as a command responder and is a multilingual agent responding to SNMPv1, v2c and v3 managers (command generators). The factory default configuration maintains SNMPv1/2c support of the community names, hence providing backward compatibility.

SNMP v1/v2c community definitions and SNMP v3 user definitions work independently, and both use the Access Control List (ACL) of the SNMP Access Control sub-screen.
Use the **SNMP Access** screen to define SNMP v1/v2c community definitions and SNMP v3 user definitions. SNMP version 1 (v1) provides a strong network management system, but its security is relatively weak. The improvements in SNMP version 2c (v2c) do not include the attempted security enhancements of other version-2 protocols. Instead, SNMP v2c defaults to SNMP-standard community strings for read-only and read/write access. SNMP version 3 (v3) further enhances protocol features, providing much improved security. SNMP v3 encrypts transmissions and provides authentication for users generating requests.

To configure SNMP v1/v2c community definitions and SNMP v3 user definitions for the AP-5131:

1. Select **System Configuration - > SNMP Access** from the AP-5131 menu tree.

SNMP v1/v2c community definitions allow read-only or read/write access to AP-5131 management information. The SNMP community includes users whose IP addresses are specified on the **SNMP Access Control** screen.

A read-only community string allows a remote device to retrieve information, while a read/write community string allows a remote device to modify settings. Symbol recommends considering adding a community definition using a site-appropriate name and access level. Set up a read/write definition (at a minimum) to facilitate full access by the AP-5131 administrator.
2. Configure the **SNMP v1/v2 Configuration** field (if SNMP v1/v2 is used) to add or delete community definitions, name the community, specify the OID and define community access.

   **Add**
   
   Click **Add** to create a new SNMP v1/v2c community definition.

   **Delete**
   
   Select **Delete** to remove a SNMP v1/v2c community definition.

   **Community**
   
   Use the **Community** field to specify a site-appropriate name for the community. The name is required to match the name used within the remote network management software.

   **OID**
   
   Use the **OID** (Object Identifier) pull-down list to specify a setting of All or a enter a Custom OID. Select **All** to assign the user access to all OIDs in the MIB. The OID field uses numbers expressed in dot notation.

   **Access**
   
   Use the **Access** pull-down list to specify **read-only (R)** access or **read/write (RW)** access for the community. Read-only access allows a remote device to retrieve AP-5131 information, while read/write access allows a remote device to modify AP-5131 settings.

3. Configure the **SNMP v3 User Definitions** field (if SNMP v3 is used) to add and configure SNMP v3 user definitions.

   SNMP v3 user definitions allow read-only or read/write access to management information as appropriate.

   **Add**
   
   Click **Add** to create a new entry for an SNMP v3 user.

   **Delete**
   
   Select **Delete** to remove an entry for an SNMP v3 user.

   **Username**
   
   Specify a username by typing an alphanumeric string of up to 31 characters.

   **Security Level**
   
   Use the **Security Level** area to specify a security level of **noAuth** (no authorization), **AuthNoPriv** (authorization without privacy), or **AuthPriv** (authorization with privacy).

   The **noAuth** setting specifies no login authorization or encryption for the user.

   The **AuthNoPriv** setting requires login authorization, but no encryption.

   The **AuthPriv** setting requires login authorization and uses the **Data Encryption Standard (DES)** protocol.
4. Specify the users who can read and optionally modify the SNMP-capable client.

 OID

 Use the OID (Object Identifier) area to specify a setting of All or enter a Custom OID. Select All to assign the user access to all OIDs in the MIB. The OID field uses numbers expressed in dot notation.

 Passwords

 Select Passwords to display the Password Settings screen for specifying authentication and password settings for an SNMP v3 user. The maximum password length is 11 characters. Use the Authentication Algorithm drop-down menu to specify MD5 or SHA1 as the authentication algorithm. Use the Privacy Algorithm drop-down menu to define an algorithm of DES or AES-128bit. When entering the same username on the SNMP Traps and SNMP Access screens, the password entered on the SNMP Traps page overwrites the password entered on the SNMP Access page. To avoid this problem, enter the same password on both pages.

 Access

 Use the Access pull-down list to specify read-only (R) access or read/write (RW) access for a user. Read-only access permits a user to retrieve AP-5131 information, while read/write access allows a user to modify AP-5131 settings.

 SNMP Access Control

 Click the SNMP Access Control button to display the SNMP Access Control screen for specifying which users can read SNMP-generated information and potentially modify related settings from an SNMP-capable client.

 The SNMP Access Control screen’s Access Control List (ACL) uses Internet Protocol (IP) addresses to restrict access to the AP’s SNMP interface. The ACL applies to both SNMP v3 user definitions and SNMP v1/v2c community definitions.

 For detailed instructions of configuring SNMP user access and modification privileges, see Configuring SNMP Access Control on page 4-17.

 5. If configuring SNMP v3 user definitions, set the SNMP v3 engine ID.

 AP-5131 SNMP v3 Engine ID

 The AP-5131 SNMP v3 Engine ID field lists the unique SNMP v3 Engine ID for the AP-5131. This ID is used in SNMP v3 as the source for a trap, response or report. It is also used as the destination ID when sending get, getnext, getbulk, set or inform commands.
6. Click **Apply** to save any changes to the SNMP Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

7. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the SNMP Access screen to the last saved configuration.

8. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

For additional SNMP configuration information, see:

- Configuring SNMP Access Control
- Enabling SNMP Traps
- Configuring Specific SNMP Traps
- Configuring SNMP RF Trap Thresholds

**4.4.1 Configuring SNMP Access Control**

Use the **SNMP Access Control** screen (as launched from the SNMP Access screen) to specify which users can read SNMP generated information and, if capable, modify related settings from an SNMP-capable client.

Use the SNMP Access Control screen’s **Access Control List (ACL)** to limit, by Internet Protocol (IP) address, who can access the AP-5131 SNMP interface.

**NOTE**  The ACL applies to both SNMP v3 user definitions and SNMP v1/v2c community definitions on the AP-5131 SNMP Access screen.

To configure SNMP user access control for the AP-5131:

1. Select **System Configuration -> SNMP Access** from the AP-5131 menu tree. Click on the **SNMP Access Control** button from within the SNMP Access screen.
2. Configure the SNMP Access Control screen to add the IP addresses of those users receiving SNMP access.

**Access Control List**

Enter Start IP and End IP addresses (numerical addresses only, no DNS names supported) to specify a range of user that can access the AP-5131 SNMP interface. An SNMP-capable client can be set up whereby only the administrator (for example) can use a read/write community definition.

Use just the Starting IP Address column to specify a single SNMP user. Use both the Starting IP Address and Ending IP Address columns to specify a range of addresses for SNMP users.

To add a single IP address to the ACL, enter the same IP address in the Start IP and End IP fields.

Leave the ACL blank to allow access to the SNMP interface from the IP addresses of all authorized users.

**Add**

Click **Add** to create a new ACL entry.

**Edit**

Click **Edit** to revise an existing ACL entry.

**Delete**

Click **Delete** to remove a selected ACL entry for one or more SNMP users.
4.4.2 Enabling SNMP Traps

SNMP provides the ability to send traps to notify the administrator that trap conditions are met. Traps are network packets containing data relating to network devices, or SNMP agents, that send the traps. SNMP management applications can receive and interpret these packets, and optionally can perform responsive actions. SNMP trap generation is programmable on a trap-by-trap basis.

Use the **SNMP Traps Configuration** screen to enable traps and to configure appropriate settings for reporting this information. Trap configuration depends on the network machine that receives the generated traps. SNMP v1/v2c and v3 trap configurations function independently. In a mixed SNMP environment, generated traps can be sent using configurations for both SNMP v1/v2c and v3.

To configure SNMP traps on the AP-5131:

1. Select **System Configuration - > SNMP Access - > SNMP Trap Configuration** from the AP-5131 menu tree.
2. Configure the **SNMP v1/v2c Trap Configuration** field (if SNMP v1/v2c Traps are used) to modify the following:

- **Add**
  - Click **Add** to create a new SNMP v1/v2c Trap Configuration entry.

- **Delete**
  - Click **Delete** to remove a selected SNMP v1/v2c Trap Configuration entry.

- **Destination IP**
  - Specify a numerical (non DNS name) destination IP address for receiving the traps sent by the AP-5131 SNMP agent.

- **Port**
  - Specify a destination User Datagram Protocol (UDP) port for receiving traps. The default is 162.

- **Community**
  - Enter a community name specific to the SNMP-capable client that receives the traps.

- **SNMP Version**
  - Use the SNMP Version drop-down menu to specify v1 or v2.
  - Some SNMP clients support only SNMP v1 traps, while others support SNMP v2 traps and possibly both, verify the correct traps are in use with clients that support them.

3. Configure the **SNMP v3 Trap Configuration** field (if SNMP v3 Traps are used) to modify the following:
Add Click Add to create a new SNMP v3 Trap Configuration entry.

Delete Select Delete to remove an entry for an SNMP v3 user.

Destination IP Specify a numerical (non DNS name) destination IP address for receiving the traps sent by the AP-5131 SNMP agent.

Port Specify a destination User Datagram Protocol (UDP) port for receiving traps.

Username Enter a username specific to the SNMP-capable client receiving the traps.

Security Level Use the Security Level drop-down menu to specify a security level of noAuth (no authorization), AuthNoPriv (authorization without privacy), or AuthPriv (authorization with privacy).

Passwords Select Passwords to display the Password Settings screen for specifying authentication and password settings for an SNMP v3 user. The maximum password length is 11 characters. Use the Authentication Algorithm drop-down menu to specify MD5 or SHA1 as the authentication algorithm. Use the Privacy Algorithm drop-down menu to define an algorithm of DES or AES-128bit.

If entering the same username on the SNMP Traps and SNMP Access screens, the password entered on the SNMP Traps page overwrites the password entered on the SNMP Access page. To avoid this problem, enter the same password on both pages.

4. Click Apply to save any changes to the SNMP Trap Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

5. Click Undo Changes (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP Trap Configuration screen to the last saved configuration.

6. Click Logout to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.
4.4.3 Configuring Specific SNMP Traps

Use the SNMP Traps screen to enable specific traps on the AP-5131. Symbol recommends defining traps to capture unauthorized devices operating within the AP-5131 coverage area. Trap configuration depends on the network machine that receives the generated traps. SNMP v1/v2c and v3 trap configurations function independently. In a mixed SNMP environment, traps can be sent using configurations for both SNMP v1/v2c and v3.

To configure specific SNMP traps on the AP-5131:


2. Configure the MU Traps field to generate traps for MU associations, MU association denials and MU authentication denials. When a trap is enabled, a trap is sent every 5 seconds until the condition no longer exists.

- **MU associated**: Generates a trap when an MU becomes associated with one of the AP-5131’s WLANs.
- **MU unassociated**: Generates a trap when an MU becomes unassociated with (or gets dropped from) one of the AP-5131’s WLANs.
3. Configure the **SNMP Traps** field to generate traps when SNMP capable MUs are denied authentication privileges or are subject of an ACL violation. When a trap is enabled, a trap is sent every 5 seconds until the condition no longer exists.

   **MU associated**
   Generates a trap when an MU becomes associated with one of the AP-5131’s WLANs.

   **MU denied association**
   Generates a trap when an MU is denied association to a AP-5131 WLAN. Can be caused when the maximum number of MUs for a WLAN is exceeded or when an MU violates the AP-5131’s Access Control List (ACL).

   **MU denied authentication**
   Generates a trap when an MU is denied authentication on one of the AP’s WLANs. Can be caused by the MU being set for the wrong authentication type for the WLAN or by an incorrect key or password.

4. Configure the **Network Traps** field to generate traps when the AP-5131’s link status changes or when the AP’s firewall detects a DOS attack.

   **Physical port status change**
   Generates a trap whenever the status changes on the AP-5131. The physical port status changes when a link is lost between the AP-5131 and a connected device.

   **Denial of service (DOS) attempts**
   Generates a trap whenever a Denial of Service (DOS) attack is detected by the AP-5131 firewall. A new trap is sent at the specified interval until the attack has stopped.

   **Send trap every**
   Defines the interval in seconds the AP-5131 uses to generate a trap until the Denial of Service attack is stopped. Default is 10 seconds.
5. Configure the **System Traps** field to generate traps when the AP-5131 re-initializes during transmission, saves its configuration file. When a trap is enabled, a trap is sent every 5 seconds until the condition no longer exists.

- **System Cold Start**
  Generates a trap when the AP-5131 re-initializes while transmitting, possibly altering the SNMP agent’s configuration or protocol entity implementation.

- **Configuration Changes**
  Generates a trap whenever changes to the AP-5131’s configuration file are saved.

- **Rogue AP detection**
  Generates a trap if a Rogue AP is detected by the AP-5131.

- **AP Radar detection**
  Generates a trap if an AP is detected using a form of radar detection.

6. Click **Apply** to save any changes to the SNMP Traps screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

7. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP Traps screen to the last saved configuration.

8. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 4.4.4 Configuring SNMP RF Trap Thresholds

Use the **SNMP RF Trap Threshold** screen as a means to track RF activity and the AP-5131’s radio and associated MU performance. SNMP RF Traps are sent when RF traffic exceeds defined limits set in the **RF Trap Thresholds** field of the SNMP RF Traps screen. Thresholds are displayed for the AP-5131, WLAN, selected radio and the associated MU.

To configure specific SNMP RF Traps on the AP-5131:

1. Select **System Configuration - > SNMP Access - > SNMP RF Trap Thresholds** from the AP-5131 menu tree.
2. Configure the **RF Trap Thresholds** field to define device threshold values for SNMP traps.

**NOTE** Average Bit Speed, % of Non-Unicast, Average Signal, Average Retries, % Dropped and % Undecryptable are not AP-5131 statistics.

- **Pkts/s**
  - Enter a maximum threshold for the total throughput in Pps (Packets per second).

- **Throughput**
  - Set a maximum threshold for the total throughput in Mbps (Megabits per second).

- **Average Bit Speed**
  - Enter a minimum threshold for the average bit speed in Mbps (Megabits per second).

- **% Non-Unicast**
  - Set a maximum threshold for the total percentage of packets that are non-unicast for each device. Non-unicast packets include broadcast and multi-cast traffic.

- **Average Signal**
  - Enter a minimum threshold for the average signal strength in dBm for each device.
3. Configure the **Minimum Packets** field to define a minimum packet throughput value for trap generation.

4. Click **Apply** to save any changes to the SNMP RF Traps screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP RF Traps screen to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 4.5 Configuring Network Time Protocol (NTP)

*Network Time Protocol (NTP)* manages time and/or network clock synchronization in the AP-5131-managed network environment. NTP is a client/server implementation. The AP-5131 (an NTP client) periodically synchronizes its clock with a master clock (an NTP server). For example, the AP-5131 resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Time synchronization is recommended for the AP’s network operations. For sites using Kerberos authentication, time synchronization is required.

Use the **NTP Servers** screen to enable NTP and specify the IP addresses and ports of available NTP servers.
To manage clock synchronization on the AP-5131:

1. Select **System Configuration -> NTP Servers** from the AP-5131 menu tree.

2. Ensure the **Current Time** field reflects the appropriate time for the AP-5131.

   - **Time**
     
     Displays the current time based on the AP-5131 system clock. If NTP is disabled or if there are no servers available, the system time displays the AP-5131 uptime starting at 1970-01-01 00:00:00, with the time and date advancing. The displayed time auto updates every 5 seconds.

   - **Refresh**
     
     Click the **Refresh** button to update the displayed date and time.

3. Configure the **Server Configuration** field to define server network address information required to acquire the AP-5131 network time.

---

**NOTE**

The current time is not set accurately when initially connecting to the AP-5131. Until a server is defined to provide the AP-5131 the correct time, the AP-5131 displays 1970-01-01 00:00:00 as the default time.
4. Click **Apply** to save any changes to the NTP Servers screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on NTP Servers screen to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 4.6 Logging Configuration

The AP-5131 provides the capability for periodically logging system events that prove useful in assessing the throughput and performance of the AP-5131 or troubleshooting problems on the AP-5131 managed *Local Area Network (LAN)*. Use the **Logging Configuration** screen to set the desired logging level (standard syslog levels) and view or save the current AP-5131 system log.

To configure event logging for the AP-5131:

1. Select **System Configuration - > Logging Configuration** from the AP-5131 menu tree.
2. Configure the Log Options field to save event logs, set the log level and optionally port the AP-5131’s log to an external server.

View Log

Click View to save a log of events retained on the AP-5131. The system displays a prompt requesting the administrator password before saving the log. After the password has been entered, click Get File to display a dialogue with buttons to Open or Save the log.txt file. Click Save and specify a location to save the log file. Use the WordPad application to view the saved log.txt file on a Microsoft Windows based computer. Do not view the log file using Notepad, as the Notepad application does not properly display the formatting of the AP-5131 log file. Log entries are not saved in the AP-5131. While the AP is in operation, log data temporarily resides in memory. AP memory is completely cleared each time the AP reboots.
3. Click **Apply** to save any changes to the Logging Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

4. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Logging Configuration screen to the last saved configuration.

5. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 4.7 Importing/Exporting Configurations

All of the configuration settings for an AP-5131 can be obtained from another AP-5131 in the form of a text file. Additionally, all of the AP-5131’s settings can be downloaded to another AP-5131. Use the file-based configuration feature to speed up the setup process significantly at sites using multiple AP-5131’s. Another benefit is the opportunity to save the current AP configuration before making significant changes or restoring the default configuration. All options on the AP-5131 are deleted and

---

**Logging Level**

Use the **Logging Level** drop-down menu to select the desired log level for tracking system events. Eight logging levels, (0 to 7) are available. **Log Level 6: Info** is the AP-5131 default log level. These are the standard UNIX/LINUX syslog levels. The levels are as follows:

- 0 - Emergency
- 1 - Alert
- 2 - Critical
- 3 - Errors
- 4 - Warning
- 5 - Notice
- 6 - Info
- 7 - Debug

**Enable logging to an external syslog server**

The AP-5131 can log events to an external syslog (system log) server. Select the **Enable logging to an external syslog server** checkbox to enable the server to listen for incoming syslog messages and decode the messages into a log for viewing.

**Syslog server IP address**

If the **Enable logging to an external syslog server** checkbox is selected, the numerical (non DNS name) IP address of an external syslog server is required in order to route the syslog events to that destination.
updated by the imported file. Therefore, the imported configuration is not a merge with the configuration of the target AP-5131. The exported file can be edited with any document editor if necessary.

**CAUTION**  A single-radio model AP-5131 cannot import/export its configuration to a dual-radio model AP-5131. In turn, a dual-radio model AP-5131 cannot import/export its configuration to a single-radio AP-5131.

Use the **Config Import/Export** screen to configure an import or export operation for AP-5131 configuration settings.

**NOTE**  Use the **System Settings** screen as necessary to restore an AP-5131 default configuration. For more information on restoring configurations, see Configuring System Settings on page 4-2.

To create an importable/exportable AP-5131 configuration file:

1. Select **System Configuration - > Config Import/Export** from the AP-5131 menu tree.

2. Configure the **FTP and TFTP Import/Export** field to import/export configuration settings.
3. Configure the **HTTP Import/Export** field to import/export AP-5131 configuration settings using HTTP.

**CAUTION** For HTTP downloads (exports) to be successful, pop-up messages must be disabled.
4. Refer to the **Status** field to assess the completion of the import/export operation.

**Status**

After executing an operation (by clicking any of the buttons in the window), check the Status field for a progress indicator and messages about the success or errors in executing the Import/Export operation. Possible status messages include:

- ambiguous input before marker: line `<number>`
- unknown input before marker: line `<number>`
- ignored input after marker: line `<number>`
- additional input required after marker: line `<number>`
- invalid input length: line `<number>`
- error reading input: line `<number>`
- import file from incompatible hardware type: line `<number>`

- [0] Import operation done
- [1] Export operation done
- [2] Import operation failed
- [3] Export operation failed
- [4] File transfer in progress
- [5] File transfer failed
- [6] File transfer done
- Auto cfg update: Error in applying config
- Auto cfg update: Error in getting config file
- Auto cfg update: Aborting due to fw update failure

The `<number>` value appearing at the end of some messages relates to the line of the configuration file where an error or ambiguous input was detected.
5. Click **Apply** to save the filename and Server IP information. The Apply button does not execute the import or export operation, only saves the settings entered.

6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on Config Import/Export screen to the last saved configuration.

7. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 4.8 Updating Device Firmware

Symbol periodically releases updated versions of the AP-5131 device firmware to the Symbol Web site. If the AP-5131 firmware version displayed on the **System Settings** page (see **Configuring System Settings on page 4-2**) is older than the version on the Web site, Symbol recommends updating the AP-5131 to the latest firmware version for full feature functionality.

If a firmware update is required, use the **Firmware Update** screen to specify a filename and define a file location for updating the firmware.

**NOTE**  The firmware file must be available from an FTP or TFTP site to perform the update.

**CAUTION**  Make sure a copy of the AP-5131’s configuration is saved before updating the firmware.

To conduct a firmware update on the AP-5131:

1. Export the AP-5131 current configuration settings before updating the firmware to have the most recent settings available after the firmware is updated.
Refer to Importing/Exporting Configurations on page 4-30 for instructions on exporting the AP-5131’s current configuration to have it available after the firmware is updated.

2. Select **System Configuration** - > **Firmware Update** from the AP-5131 menu tree.

3. Configure the **DHCP Options** field to enable automatic firmware and/or configuration file updates when the selected LAN or WAN interface detects an updated file.

   DHCP options are used for out-of-the-box rapid deployment for Symbol wireless products. The following are the two DHCP options available on the AP-5131:
   - Enable Automatic Firmware Update
   - Enable Automatic Configuration Update

   These options can be used to update newer firmware and configuration files on the AP-5131 through either the LAN or WAN interface. The AP-5131 uses DHCP Vendor Specific Option 43 with the following options embedded within it:
The Vendor Class Identifier used is **SymbolAP.5131-V1-0**

The DHCP Server needs to be configured with the above mentioned vendor specific options and vendor class identifier. The interface selected (LAN or WAN) on the AP-5131, must be configured as a DHCP client for the Auto DHCP Update feature to function properly.

<table>
<thead>
<tr>
<th>Option Code</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>181</td>
<td>IP address</td>
</tr>
<tr>
<td>187</td>
<td>String</td>
</tr>
<tr>
<td>188</td>
<td>String</td>
</tr>
</tbody>
</table>

**Enable Automatic Firmware Update**
Select this checkbox to allow an automatic firmware update each time firmware versions are found to be different between the AP-5131 and the specified LAN or WAN interface. This option is used in conjunction with other DHCP options configured on a DHCP server.

Symbol recommends selecting the **Enable Automatic Configuration Update** checkbox if auto-updating AP-5131 firmware, as backing up the AP-5131 configuration is always recommended before updating device firmware. If this function is disabled, the firmware update is required to be done manually. If this option is enabled, the AP-5131 initiates an update anytime the AP-5131 reboots. If the files located on the DHCP server are different from the existing files on the AP-5131, the files are updated. The default setting is enabled on the AP-5131 WAN port.

**Enable Automatic Configuration Update**
Select this checkbox to allow an automatic configuration file update each time the configuration file versions are found to be different between the AP-5131 and the selected LAN or WAN interface. If this function is disabled, the configuration file update is required to be done manually. If this function is disabled, the firmware update is required to be done manually. If this option is enabled, the AP-5131 initiates an update anytime the AP-5131 reboots. If the files located on the DHCP server are different from the existing files on the AP-5131, the files are updated. The default setting is enabled on the AP-5131 WAN port.
Configure the Update Firmware field as required to set a filename and target firmware file upload location for manual firmware updates.

4. Specify the name of the target firmware file within the Filename field.
5. If the target firmware file resides within a directory, specify a complete path for the file within the Filepath(optional) field.
6. Enter an IP address for the FTP or TFTP server used for the update. Only numerical IP address names are supported, no DNS can be used.
7. Use the drop-down menu to specify the FTP or TFTP server’s location. The server can reside on the WAN or on the LAN.
8. Select either the FTP or TFTP button to define whether the firmware file resides on a FTP or TFTP server.
9. Set the following FTP or TFTP parameters:
   - Username - Specify a username for the FTP server login.
   - Password - Specify a password for FTP server login. Default is symbol.

**NOTE** Click Apply to save the settings before performing the firmware update. The user is not able to navigate the AP-5131 user interface while the firmware update is in process.

10. Click the Perform Update button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update.
11. After the AP reboots, return to the Firmware Update screen. Check the Status field to verify whether the firmware update was successful. If an error occurs, one of the following error messages will display:
    - FAIL: auto fw update check
    - FAIL: network activity time out
    - FAIL: firmware check
    - FAIL: exceed memory limit
    - FAIL: authentication
    - FAIL: connection time out
FAIL: control channel error
FAIL: data channel error
FAIL: channel closed unexpected
FAIL: establish data channel
FAIL: accept data channel
FAIL: user interrupted
FAIL: no valid interface found
FAIL: conflict ip address
FAIL: command exchange time out
FAIL: invalid subnet number

12. Confirm the AP-5131's configuration is the same as before the firmware update. If they are not, restore the settings. Refer to Importing/Exporting Configurations on page 4-30 for instructions on exporting the configuration back to the AP-5131.

13. Click Apply to save the filename and filepath information entered into the Firmware Update screen. The Apply button does not execute the firmware, only saves the update settings entered.

14. Click Undo Changes (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on Firmware Update screen to the last saved configuration.

15. Click Logout to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.
Configuring network management includes configuring network aspects in numerous areas. See the following sections for more information on AP-5131 network management:

- Configuring the LAN Interface
- Configuring WAN Settings
- Enabling Wireless LANs (WLANs)
- Configuring Router Settings

### 5.1 Configuring the LAN Interface

The AP-5131 has one LAN port and thus must manage all data traffic over the LAN connection carefully as either a DHCP client, BOOTP client, DHCP server or using neither DHCP or BOOTP. The AP-5131 LAN port has its own MAC address. The LAN port MAC address is always the value of the AP-5131 WAN port MAC address plus 1. The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens. For information on locating the AP-5131 MAC addresses, see Viewing WAN Statistics on page 7-2 and Viewing LAN Statistics on page 7-5.
The AP-5131 can use Dynamic Host Configuration Protocol (DHCP) to obtain a leased IP address and configuration information from a remote server. DHCP is based on the BOOTP protocol and can coexist or interoperate with BOOTP.

Use the LAN Configuration screen to define the LAN interface and assign a timeout value to disable the LAN connection if no data traffic is detected within a defined interval. The LAN Configuration screen is also used to define advanced DHCP server settings to generate a list of static MAC to IP mappings for reserved clients and optionally configure VLAN mappings to individual WLANs (up to 16 WLANs available per AP-5131). The LAN Configuration screen also contains a Type Filter submenu item used to prevent specific (an potentially unnecessary) frames from being processed by the AP-5131 in order to improve throughput.

To configure the AP-5131 LAN interface:

1. Select Network Configuration -> LAN Configuration from the AP-5131 menu tree.

2. Configure the LAN Setting field to enable the AP-5131 LAN interface, assign a timeout value, enable 802.1q trunking, configure VLAN mapping and enable 802.1x authentication.

Enable LAN Interface  Select the checkbox to forward data traffic over the AP-5131 LAN connection. The LAN connection is enabled by default.
3. Configure the **DHCP** field to define the type of LAN interface used.

**NOTE**  Symbol recommends that the WAN and LAN ports should not both be configured as DHCP clients.
This interface is a DHCP Client

Select this button to enable DHCP to set AP-5131 network address information via the LAN connection. This is recommended if the AP-5131 resides within a large corporate network or the Internet Service Provider (ISP) uses DHCP.

DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. If DHCP Client is selected, the first DHCP or BOOTP server to respond sets the IP address and network address values since DHCP and BOOTP are interoperable.

This interface is a BOOTP Client

Select this button to enable BOOTP to set AP-5131 network address information via the LAN connection.

When selected, only BOOTP responses are accepted by the AP-5131. If both DHCP and BOOTP services are required, do not select BOOTP Client.

This interface uses static IP Address

Select the This interface uses static IP Address button, and manually enter static network address information in the areas provided.

This interface is a DHCP Server

The AP-5131 can be configured to function as a DHCP server over the LAN connection. Select the This interface is a DHCP Server button and manually enter static network address information in the areas provided.

Address Assignment Range

Use the address assignment parameter to specify a range of numerical (non DNS name) IP addresses reserved for mapping client MAC addresses to IP addresses. If a manually (static) mapped IP address is within the IP address range specified, that IP address could still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

Advanced DHCP Server

Click the Advanced DHCP Server button to display a screen used for generating a list of static MAC to IP address mappings for reserved clients. For more information, see Configuring Advanced DHCP Server Settings on page 5-10.

IP Address

The network-assigned numerical (non DNS name) IP address of the AP-5131.
4. Click **Apply** to save any changes to the LAN Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LAN configuration screen to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.1.1 Configuring VLAN Support

A **Virtual Local Area Network (VLAN)** is a means to electronically separate data on the same AP-5131 from a single broadcast domain into separate broadcast domains. The AP-5131 can group devices on one or more WLANs so that they can communicate as if they were attached to the same wire, when in fact they are located on a different LAN segment. Because VLANs are based on logical instead of physical connections, they are extremely flexible. By using a VLAN, you can group by logical function instead of physical location. A maximum of 16 VLANs can be supported on the AP-5131 (regardless of the AP-5131 being single or dual-radio model). An administrator can map 16 WLANs to 16 VLANs and enable or disable dynamic VLAN assignment.

**Network Mask**

The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission. The subnet mask defines the size of the subnet.

**Default Gateway**

The **Default Gateway** parameter defines the numerical (non DNS name) IP address of a router the AP-5131 uses on the Ethernet as its default gateway.

**Domain Name**

Enter the name assigned to the primary DNS server.

**Primary DNS Server**

Enter the Primary DNS numerical (non DNS name) IP address.

**Secondary DNS Server**

Symbol recommends entering the numerical IP address of an additional DNS server (if available), used if the primary DNS server goes down. A maximum of two DNS servers can be used.

**WINS Server**

Enter the numerical (non DNS name) IP address of the WINS server. WINS is a Microsoft NetBIOS name server. Using a WINS server eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.
VLANs enable organizations to share network resources in various network segments within large areas (airports, shopping malls, etc.). A VLAN is a group of clients with a common set of requirements independent of their physical location. VLANs have the same attributes as physical LANs, but they enable system administrators to group MUs even when they are not members of the same network segment.

The AP-5131 assignment of VLANs can be implemented using Static or Dynamic assignments (often referred to as memberships) for individual WLANs. Both methods have their advantages and disadvantages. Static VLAN membership is perhaps the most widely used method because of the relatively small administration overhead and security it provides. With Static VLANs, you manually assign individual WLANs to individual VLANs.

Although static VLANs are the most common form of VLAN assignments, dynamic VLAN assignment is possible per WLAN. Configuring dynamic VLANs entail the AP-5131 sending a DHCP request for device information (such as an IP address). Additional information (such as device MAC address information) is sent to the AP-5131. The AP-5131 sends this MAC address to a host housing a copy of the Dynamic VLAN database. This database houses the records of MAC addresses and VLAN assignments. The VLAN database looks up the MAC to determine what VLAN is assigned to it. If it is not in the database, it simply uses a default VLAN assignment. The VLAN assignment is sent to the AP-5131. The AP-5131 then maps the target WLAN for the assigned VLAN and traffic passes normally, allowing for the completion of the DHCP request and further traffic.

To create new VLANs or edit the properties of an existing VLAN:

1. Select Network Configuration -> LAN from the AP-5131 menu tree.
2. Ensure the Enable 802.1q Trunking button is selected from within the LAN Setting field. Trunk links are required to pass VLAN information between destinations. A trunk port is by default a member of all the VLANs existing on the AP-5131 and carry traffic for all those VLANs. Trunking is a function that must be enabled on both sides of a link.
3. Select the VLAN Name button.
The VLAN name screen displays. The first time the screen is launched a default VLAN name of 1 and a default VLAN ID of 1 display. The VLAN name is auto-generated once the user assigns a VLAN ID. However, the user has the option of re-assigning a name to the VLAN using New VLAN and Edit VLAN screens.

To create a new VLAN, click the Create button, to edit the properties of an existing VLAN, click the Edit button.

4. Assign a unique VLAN ID (from 1 to 4095) to each VLAN added or modified.
The VLAN ID associates a frame with a specific VLAN and provides the information the AP-5131 needs to process the frame across the network. Therefore, it may be practical to assign a name to a VLAN representative or the area or type of network traffic it represents. A business may have offices in different locations and want to extend an internal LAN between the locations. An AP-5131 managed infrastructure could provide this connectivity, but it requires VLAN numbering be managed carefully to avoid conflicts between two VLANs with the same ID.

5. Define a 32 ASCII character maximum VLAN Name.
   Enter a unique name that identifies members of the VLAN. Symbol recommends selecting the name carefully, as the VLAN name should signify a group of clients with a common set of requirements independent of their physical location.

6. Click Apply to save the changes to the new or modified VLAN and return to the VLAN Name screen.

7. Click the VLAN Config button.

The VLAN Configuration screen displays.

8. Enter a Management VLAN Tag.
The Management VLAN uses a default tag value of 1. The Management VLAN is used to distinguish VLAN traffic flows. The trunk port marks the frames with special tags as they pass between the AP-5131 and its destination, these tags help distinguish data traffic.

Authentication servers (such as Radius and Kerberos) must be on the same Management VLAN. Additionally, DHCP and BOOTP servers must be on the same Management VLAN as well.

9. Define a Native VLAN Tag.

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the AP-5131 forwards untagged traffic with the native VLAN configured for the port. The Native VLAN is VLAN 1 by default. Symbol suggests leaving the Native VLAN set to 1 as other layer 2 devices also have their Native VLAN set to 1.

10. Use the checkboxes under the name of each VLAN to map specific VLANs to AP-5131 WLANs listed on the left-hand side of the screen.

Symbol recommends mapping VLANs strategically in order to keep VLANs tied to the discipline they most closely match. For example, if WLAN2 is comprised of MUs supporting the engineering area, then WLAN2 should be mapped to the engineering VLAN if one has been created.

11. Select the Dynamic checkbox to configure the VLAN mapping as a dynamic VLAN.

Using Dynamic VLAN assignments, a VMPS (VLAN Management Policy Server) dynamically assigns VLAN ports. The AP-5131 uses a separate server as a VMPS server. When a frame arrives on the AP-5131, it queries the VMPS for the VLAN assignment based on the source MAC address of the arriving frame.

If statically mapping VLANs, leave the Dynamic checkbox specific to the target WLAN and its intended VLAN unselected. The administrator is then required to configure VLAN memberships manually.

The Dynamic checkbox is enabled only when a WLAN is having EAP security configured. Otherwise, the checkbox is disabled.

12. Click Apply to return to the VLAN Name screen. Click OK to return to the LAN screen. Once at the LAN screen, click Apply to re-apply your changes.
5.1.2 Configuring Advanced DHCP Server Settings

Use the Advanced DHCP Server screen to specify (reserve) static (or fixed) IP addresses for specific devices. Every wireless, 802.11x-standard device has a unique Media Access Control (MAC) address. This address is the device’s hard-coded hardware number (shown on the bottom or back). An example of a MAC address is 00:A0:F8:45:9B:07.

The DHCP server can grant an IP address for as long as it remains in active use. The lease time is the number of seconds that an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than available IP addresses. This is useful, for example, in education and customer environments where MU users change frequently. Use longer leases if there are fewer users.

To generate a list of client MAC address to IP address mappings for the AP-5131:

1. Select Network Configuration -> LAN Configuration from the AP-5131 menu tree.
2. Click the Advanced DHCP Server button from within the LAN Configuration screen.
3. Specify a lease period in seconds for available IP addresses using the DHCP Lease Time (Seconds) parameter. An IP address is reserved for re-connection for the length of time you specify. The default interval is 86400 seconds.
4. Click the Add button to create a new table entry within the Reserved Clients field.
If a statically mapped IP address is within the IP address range in use by the DHCP server, that IP address may still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

If multiple entries exist within the Reserved Clients field, use the scroll bar to the right of the window to navigate.

5. Click the Del (delete) button to remove a selected table entry.
6. Click OK to return to the LAN Configuration page, where the updated settings within the Advanced DHCP Server screen can be saved by clicking the Apply button.
7. Click Cancel to undo any changes made. Undo Changes reverts the settings displayed to the last saved configuration.

5.1.3 Setting the Type Filter Configuration

The AP-5131 can keep a list of frame types that it forwards or discards. The Type Filtering feature prevents specific (a potentially unnecessary) frames from being processed by the AP-5131 in order to improve throughput. These include certain broadcast frames from devices that consume bandwidth, but are unnecessary to AP-5131 operations.

Use the Ethernet Type Filter Configuration screen to build a list of filter types and configure them as either allowed or denied for use with the AP-5131.

To configure type filtering on the AP-5131:

1. Select Network Configuration -> LAN -> Type Filter from the AP-5131 menu tree.

The Ethernet Type Filter Configuration screen displays. No Ethernet types are displayed by default when the screen is first launched.
2. Use the all ethernet types, except drop-down menu to designate whether the Ethernet Types defined within this screen are allowed or denied for use by the AP-5131.

3. To add an Ethernet type, click the Add button. The Add Ethernet Type screen displays. Use this screen to add one type filter option at a time, for a list of up to 16 entries.

Packet types supported for the type filtering function include 16-bit DIX Ethernet types as well as Symbol proprietary types. Select an Ethernet type from the drop down menu, or enter the Ethernet type’s hexadecimal value. Consult with your System Administrator if unsure of the implication of adding or omitting a type from the list.
4. To optionally delete a type filtering selection from the list, highlight the packet type and click the Delete button.

5. Click Apply to save any changes to the Ethernet Type Filter Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

6. Click Cancel to securely exit the Ethernet Type Filter Configuration screen without saving your changes.

7. Click Logout within the Ethernet Type Filter Configuration screen to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

5.2 Configuring WAN Settings

A Wide Area Network (WAN) is a widely dispersed telecommunications network. The AP-5131 includes one WAN port. The AP-5131 WAN port has its own MAC address. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet.

Use the WAN screen to set the WAN IP configuration and Point-to-Point Protocol over Ethernet (PPPoE) parameters.

To configure WAN settings for the AP-5131:

1. Select Network Configuration -> WAN from the AP-5131 menu tree.
2. Refer to the **WAN IP Configuration** field to enable the WAN interface, and set network address information for the WAN connection.

**NOTE** Symbol recommends that the WAN and LAN ports should not both be configured as DHCP clients.

---

**Enable WAN Interface**

Select the *Enable WAN Interface* checkbox to enable a connection between the AP-5131 and a larger network or outside world through the WAN port.

Disable this option to effectively isolate the AP-5131's WAN. No connections to a larger network or the Internet are possible. MUs cannot communicate beyond the LAN.
| **This interface is a DHCP Client** | This checkbox enables DHCP for the AP-5131 WAN connection. This is useful, if the larger corporate network or Internet Service Provider (ISP) uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. If DHCP client mode is enabled, the other WAN IP configuration parameters are grayed out. |
| **IP Address** | Specify a numerical (non DNS name) IP address for the AP-5131's WAN connection. This address defines the AP's presence on a larger network or on the Internet. Obtain a static (dedicated) IP address from the ISP or network administrator. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1. |
| **Subnet Mask** | Specify a subnet mask for the AP-5131’s WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the AP-5131 connects to a larger network. A subnet mask uses a series of four numbers expressed in dot notation (similar to an IP address). For example, 255.255.255.0 is a valid subnet mask. |
| **Default Gateway** | Specify the gateway address for the AP-5131’s WAN connection. The ISP or a network administrator provides this address. |
| **Primary DNS Server** | Specify the address of a primary Domain Name System (DNS) server. The ISP or a network administrator provides this address. A DNS server translates a domain name (for example, www.symboltech.com) into an IP address that networks can use. |
| **Secondary DNS Server** | Specify the address of a secondary DNS server if one is used. A secondary address is recommended if the primary DNS server goes down. |
3. Configure the **PPP over Ethernet** field to enable high speed dial-up connections to the AP-5131 WAN port.

**Enable**

Use the checkbox to enable Point-to-Point over Ethernet (PPPoE) for a high-speed connection that supports this protocol. Most DSL providers are currently using or deploying this protocol. PPPoE is a data-link protocol for dialup connections. PPPoE allows a host PC to use a broadband modem (DSL) for access to high-speed data networks.

**Username**

Specify a username entered when connecting to the ISP. When the Internet session begins, the ISP authenticates the username.

**Password**

Specify a password entered when connecting to the ISP. When the Internet session starts, the ISP authenticates the password.
Network Management

4. Click **Apply** to save any changes to the WAN screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.
5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the WAN screen to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.2.1 Configuring Network Address Translation (NAT) Settings

*Network Address Translation (NAT)* converts an IP address in one network to a different IP address or set of IP addresses in another network. The AP-5131 router maps its local (inside) network addresses to WAN (outside) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. NAT can be applied in one of two ways:

- **One-to-one mapping with a private side IP address**
  The private side IP address can belong to any of the private side subnets.

- **One-to-many mapping with a configurable range of private side IP addresses**
  Ranges can be specified from each of the private side subnets.

Use the **NAT** screen to configure IP address mappings. To configure IP address mappings for the AP-5131:

1. Select **Network Configuration -> WAN -> NAT** from the AP-5131 menu tree.
2. Configure the **Address Mapping** field to generate a WAN IP address, define the NAT type and set outbound/inbound NAT mappings.

**WAN IP Address**

The WAN IP addresses on the NAT screen are dynamically generated from address settings applied on the **WAN** screen.

**NAT Type**

Specify the NAT Type as **1 to 1** to map a WAN IP address to a single host (local) IP address. 1 to 1 mapping is useful when users need dedicated addresses, and for public-facing servers connected to the AP-5131.

Set the NAT Type as **1 to Many** to map a WAN IP address to multiple local IP addresses. This displays the 1 to Many Mappings button in the adjacent Outbound Mappings field. This button displays a screen for mapping the LAN IP addresses that are associated with each subnet.

Define the NAT Type as **none** when routable IP addresses are used on the internal network.
3. Click **Apply** to save any changes to the NAT, 1 to Many Mappings and Port Forwarding screens. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

4. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the NAT screen to the last saved configuration.

5. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.2.1.1 Configuring Port Forwarding

Use the **Port Forwarding** screen to configure port forwarding parameters for inbound traffic from the associated WAN IP address.

To configure port forwarding for the AP-5131:

1. Select **Network Configuration -> WAN -> NAT** from the AP-5131 menu tree.
2. Click on the **Port Forwarding** button within the **Inbound Mappings** area.
3. Configure the **Port Forwarding** screen to modify the following:

- **Add**
  - Click **Add** to create a local map that includes the name, transport protocol, start port, end port, and IP address for incoming packets.

- **Delete**
  - Click **Delete** to remove a selected local map entry.

- **Name**
  - Enter a name for the service being forwarded. The name can be any alphanumeric string and is used for identification of the service.

- **Transport**
  - Use the **Transport** pull-down menu to specify the transport protocol used in this service. The choices are **ALL**, **TCP**, **UDP**, **ICMP**, **AH**, **ESP**, and **GRE**.

- **Start Port and End Port**
  - Enter the port or ports used by the port forwarding service. To specify a single port, enter the port number in the **Start Port** area. To specify a range of ports, use both the **Start Port** and **End Port** options to enter the port numbers. For example, enter 110 in the Start Port field and 115 in the End Port field.

- **IP Address**
  - Enter the numerical (non DNS name) IP address to which the specified service is forwarded. This address must be within the specified NAT range for the associated WAN IP address.

- **Translation Port**
  - Specify the port number used to translate data for the service being forwarded.
4. Click **Ok** to return to the NAT screen. Within the NAT screen, click **Apply** to save any changes made on the Port Forwarding screen.

5. Click **Cancel** to undo any changes made on Port Forwarding screen. This reverts all settings for the Port Forwarding screen to the last saved configuration.

### 5.3 Enabling Wireless LANs (WLANs)

A *Wireless Local Area Network (WLAN)* is a data-communications system that flexibly extends the functionalities of a wired LAN. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable. Within the WLAN, roaming users can be handed off from one AP-5131 to another like a cellular phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity.

Use the AP-5131’s **Wireless Configuration** screen to create new WLANs, edit the properties of existing WLANs or delete a WLAN to create space for a new WLAN. Sixteen WLANs are available on the AP-5131 (regardless of single or dual-radio model).

To configure WLANs on the AP-5131:

1. Select **Network Configuration -> Wireless** from the AP-5131 menu tree.
If a WLAN is defined, that WLAN displays within the Wireless Configuration screen. When the AP-5131 is first booted, WLAN1 exists as a default WLAN available immediately for connection.

2. Refer to the information within the Wireless Configuration screen to view the name, ESSID, AP-5131 radio designation, VLAN ID and security policy of existing WLANs.

WLAN Name

The Name field displays the name of each WLAN that has been defined. The WLAN names can be modified within individual WLAN configuration screens. See Creating/Editing Individual WLANs on page 5-24 to change the name of a WLAN.

ESSID

Displays the Extended Services Set Identification (ESSID) associated with each WLAN. The ESSID can be modified within individual WLAN configuration screens. See Creating/Editing Individual WLANs on page 5-24 to change the ESSID of a specific WLAN.

Radio

The Radio field displays the name of the AP-5131 radio the WLAN is mapped to (either the 802.11a radio or the 802.11b/g radio). To change the radio designation for a specific WLAN, see Creating/Editing Individual WLANs on page 5-24.
3. Click the **Create** button (if necessary) to launch the **New WLAN** screen. Use the New WLAN screen to define the properties of a new WLAN that would display and be selectable within the **Wireless Configuration** screen. For additional information, see Creating/Editing Individual WLANs on page 5-24.

4. Click the **Edit** button (if necessary) to launch the **Edit WLAN** screen. Use the Edit WLAN screen to revise the properties of an existing WLAN that would continue display and be selectable within the **Wireless Configuration** screen. For additional information, see Creating/Editing Individual WLANs on page 5-24.

5. Consider using the **Delete** button to remove an existing WLAN if it has become outdated and is no longer required or if you are coming close the maximum 16 WLANs available per AP-5131.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.3.1 Creating/Editing Individual WLANs

If the WLANs displayed within the **Wireless Configuration** screen do not satisfy your network requirements, you can either create a new WLAN or edit the properties of an existing WLAN.

#### VLAN

The **VLAN** field displays the specific VLAN the target WLAN is mapped to. For information on VLAN configuration for the WLAN, see Configuring VLAN Support on page 5-5.

#### Security Policy

The **Security Policy** field displays the security profile configured for the target WLAN. For information on configuring security for a WLAN, see Enabling Authentication and Encryption Schemes on page 6-5.

#### QoS Policy

The **QoS Policy** field displays the quality of service currently defined for the WLAN. This policy outlines which data types receive priority for the user base comprising the WLAN. For information on QoS configuration for the WLAN, see Setting the WLAN Quality of Service (QoS) Policy on page 5-31.

**NOTE** Before editing the properties of an existing WLAN, ensure it is not being used by an AP-5131 radio, or is a WLAN that is needed in its current configuration. Once updated, the previous configuration is not available unless saved.
Use the New WLAN and Edit WLAN screens as required to create/modify a WLAN. To create a new WLAN or edit the properties of an existing WLAN:

1. Select **Network Configuration -> Wireless** from the AP-5131 menu tree.
   
   The Wireless Configuration screen displays.

2. Click the **Create** button to configure a new WLAN, or highlight a WLAN and click the **Edit** button to modify an existing WLAN.

   Either the **New WLAN** or **Edit WLAN** screen displays.

3. Set the parameters in the **Configuration** field as required for the WLAN.

   **ESSID**
   
   Enter the *Extended Services Set Identification (ESSID)* associated with the WLAN. The WLAN name is auto-generated using the ESSID until changed by the user. The maximum number of characters that can be used for the ESSID is 32.

   **Name**
   
   Define or revise the name for the WLAN. The name should be logical representation of WLAN coverage area (engineering, marketing etc.). The maximum number of characters that can be used for the name is 31.

   **Available On**
   
   Use the **Available On** checkboxes to define which AP-5131 radio (802.11a or 802.11b/g) the target WLAN will reside.
Max MUs

Use the Max MUs field to define the number of MUs permitted to interoperate within the new or revised WLAN. The maximum (and default) is 127. Select a number that is appropriate with the intended radio traffic of that WLAN's radio coverage area.

NOTE: If 802.11a is selected as the radio used for the WLAN, the WLAN cannot use a Kerberos supported security policy.

4. Configure the Security field as required to set the data protection requirements for the WLAN.

Security Policy

Use the scroll down Security Policies menu to select the security scheme best suited for the new or revised WLAN. Click the Create button to jump to the New Security Policy screen where a new policy can be created to suit the needs of the WLAN. For more information, see Configuring WLAN Security Policies on page 5-27.

MU Access Control

Select an ACL policy suiting the WLAN's MU interoperability requirements from the drop-down menu. If the existing ACL policies do not satisfy the requirements of the WLAN, a new ACL policy can be created by pressing the Create button. For more information, see Configuring a WLAN Access Control List (ACL) on page 5-29.

Kerberos User Name

Displays the read-only Kerberos User Name used to associate the wireless client. This value is the ESSID of the AP-5131.

Kerberos Password

Enter a Kerberos password if Kerberos has been selected as the security scheme from within the Security Policies field. The field is grayed out if Kerberos has not been selected for the WLAN. For information on configuring Kerberos, see Configuring Kerberos Authentication on page 6-9.

5. Configure the Advanced field as required to set MU interoperability permissions, secure beacon transmissions, broadcast ESSID acceptance and Quality of Service (QoS) policies.
6. Click **Apply** to save any changes to the WLAN screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

7. Click **Cancel** to securely exit the New WLAN or Edit WLAN screen and return to the Wireless Configuration screen.

### 5.3.1.1 Configuring WLAN Security Policies

As WLANs are being defined for an AP-5131, a security policy can be created or an existing policy edited (using the **Create** or **Edit** buttons within the **Security Configuration** screen) to best serve the security requirements of the WLAN. Once new policies are defined, they are available within the **New WLAN** or **Edit WLAN** screens and can be mapped to any WLAN. A single security policy can be used by more than one WLAN if its logical to do so. For example, there may be two or more WLANs within close proximity of each other requiring the same data protection scheme.

To create a new security policy or modify an existing policy:

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disallow MU to MU Communication</strong></td>
<td>The AP-5131’s MU-MU Disallow feature prohibits MUs from communicating with each other even if they are on different WLANs, assuming one of the WLANs is configured to disallow MU-MU communication. Therefore, if an MU's WLAN is configured for MU-MU disallow, it will not be able to communicate with any other MUs connected to this AP-5131.</td>
</tr>
<tr>
<td><strong>Use Secure Beacon</strong></td>
<td>Select the <strong>Use Secure Beacon</strong> checkbox to not transmit the AP-5131's ESSID. If a hacker tries to find an ESSID via an MU, the AP-5131’s ESSID does not display since the ESSID is not in the beacon. Symbol recommends keeping the option enabled to reduce the likelihood of hacking into the WLAN.</td>
</tr>
<tr>
<td><strong>Accept Broadcast ESSID</strong></td>
<td>Select the <strong>Accept Broadcast ESSID</strong> checkbox to associate an MU that has a blank ESSID (regardless of which ESSID the AP-5131 is currently using). Sites with heightened security requirements may want to leave the checkbox unselected and configure each MU with an ESSID. The default is unselected, thus not allowing the acceptance of broadcast ESSIDs.</td>
</tr>
<tr>
<td><strong>Quality of Service Policy</strong></td>
<td>If QoS policies are undefined (none), select the <strong>Create</strong> button to launch the <strong>New QoS Policy</strong> screen. Use this screen to create a QoS policy, wherein data traffic for the new or revised WLAN can be prioritized to best suit the MU transmissions within that WLAN. For more information, see <strong>Setting the WLAN Quality of Service (QoS) Policy</strong> on page 5-31.</td>
</tr>
</tbody>
</table>
1. Select **Network Configuration -> Wireless -> Security** from the AP-5131 menu tree.

![Security Configuration Screen]

The **Security Configuration** screen appears with existing policies and their attributes displayed.

**NOTE** When the AP-5131 is first launched, a single security policy (default) is available and mapped to WLAN 1. It is anticipated numerous additional security policies will be created as the list of WLANs grows.

Configuring a WLAN security scheme with a discussion of all the authentication and encryption options available is beyond the scope of this chapter. Chapter 6 of the AP-5131 *Product Reference Guide* is dedicated to configuring AP-5131 security. For detailed information on the authentication and encryption options available to the AP-5131 and how to configure them, see to Configuring Security Options on page 6-2 and locate the section that describes your intended security scheme.

2. Click **Logout** to exit the Security Configuration screen.
5.3.1.2 Configuring a WLAN Access Control List (ACL)

An Access Control Lists (ACL) affords a system administrator the ability to grant or restrict MU access by specifying a MU MAC address or range of MAC addresses to either include or exclude from AP-5131 connectivity. Use the Mobile Unit Access Control List Configuration screen to create new ACL policies (using the New MU ACL Policy sub-screen) or edit existing policies (using the Edit MU ACL Policy sub-screen). Once new policies are defined, they are available for use within the New WLAN or Edit WLAN screens to assign to specific WLANs based on MU interoperability requirements.

Symbol recommends using the New MU ACL Policy or Edit MU ACL Policy screens strategically to name and configure ACL policies meeting the requirements of the particular WLANs they may map to. However, be careful not to name policies after specific WLANs, as individual ACL policies can be used by more than one WLAN. For detailed information on assigning ACL policies to specific WLANs, see Creating/Editing Individual WLANs on page 5-24.

To create or edit ACL policies for WLANs:

1. Select Network Configuration -> Wireless -> MU ACL from the AP-5131 menu tree.
   The Mobile Unit Access Control List Configuration screen displays with existing ACL policies and their current WLAN (if mapped to a WLAN).

---

**NOTE**  When the AP-5131 is first launched, a single ACL policy (default) is available and mapped to WLAN 1. It is anticipated numerous additional ACL policies will be created as the list of WLANs grows.
2. Click the **Create** button to configure a new ACL policy, or select a policy and click the **Edit** button to modify an existing ACL policy. The AP-5131 supports a maximum of 16 MU ACL policies.
Either the **New MU ACL Policy** or **Edit MU ACL Policy** screens display.

3. Assign a name to the new or edited ACL policy that represents an inclusion or exclusion policy specific to a particular type of MU traffic you may want to use with a single or group of WLANs. More than one WLAN can use the same ACL policy.

4. Configure the parameters within the **Mobile Unit Access Control List** field to allow or deny MU access to the AP-5131.

The MU adoption list identifies MUs by their MAC address. The MAC address is the MU’s unique **Media Access Control** number printed on the device (for example, 00:09:5B:45:9B:07) by the manufacturer. A maximum of 200 MU MAC addresses can be added to the New/Edit MU ACL Policy screen.

5. Click **Apply** to save any changes to the New MU ACL Policy or Edit MU ACL Policy screen and return to the Mobile Unit Access Control List Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

6. Click **Cancel** to securely exit the New MU ACL Policy or Edit MU ACL Policy screen and return to the Mobile Unit Access Control List Configuration screen.

7. Click **Logout** within the Mobile Unit Access Control List Configuration screen to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.3.1.3 Setting the WLAN Quality of Service (QoS) Policy

The AP-5131 can keep a list of QoS policies that can be used from the **New WLAN** or **Edit WLAN** screens to map to individual WLANs. Use the **Quality of Service Configuration** screen to configure WMM policies that can improve the user experience for audio, video and voice applications by shortening the time between packet transmissions for higher priority (multimedia) traffic.

Use the **Quality of Service Configuration** screen to define the QoS policies for advanced network traffic management and multimedia applications support. If the existing QoS policies are insufficient,
a new policy can be created or an existing policy can be modified using the **New QoS Policy** or **Edit QoS Policy** screens. Once new policies are defined, they are available for use within the **New WLAN** or **Edit WLAN** screens to assign to specific WLANs based on MU interoperability requirements.

Symbol recommends using the New QoS Policy and Edit QoS Policy screens strategically to name and configure QoS policies meeting the requirements of the particular WLANs they may map to. However, be careful not to name policies after specific WLANs, as individual QoS policies can be used by more than one WLAN. For detailed information on assigning QoS policies to specific WLANs, see *Creating/Editing Individual WLANs on page 5-24*.

To configure QoS policies:

1. Select **Network Configuration** -> **Wireless** -> **QoS** from the AP-5131 menu tree.

The **Quality of Service Configuration** screen displays with existing QoS policies and their current WLAN (if mapped to a WLAN).

| NOTE | When the AP-5131 is first launched, a single QoS policy (default) is available and mapped to WLAN 1. It is anticipated additional QoS policies will be created as the list of WLANs grows. |
2. Click the Create button to configure a new QoS policy, or select a policy and click the Edit button to modify an existing QoS policy. The AP-5131 supports a maximum of 16 QoS policies.
3. Assign a name to the new or edited QoS policy that makes sense to the AP-5131 traffic receiving priority. More than one WLAN can use the same QoS policy.

4. Select the **Support Voice prioritization** checkbox to allow legacy voice prioritization. Certain products may not receive priority over other voice or data traffic. Consequently, ensure the **Support Voice Prioritization** checkbox is selected if using products that do not support Wi-Fi Multimedia (WMM) to provide preferred queuing for these VOIP products.

If the **Support Voice Prioritization** checkbox is selected, the AP-5131 will detect non-WMM capable (legacy) phones that connect to the AP-5131 and provide priority queueing for their traffic over normal data.
5. Use the two **Multicast Address** fields to specify one or two MAC addresses to be used for multicast applications. Some VoIP devices make use of multicast addresses. Using this mechanism ensures that the multicast packets for these devices are not delayed by the packet queue.

6. Select the **Enable Wi-Fi Multimedia (WMM) QoS Extensions** checkbox to configure the AP-5131’s QoS Access Categories. The Access Categories are not configurable unless the checkbox is selected. Access Categories include:

- **Background**
  Backgrounds traffic is typically of a low priority (file transfers, print jobs etc.). Background traffic typically does not have strict latency (arrival) and throughput requirements.

- **Best Effort**
  Best Effort traffic includes traffic from legacy devices or applications lacking QoS capabilities. Best Effort traffic is negatively impacted by data transfers with long delays as well as multimedia traffic.

- **Video**
  Video traffic includes music streaming and application traffic requiring priority over all other types of network traffic.

- **Voice**
  Voice traffic includes VoIP traffic and typically receives priority over Background and Best Effort traffic.

7. Configure the **CW min** and **CW max** (contention windows), **AIFSN** (*Arbitrary Inter-Frame Space Number*) and **TXOPs Time** (opportunity to transmit) for each Access Category. Their values are explained below.

   - **CW Min**
     The contention window minimum value is the least amount of time the MU waits before transmitting when there is no other data traffic on the network. The longer the interval, the lesser likelihood of collision. This value should be set to a smaller increment for higher priority traffic. Reduce the value when traffic on the WLAN is anticipated as being smaller.
8. Select the **Set Default Values** button (if needed), to restore all the field values to their factory defaults. Symbol recommends default settings in most usage scenarios.

9. Click **Apply** to save any changes to the New QoS Policy or Edit QoS Policy screen to return to the Quality of Service Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

10. Click **Cancel** to securely exit the New QoS Policy or Edit QoS Policy screen to return to the Quality of Service Configuration screen.

11. Click **Logout** within the Quality of Service Configuration screen to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.3.2 Setting the WLAN’s Radio Configuration

Each AP-5131 WLAN can have a separate 802.11a or 802.11b/g radio configured and mapped to that WLAN. The first step is to enable the radio.

One of two possible radio configuration pages are available on the AP-5131 depending on which model SKU is purchased. If the AP-5131 is a single-radio model, the **Radio Configuration** screen enables you to configure the single radio for either 802.11a or 802.11b/g use. The Radio Configuration screen contains two radio buttons whose selection is mutually exclusive.
If the AP-5131 is a dual-radio model, the Radio Configuration screen enables you to configure one radio for 802.11a use and the other for 802.11b/g (no other alternatives exist for the dual-radio model). Using a dual-radio AP-5131, individual 802.11a and 802.11b/g radios can be enabled or disabled using the Radio Configuration screen checkboxes.

To set the AP-5131 radio configuration (this example is for a dual-radio AP-5131):


2. Enable the radio(s) using the Enable Radio checkbox(es).

   If using a single-radio model, enable the radio then select either 802.11a (5 GHz) or 802.11b/g (2.4 GHz) from the RF band of operation field. Only one RF band option is permissible in a single-radio model.

   If using a dual-radio model, enable either 802.11a (5 GHz) or 802.11b/g (2.4 GHz) from the RF band of operation field.

   **CAUTION** If a radio is disabled, be careful not to accidentally configure a new WLAN, expecting the radio to be operating when you have forgotten it was disabled.
3. Click **Apply** to save any changes to the Radio Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

4. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Radio Configuration screen to the last saved configuration.

5. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

Once the target radio has been enabled from the Radio Configuration screen, configure the radio’s properties by selecting it from the AP-5131 menu tree.

For more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-38.*

### 5.3.2.1 Configuring the 802.11a or 802.11b/g Radio

Configure an 802.11a or 802.11b/g radio by selecting the radio’s name (as defined using the 802.11a or 802.11b/g radio configuration screen described below) as a sub-menu item under the Radio Configuration menu item. Use the radio configuration screen to set the radio’s placement properties, define the radio’s threshold and QoS settings, set the radio’s channel and antenna settings and define beacon and DTIM intervals.

To configure the AP-5131’s 802.11a or 802.11b/g radio:

1. Select **Network Configuration -> Wireless -> Radio Configuration -> Radio1** (default name) from the AP-5131 menu tree.

On a single-radio AP-5131, Radio1 could either be an 802.11a or 802.11b/g radio depending on which radio has been enabled.
2. Configure the **Properties** field to assign a name and placement designation for the radio.

   **Placement**
   Use the **Placement** drop-down menu to specify whether the radio is located outdoors or indoors. Default placement depends on the country of operation selected for the AP-5131.

   **MAC Address**
   The AP-5131, like other Ethernet devices, has a unique, hardware encoded **Media Access Control (MAC)** or IEEE address. MAC addresses determine the device sending or receiving data. A MAC address is a 48-bit number written as six hexadecimal bytes separated by colons. For example: 00:A0:F8:24:9A:C8

   **Radio Type**
   The **Radio Type** parameter simply displays the radio type as 802.11a or 802.11b/g. This field is read only and always displays the radio type selected from the AP-5131 menu tree under the Radio Configuration item.

3. Configure the **Radio Setting** field to assign a channel, antenna diversity setting, radio transmit power level and data rate.
Channel Setting

The following channel setting options exist:

- **User Selection** - If selected, use the drop-down menu to specify the legal channel for the intended country of operation. The drop-down menu is not available if this option is not selected.
- **Automatic Selection** - Enables the AP-5131 to auto-select the channel of operation. For example, if three AP-5131’s are operating on 802.11b/g, each AP-5131 would be set to a non-overlapping channel (1, 6 and 11). If using the AP-5131’s 802.11a radio, a **Uniform Spreading** option is available (and is the default setting for the 802.11a radio). To comply with **Dynamic Frequency Selection** (DFS) requirements in the European Union, the 802.11a radio uses a randomly selected channel each time the AP-5131 is powered on.

Antenna Diversity

 Specifies the antenna selection for the 802.11a radio. Options include **Primary Only**, **Secondary Only** and **Full Diversity**. The default setting is Primary. However, Diversity can improve performance and signal reception in areas where interference is significant and is recommended when two antennas are supported.

Power Level

The **Power Level** parameter defines the transmit power of the 802.11a or 802.11b/g antenna(s). The values are expressed in dBm and mW.

802.11 b/g mode

Specify **b only**, **g only** or **b and g** to define whether the 802.11b/g radio transmits in the 2.4 Ghz band exclusively for 802.11b (legacy) clients or transmits in the 2.4 Ghz band for 802.11g clients. Selecting **b and g** enables the AP-5131 to transmit to both b and g clients if legacy clients (802.11b) partially comprise the network. Select accordingly based on the MU requirements of the network. This parameter does not apply to AP-5131 802.11a radios.

Set Rates

Click the **Set Rates** button to display a window for selecting minimum and maximum data transmit rates for the radio. At least one **Basic Rate** must be selected as a minimum transmit rate value. **Supported Rates** define the data rate the radio defaults to if a higher selected data rate cannot be maintained. Click **OK** to implement the selected rates and return to the 802.11a or 802.11b/g radio configuration screen. Clicking **Cancel** reverts the Set Rates screen to the last saved configuration. Symbol recommends using the default rates unless qualified to understand the performance risks of changing them.
4. Configure the **Performance** field to set the preamble, thresholds values, data rates and QoS values for the radio.

*Support Short Preamble*  The preamble is approximately 8 bytes of packet header generated by the AP-5131 and attached to the packet prior to transmission from the 802.11b radio. The preamble length for 802.11b transmissions is data rate dependant. The short preamble is 50% shorter than the long preamble. Leave the checkbox unselected if in a mixed MU/AP environment, as MUs and the AP-5131 are required to have the same RF Preamble settings for interoperability. The default is Disabled. The preamble length for 802.11a and 802.11g transmissions is the same, with no long or short preamble lengths.

*RTS Threshold*  RTS allows the AP-5131 to use RTS (Request To Send) on frames longer than the specified length. The default is 2341 bytes.
5. Refer to the **Beacon Settings** field to set the radio beacon and DTIM intervals.

**Set RF QoS**

Click the **Set RF QoS** button to display the **Set RF QOS** screen to set QoS parameters for the AP-5131 radio. This setting should not be confused with the QoS configuration screen used for a WLAN. The Set RF QoS screen initially appears with default values displayed.

Configure the **CW min** and **CW max** (contention window), **AIFSN** (**Arbitrary Inter-Frame Space Number**) and **TXOPs Time** for each Access Category. These are the QoS policies for the 802.11a or 802.11b/g radio, not the QoS policies configured for the WLAN (as created or edited from the Quality of Service Configuration screen). Click the **Set Default Values** button to restore factory default CW, AIFSN and TXOPs values to the Set RF QoS screen.

Click **OK** to implement the selected QoS values and return to the 802.11a or 802.11b/g radio configuration screen. Clicking **Cancel** reverts the screen to the last saved configuration.
Network Management

6. Select the **Advanced Settings** tab to strategically map BSSIDs to WLANs in order to define them as primary WLANs.

- **Beacon Interval**
  The beacon interval controls the performance of power save stations. A small interval may make power save stations more responsive, but it will also cause them to consume more battery power. A large interval makes power save stations less responsive, but could increase power savings.
  The default is 100. Avoid changing this parameter as it can adversely affect performance.

- **DTIM Interval**
  The DTIM interval defines how often broadcast frames are delivered. If a system has an abundance of broadcast traffic and it needs to be delivered quickly, Symbol recommends decreasing the DTIM interval. However, decreasing the DTIM interval decreases the battery life on power save stations. The default is 10. Symbol recommends using the default value unless qualified to understand the performance risks of changing it.

![Image of AP-5131 Access Point interface](image)
Defining Primary WLANs allows an administrator to dedicate BSSIDs (4 BSSIDs are available for mapping) to WLANs. From that initial BSSID assignment, Primary WLANs can be defined from within the WLANs assigned to BSSID groups 1 through 4. Each BSSID beacons only on the primary WLAN.

The user should assign each WLAN to its own BSSID. In cases where more than four WLANs are required, WLANs should be grouped according to their security policies so all of the WLANs on a BSSID have the same security policy. It is generally a bad idea to have WLANs with different security policies on the same BSSID, as this will result in warning or error messages.

### NOTE

If using a single-radio AP-5131, there are 4 BSSIDs available. If using a dual-radio AP-5131, 4 BSSIDs for the 802.11b/g radio and 4 BSSIDs for the 802.11a radio are available.

<table>
<thead>
<tr>
<th>WLAN</th>
<th>Lists the WLAN names available to the 802.11a or 802.11b/g radio that can be assigned to a BSSID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>Assign a BSSID value of 1 through 4 to a WLAN in order to map the WLAN to a specific BSSID.</td>
</tr>
<tr>
<td>BC/MC Cipher</td>
<td>A read only field displaying the downgraded BC/MC (Broadcast/Multicast) cipher for a WLAN based on the BSSID and VLAN ID to which it has been mapped.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the following color coded status:</td>
</tr>
<tr>
<td></td>
<td>Red - Error (Invalid Configuration)</td>
</tr>
<tr>
<td></td>
<td>Yellow - Warning (Broadcast Downgrade)</td>
</tr>
<tr>
<td></td>
<td>Green - Good (Configuration is OK)</td>
</tr>
<tr>
<td>Message</td>
<td>Displays the verbal status of the WLAN and BSSID assignments. If the Status column displays green, the Message will typically be <strong>Configuration is OK</strong>. If yellow, a description of invalid configuration displays.</td>
</tr>
</tbody>
</table>

7. Use the Primary WLAN drop-down menu to select a WLAN from those WLANs sharing the same BSSID. The selected WLAN is the primary WLAN for the specified BSSID.
8. Click **Apply** to save any changes to the Radio Settings and Advanced Settings screens. Navigating away from the screen without clicking Apply results in changes to the screens being lost.

9. Click **Undo Changes** (if necessary) to undo any changes made to the screen and its sub-screens. Undo Changes reverts the settings to the last saved configuration.

10. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 5.3.3 Configuring Bandwidth Management Settings

The AP-5131 can be configured to grant individual WLAN’s network bandwidth priority levels. Use the **Bandwidth Management** screen to control the network bandwidth allotted to WLANs. Symbol recommends defining a weighed scheme as needed when WLAN traffic supporting a specific network segment becomes critical.

1. Select **Network Configuration -> Wireless -> Bandwidth Management** from the AP-5131 menu tree.

2. Use the **Bandwidth Share Mode** drop-down menu to define the order enabled WLANs receive AP-5131 services. Select one of the following three options:
3. Configure the **Bandwidth Share for Each WLAN** field to set a raw weight (for WLANs using the Weighted Round-Robin option) for each WLAN. The weight % changes as the weight is entered.

If a WLAN has not been enabled from the Wireless screen, it is not configurable using the Bandwidth Management screen. To enable a specific WLAN, see *Enabling Wireless LANs (WLANs)* on page 5-22.

<table>
<thead>
<tr>
<th>First In First Out</th>
<th>WLANs receive services from the AP-5131 on a first-come, first-served basis. This is the default setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round-Robin</td>
<td>Each WLAN receives AP-5131 services in turn as long the AP-5131 has data traffic to forward.</td>
</tr>
<tr>
<td>Weighted Round-Robin</td>
<td>If selected, a weighting (prioritization) scheme (configured within the QoS Configuration screen) is used to define which WLANs receive AP-5131 resources first.</td>
</tr>
</tbody>
</table>

4. Click **Apply** to save any changes to the Bandwidth Management screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Bandwidth Management screen to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.
5.4 Configuring Router Settings

The AP-5131 router uses routing tables and protocols to forward data packets from one network to another. The AP-5131 router manages traffic within the network, and directs traffic from the WAN to destinations on the AP-5131 managed LAN. Use the AP-5131 Router screen to view the router’s connected routes. To access the Router screen.

1. Select Network Configuration -> Router from the AP-5131 menu tree.

2. Refer to the AP-5131 Router Table field to view existing routes.

The AP-5131 Router Table field displays a list of connected routes between an enabled subnet and the router. These routes can be changed by modifying the IP address and subnet masks of the enabled subnets.
The information in the AP-5131 Router Table is dynamically generated from settings applied on the **WAN** screen. The destination for each subnet is its IP address. The subnet mask (or network mask) and gateway settings are those belonging to each subnet. Displayed interfaces are those associated with destination IP addresses. To change any of the network address information within the WAN screen, see *Configuring WAN Settings on page 5-13*.

3. Use the **User Defined Routes** field to add or delete static routes.

The User Defined Routes field allows the administrator to view, add or delete internal static (dedicated) routes. Internal static routes are dedicated routes for data that travels from the WAN, through the AP-5131, and to a specified location.

   a. Click the **Add** button to create a new table entry.
   
   b. Highlight an entry and click the **Del** (delete) button to remove an entry.
   
   c. Specify the destination IP address, subnet mask, and gateway information for the internal static route.
   
   d. Select an enabled subnet from the **Interface(s)** column’s drop-down menu to complete the table entry. Information in the **Metric** column is a user-defined value (from 1 to 65535) used by router protocols to determine the best hop routes.

4. Click the **Apply** button to save the changes.

5. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.
Configuring Access Point Security

Security measures for the AP-5131 and its WLANs are critical. Use the available AP-5131 security options to protect the AP-5131 LAN from wireless vulnerabilities, and safeguard the transmission of RF packets between the AP-5131 and its associated MUs.

WLAN security can be configured on an ESS by ESS basis on the AP-5131. Sixteen separate ESSIDs (WLANs) can be supported on an AP-5131, and must be managed (if necessary) between the 802.11a and 802.11b/g radio. The user has the capability of configuring separate security policies for each WLAN. Each security policy can be configured based on the authentication (Kerberos, 802.1x EAP) or encryption (WEP, KeyGuard, WPA/TKIP or WPA2/CCMP) scheme best suited to the coverage area that security policy supports.

The AP-5131 can also create VPN tunnels to securely route traffic through a IPSEC tunnel and block transmissions with devices interpreted as Rogue AP’s.
6.1 Configuring Security Options

To configure the data protection options available on the AP-5131, refer to the following:

- To set an administrative password for secure AP-5131 logins, see Setting Passwords on page 6-3.
- Refer to Enabling Authentication and Encryption Schemes on page 6-5 to display security policy screens used to configure the authentication and encryption schemes available to the AP-5131. These security policies can be used on more than one WLAN.
- To create a security policy supporting 802.1x EAP, see Configuring 802.1x EAP Authentication on page 6-11.
- To define a security policy supporting Kerberos, see Configuring Kerberos Authentication on page 6-9.
- To create a security policy supporting WEP, see Configuring WEP Encryption on page 6-15.
- To configure a security policy supporting KeyGuard, see Configuring KeyGuard Encryption on page 6-17.
- To define a security policy supporting WPA-TKIP, see Configuring WPA Using TKIP on page 6-19.
- To create a security policy supporting WPA2-CCMP, see Configuring WPA2-CCMP (802.11i) on page 6-22.
- To configure the AP-5131 to block specific kinds of HTTP, SMTP and FTP data traffic, see Configuring Firewall Settings on page 6-25.
- To create VPN tunnels allowing traffic to route securely through a IPSEC tunnel to a private network, see Configuring VPN Tunnels on page 6-33.
- To configure the AP-5131 to block transmissions with devices detected as Rogue AP's (hostile devices), see Configuring Rogue AP Detection on page 6-51.
6.2 Setting Passwords

Before setting the AP-5131 security parameters, verify an administrative password for the AP-5131 has been created to restrict access to the device before advanced device security is configured.

To password protect and restrict AP-5131 device access:

1. Connect a wired computer to the AP-5131 LAN port using a standard CAT-5 cable.
2. Set up the computer for TCP/IP DHCP network addressing and make sure the DNS settings are not hardcoded.
3. Start up Internet Explorer (with Sun Micro Systems' Java Runtime Environment (JRE) 1.5 or higher installed) and type in the default IP address in the address field: 192.168.0.1. If the default IP address has been changed, ensure the correct IP address is entered.

NOTE For optimum compatibility use Sun Microsystems' JRE 1.5 or higher (available from Sun's Web site), and be sure to disable Microsoft's Java Virtual Machine if it is installed.

NOTE DNS names are not supported as a valid IP address for the AP-5131. The user is required to enter a numerical IP address.

The AP-5131 Login screen displays.
4. Log in using the “admin” as the default User ID and “symbol” as the default Password. If the default login is successful, the Change Admin Password window displays. Change the default login and password to significantly decrease the likelihood of hacking.

5. Enter the previous password and the new admin password in the two fields provided. Click the Apply button. Once the admin password has been created/updated, the System Settings screen displays. If the AP-5131 has not had its System Settings (device name, location etc.) configured, see Configuring System Settings on page 4-2.

Once the password has been set, refer back to Configuring Security Options on page 6-2 to determine which AP-5131 security feature to configure next.

6.2.1 Resetting the AP-5131 Password

The AP-5131 Command Line Interface (CLI) enables users who forget their password to reset it to the factory default (symbol). From there, a new password can be defined.

To reset the AP-5131 password back to its default setting:

1. Connect one end of a null modem serial cable to the AP-5131’s serial connector.
2. Attach the other end of the null modem serial cable to the serial port of a PC running HyperTerminal or a similar emulation program.
3. Set the HyperTerminal program to use 19200 baud, 8 data bits, 1 stop bit, no parity, no flow control and auto-detect for terminal emulation.
4. Press <ESC> or <Enter> to access the AP-5131 CLI.
   A serial connection has now been established and the user should be able to view the serial connection window.
5. Reset the AP-5131.
An AP-5131 can be reset by removing and re-inserting the LAN cable or removing and re-inserting the power cable.

As the AP-5131 is re-booting, a “Press esc key to run boot firmware” message displays.

6. Quickly press <ESC>.

| CAUTION | If the <ESC> key is not pressed within three seconds after the “Press esc key to run boot firmware” message displays, the AP-5131 will continue to boot.

If the <ESC> key is pressed within three seconds a boot> prompt displays.

7. Type the following at the boot prompt:

   passwd default

8. Reset the AP-5131 by typing the following at the boot prompt:

   reset system

   When the AP-5131 re-boots again, the password will return to its default value of “symbol.”

You can now access the AP-5131.

### 6.3 Enabling Authentication and Encryption Schemes

To complement the built-in firewall filters on the WAN side of the AP-5131, the WLAN side of the AP-5131 supports authentication and encryption schemes. Authentication is a challenge-response procedure for validating user credentials such as username, password, and sometimes secret-key information. The AP-5131 provides two schemes for authenticating users: 802.1x EAP and Kerberos.

Encryption applies a specific algorithm to alter its appearance and prevent unauthorized reading. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver must employ the same encryption/decryption method to interoperate.

*Wired Equivalent Privacy (WEP)* is available in two encryption modes: 40 bit (also called WEP 64) and 104 bit (also called WEP 128). The 104-bit encryption mode provides a longer algorithm (better security) that takes longer to decode (hack) than the 40-bit encryption mode.

Each WLAN (16 WLANs available in total to an AP-5131 regardless of the model) can have a separate security policy. However, more than one WLAN can use the same security policy. Therefore, to avoid confusion, do not name security policies the same name as WLANs. Once security policies have been created, they are selectable within the **Security** field of each **WLAN** screen. If the existing default
security policy does not satisfy the data protection requirements of a specific WLAN, a new security policy (using the authentication and encryption schemes discussed above) can be created.

To enable an existing WLAN security policy or create a new policy:

1. Select **Network Configuration** -> **Wireless** -> **Security** from the AP-5131 menu tree.
   
The **Security Configuration** screen displays.

2. If a new security policy is required, click the **Create** button.

The **New Security Policy** screen displays with the **Manually Pre-shared key/No authentication** and **No Encryption** options selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a guest network wherein no sensitive data is either transmitted or received.

However, selecting any other authentication or encryption checkbox displays a configuration field for the selected security scheme within the **New Security Policy** screen.
3. Use the **Name** field to define a logical security policy name.

Remember, multiple WLANs can share the same security policy, so be careful not to name security policies after specific WLANs or risk defining a WLAN to single policy. Symbol recommends naming the policy after the attributes of the authentication or encryption type selected (for example, *WPA2 Allow TKIP*).

4. Enable and configure an **Authentication** option if necessary for the target security policy.

   *Manually Pre-Shared Key / No Authentication*  
   Select this button to disable authentication. This is the default value for the **Authentication** field.

   *Kerberos*  
   Select the **Kerberos** button to display the **Kerberos Configuration** field within the New Security Policy screen. For specific information on configuring Kerberos, see *Configuring Kerberos Authentication on page 6-9*.

   *802.1x EAP*  
   Select the **802.1x EAP** button to display the **802.1x EAP Settings** field within the New Security Policy screen. For specific information on configuring EAP, see *Configuring 802.1x EAP Authentication on page 6-11*.

5. Enable and configure an **Encryption** option if necessary for the target security policy.

   *No Encryption*  
   If **No Encryption** is selected, encryption is disabled for the security policy. If security is not an issue, this setting avoids the overhead an encryption protocol causes on the AP-5131. No Encryption is the default value for the Encryption field.

   *WEP 64 (40-bit key)*  
   Select the **WEP 64 (40 bit key)** button to display the **WEP 64 Settings** field within the New Security Policy screen. For specific information on configuring WEP 64, see *Configuring WEP Encryption on page 6-15*.
6. Click **Apply** to keep changes made within the New Security Policy screen (if any).

Configure encryption or authentication supported security policies by referring to the following:

**AP-5131 authentication**
- To create a security policy supporting Kerberos, see [*Configuring Kerberos Authentication on page 6-9*](#).
- To define a security policy supporting 802.1x EAP, see [*Configuring 802.1x EAP Authentication on page 6-11*](#).

**AP-5131 encryption**
- To create a security policy supporting WEP, see [*Configuring WEP Encryption on page 6-15*](#).
- To define a security policy supporting KeyGuard, see [*Configuring KeyGuard Encryption on page 6-17*](#).
- To configure a security policy supporting WPA/TKIP, see [*Configuring WPA Using TKIP on page 6-19*](#).
- To create a security policy supporting WPA2/CCMP, see [*Configuring WPA2-CCMP (802.11i) on page 6-22*](#).
7. Click **Cancel** to return to the target WLAN screen without keeping any of the changes made within the New Security Policy screen.

### 6.4 Configuring Kerberos Authentication

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection. Once a client and server use Kerberos to prove their identity, they can encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the AP-5131 with Symbol clients.

---

**CAUTION** Kerberos makes no provisions for host security. Kerberos assumes that it is running on a trusted host with an untrusted network. If host security is compromised, Kerberos is compromised as well.

Kerberos uses the *Network Time Protocol (NTP)* for synchronizing the clocks of its *Key Distribution Center (KDC)* server(s). Use the *NTP Servers* screen to specify the IP addresses and ports of available NTP servers. Kerberos requires the *Enable NTP on AP-5131* checkbox be selected for authentication to function properly. See [*Configuring Network Time Protocol (NTP)* on page 4-26](#) to configure the NTP server.

---

**NOTE** If 802.11a is selected as the radio used for a specific WLAN, the WLAN cannot use a Kerberos supported security policy, as no 802.11a clients can support Kerberos on the AP-5131.

To configure Kerberos on the AP-5131:

1. Select **Network Configuration -> Wireless -> Security** from the AP-5131 menu tree. If security policies supporting Kerberos exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting Kerberos, continue to step 2.

2. Click the **Create** button to configure a new policy supporting Kerberos. The *New Security Policy* screen displays with no authentication or encryption options selected.

3. Select the **Kerberos** radio button.
The *Kerberos Configuration* field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.

5. Set the **Kerberos Configuration** field as required to define the parameters of the Kerberos authentication server and AP-5131.

- **Realm Name**
  
  Specify a realm name that is case-sensitive, for example, SYMBOL.COM. The realm name is the name domain/realm name of the KDC Server. A realm name functions similarly to a DNS domain name. In theory, the realm name is arbitrary. However, in practice a Kerberos realm is named by uppercasing the DNS domain name that is associated with hosts in the realm.
Configuring Access Point Security

6. Click the **Apply** button to return to the **WLAN** screen to save any changes made within the Kerberos Configuration field of the New Security Policy screen.

7. Click the **Cancel** button to undo any changes made within the Kerberos Configuration field and return to the **WLAN** screen. This reverts all settings for the Kerberos Configuration field to the last saved configuration.

6.5 Configuring 802.1x EAP Authentication

The IEEE 802.1x standard ties the 802.1x EAP authentication protocol to both wired and wireless LAN applications.

The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). The AP-5131 passes EAP packets from the client to an authentication server on the wired side of the AP-5131. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the MU's identity.

To configure 802.1x EAP authentication on the AP-5131:

1. Select **Network Configuration -> Wireless -> Security** from the AP-5131 menu tree.

   If security policies supporting 802.1x EAP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited
by clicking the **Edit** button. To configure a new security policy supporting 802.1x EAP, continue to step 2.

2. Click the **Create** button to configure a new policy supporting 802.1x EAP.

   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select the **802.1x EAP** radio button.

   The **802.1x EAP Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.

5. Configure the **Server Settings** field as required to define address information for the authentication server.
### Radius Server Address
Specify the numerical (non-DNS) IP address of a primary Remote Dial-In User Service (RADIUS) server. Optionally, specify the IP address of a secondary server. The secondary server acts as a failover server if the primary server cannot be contacted. An ISP or a network administrator provides these addresses. RADIUS is a client/server protocol and software enabling remote-access clients to communicate with a server used to authenticate users and authorize access to the requested system or service.

### RADIUS Port
Specify the port on which the primary RADIUS server is listening. Optionally, specify the port of a secondary (failover) server. Older RADIUS servers listen on ports 1645 and 1646. Newer servers listen on ports 1812 and 1813. Port 1645 or 1812 is used for authentication. Port 1646 or 1813 is used for accounting. The ISP or a network administrator needs to confirm the appropriate primary and secondary port numbers for authentication.

### RADIUS Shared Secret
Specify a shared secret for authentication on the primary RADIUS server. The shared secret is required to match the shared secret on the Radius server. Optionally, specify a shared secret for a secondary (failover) server. Use shared secrets to verify RADIUS messages (with the exception of the Access-Request message) sent by a RADIUS-enabled device configured with the same shared secret.

Apply the qualifications of a well-chosen password to the generation of a shared secret. Generate a random, case-sensitive string using letters, numbers and symbols. Verify the shared secret is at least 22 characters to protect the RADIUS server from brute-force attacks. An example of a strong and secure shared secret is: `8d#>9fq4bV)H7%a3-zE13sW`.

6. Select the **Advanced Settings** tab as required to specify a MU quiet period, timeout interval, transmit period, and retry period for MUs and the authentication server.

<table>
<thead>
<tr>
<th><strong>MU Quiet Period</strong>&lt;br&gt;<strong>(1-65535) secs</strong></th>
<th>Specify an idle time (in seconds) between MU authentication attempts, as required by the authentication server. The default is 10 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MU Timeout</strong>&lt;br&gt;<strong>(1-255) secs</strong></td>
<td>Define the time (in seconds) for the AP-5131’s retransmission of EAP-Request packets. The default is 10 seconds.</td>
</tr>
</tbody>
</table>
7. Select the **Reauthentication** tab as required to define authentication connection policies, intervals and maximum retries.

   **Enable Reauthentication**  
   Select the **Enable Reauthentication** checkbox to configure a wireless connection policy so MUs are forced to reauthenticate periodically. Periodic repetition of the EAP process provides ongoing security for current authorized connections.

   **Period (30-9999) secs**  
   Set the EAP reauthentication period to a shorter time interval (at least 30 seconds) for tighter security on the WLAN’s connections. Set the EAP reauthentication period to a longer time interval (at most, 9999 seconds) to relax security on wireless connections. The reauthentication period setting does not affect wireless connection throughput. The default is 3600 seconds.

   **Max. Retries (1-99) retries**  
   Define the maximum number of MU retries to reauthenticate after failing to complete the EAP process. Failure to reauthenticate in the specified number of retries results in a terminated connection. The default is 2 retries.

8. Select the **Radius Accounting** tab as required to define a timeout period and retry intervalSyslog for MUs interoperating with the AP-5131 and EAP authentication server.

   **Enable Accounting**  
   Select the **Enable Accounting** checkbox to implement the MU timeout and retry definitions configured within the Radius Accounting field.
Configuring Access Point Security

9. Click the **Apply** button to save any changes made within the 802.1x EAP Settings field (including all 5 selectable tabs) of the New Security Policy screen.

10. Click the **Cancel** button to undo any changes made within the 802.1x EAP Settings field and return to the **WLAN** screen. This reverts all settings for the 802.1x EAP Settings field to the last saved configuration.

### 6.6 Configuring WEP Encryption

**Wired Equivalent Privacy (WEP)** is a security protocol specified in the *IEEE Wireless Fidelity (Wi-Fi)* standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP may be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP on the AP-5131:

1. Select **Network Configuration** -> **Wireless** -> **Security** from the AP-5131 menu tree.

   If security policies supporting WEP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting WEP, continue to step 2.

2. Click the **Create** button to configure a new policy supporting WEP.

   The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select either the **WEP 64 (40 bit key)** or **WEP 128 (104 bit key)** radio button.
The **WEP 64 Settings** or **WEP 128 Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.

5. Configure the **WEP 64 Settings** or **WEP 128 Settings** field as required to define the Pass Key used to generate the WEP keys. These keys must be the same between the AP-5131 and its MU to encrypt packets between the two devices.

   **Pass Key**
   Specify a 4 to 32 character pass key and click the **Generate** button. The pass key can be any alphanumeric string. The AP-5131, other proprietary routers and Symbol MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Symbol adapters need to use WEP keys manually configured as hexadecimal numbers.
Configuring Access Point Security

6-17

Default (hexadecimal) keys for WEP 64 include:

Key 1 1011121314
Key 2 2021222324
Key 3 3031323334
Key 4 4041424344

Default (hexadecimal) keys for WEP 128 include:

Key 1 101112131415161718191A1B1C
Key 2 202122232425262728292A2B2C
Key 3 303132333435363738393A3B3C
Key 4 404142434445464748494A4B4C

6. Click the Apply button to save any changes made within the WEP 64 Setting or WEP 128 Setting field of the New Security Policy screen.

7. Click the Cancel button to undo any changes made within the WEP 64 Setting or WEP 128 Setting field and return to the WLAN screen. This reverts all settings to the last saved configuration.

6.7 Configuring KeyGuard Encryption

KeyGuard is a proprietary encryption method developed by Symbol Technologies. KeyGuard is Symbol’s enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

WPA2-CCMP (not KeyGuard) offers the highest level of security among the encryption methods available with the AP-5131.

If security policies supporting KeyGuard exist, they appear within the Security Configuration screen. These existing policies can be used as is, or their properties edited by clicking the Edit button. To configure a new security policy supporting KeyGuard, continue to step 2.

2. Click the Create button to configure a new policy supporting KeyGuard.
   The New Security Policy screen displays with no authentication or encryption options selected.

3. Select the KeyGuard radio button.
   The KeyGuard Settings field displays within the New Security Policy screen.

4. Ensure the Name of the security policy entered suits the intended configuration or function of the policy.

5. Configure the KeyGuard Settings field as required to define the Pass Key used to generate the WEP keys used with the KeyGuard algorithm. These keys must be the same between the AP-5131 and its MU to encrypt packets between the two devices.
Configuring Access Point Security

6-19

Default (hexadecimal) keys for KeyGuard include:

6. Click the Apply button to save any changes made within the KeyGuard Setting field of the New Security Policy screen.

7. Click the Cancel button to undo any changes made within the KeyGuard Setting field and return to the WLAN screen. This reverts all settings to the last saved configuration.

6.8 Configuring WPA Using TKIP

Wi-Fi Protected Access (WPA) is a robust encryption scheme specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

WPA’s encryption method is Temporal Key Integrity Protocol (TKIP). TKIP addresses WEP’s weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector. WPA also provides strong user authentication based on 802.1x EAP.

To configure WPA-TKIP encryption on the AP-5131:
1. Select **Network Configuration** - > **Wireless** - > **Security** from the AP-5131 menu tree. If security policies supporting WPA-TKIP exist, they appear within the **Security Configuration** screen. These existing policies can be used as is, or their properties edited by clicking the **Edit** button. To configure a new security policy supporting WPA-TKIP, continue to step 2.

2. Click the **Create** button to configure a new policy supporting WPA-TKIP. The **New Security Policy** screen displays with no authentication or encryption options selected.

3. Select the **WPA/TKIP** radio button. The **WPA/TKIP Settings** field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.

5. Configure the **Key Rotation Settings** area as needed to broadcast encryption key changes to MUs and define the broadcast interval.
6. Configure the **Key Settings** area as needed to set an ASCII Passphrase and key values.

**Broadcast Key Rotation**

Select the **Broadcast Key Rotation** checkbox to enable or disable the broadcasting of encryption-key changes to MUs. Only broadcast key changes when required by associated MUs to reduce the transmissions of sensitive key information. This value is disabled by default.

**Update broadcast keys every (300-604800 seconds)**

Specify a time period in seconds for broadcasting encryption-key changes to MUs. Set key broadcasts to a shorter time interval (at least 30 seconds) for tighter security on the WLAN’s wireless connections. Set key broadcasts to a longer time interval (at most, 80000 seconds) to extend the key times for wireless connections. Default is 86,400 seconds.

6. **ASCII Passphrase**

To use an ASCII passphrase (and not a hexadecimal value), select the checkbox and enter an alphanumeric string of 8 to 63 characters. The alphanumeric string allows character spaces. The AP-5131 converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

6. **256-bit Key**

To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

Default (hexadecimal) 256-bit keys for WPA/TKIP include:

- 1011121314151617
- 18191A1B1C1D1E1F
- 2021222324252627
- 28292A2B2C2D2E2F

7. Click the **Apply** button to save any changes made within the WPA/TKIP Settings field of the New Security Policy screen.

8. Click the **Cancel** button to undo any changes made within the WPA/TKIP Settings field and return to the **WLAN** screen. This reverts all settings to the last saved configuration.
6.9 Configuring WPA2-CCMP (802.11i)

WPA2 is a newer 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. CCMP is the security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Chaining (CBC) technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a Robust Security Network (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the AP-5131 provides.

To configure WPA2-CCMP on the AP-5131:

1. Select **Network Configuration -> Wireless -> Security** from the AP-5131 menu tree.
   - If security policies supporting WPA2-CCMP exist, they appear within the Security Configuration screen. These existing policies can be used as is, or their properties edited by clicking the Edit button. To configure a new security policy supporting WPA2-CCMP, continue to step 2.

2. Click the **Create** button to configure a new policy supporting WPA2-CCMP.
   - The New Security Policy screen displays with no authentication or encryption options selected.

3. Select the **WPA2/CCMP (802.11i)** checkbox.
   - The WPA2/CCMP Settings field displays within the New Security Policy screen.

4. Ensure the **Name** of the security policy entered suits the intended configuration or function of the policy.
5. Configure the **Key Rotation Settings** field as required to set Broadcast Key Rotation and the update interval.

**Broadcast Key Rotation**
Select the **Broadcast Key Rotation** checkbox to enable or disable the broadcasting of encryption key changes to MUs. Only broadcast key changes when required by associated MUs to reduce the transmissions of sensitive key information. This option is disabled by default.

**Update broadcast keys every (300-604800 seconds)**
Specify a time period in seconds for broadcasting encryption key changes to MUs. Set key broadcasts to a shorter interval (at least 30 seconds) for tighter security on the WLAN’s wireless connections. Set key broadcasts to a longer interval to extend the key times for wireless connections. Default is 86,400 seconds.

6. Configure the **Key Settings** area as needed to set an ASCII Passphrase and 128-bit key.
ASCII Passphrase  To use an ASCII passphrase (and not a hexadecimal value), select the checkbox enter an alphanumeric string of 8 to 63 characters. The string allows character spaces. The AP-5131 converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

256-bit Key  To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

Default (hexadecimal) 256-bit keys for WP2A/CCMP include:
1011121314151617
18191A1B1C1D1E1F
2021222324252627
28292A2B2C2D2E2F

7. Configure the **WPA2-CCMP Mixed Mode** field as needed to allow TKIP and WPA2 client interoperation.

Allow WPA-TKIP clients  WPA2-CCMP Mixed Mode enables WPA2-CCMP and WPA-TKIP clients to operate together on the network. Enabling this option allows backwards compatibility for clients that support WPA-TKIP but do not support WPA2-CCMP. Symbol recommends enabling this feature if WPA-TKIP supported MUs operate within a WLAN populated by WPA2-CCMP enabled clients.

8. Configure the **Fast Roaming (802.1x only)** field as required to enable additional AP-5131 roaming and key caching options. This feature is applicable only when using 802.1x EAP authentication with WPA2/CCMP.

Pre-Authentication  Selecting this option enables an associated MU to carry out an 802.1x authentication with another AP-5131 before it roams to it. The AP-5131 caches the keying information of the client until it roams to the other AP-5131. This enables the roaming client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. This feature is only supported when 802.1x EAP authentication is enabled.

9. Click the **Apply** button to save any changes made within the WPA2/CCMP Settings field of the New Security Policy screen.
10. Click the **Cancel** button to undo any changes made within the WPA2/CCMP Settings field and return to the **WLAN** screen. This reverts all settings to the last saved configuration.

### 6.10 Configuring Firewall Settings

The AP-5131’s firewall is a set of related programs located in the gateway on the WAN side of the AP-5131. The firewall uses a collection of filters to screen information packets for known types of system attacks. Some of the AP-5131’s filters are continuously enabled, others are configurable.

Use the AP-5131’s **Firewall** screen to enable or disable the configurable firewall filters. Enable each filter for maximum security. Disable a filter if the corresponding attack does not seem a threat in order to reduce processor overhead. Use the WLAN Security screens (WEP, Kerberos etc.) as required for setting user authentication and data encryption parameters.

To configure the AP-5131 firewall settings:

1. Select **Network Configuration -> Firewall** from the AP-5131 menu tree.

2. Refer to the **Global Firewall Disable** field to enable or disable the AP-5131 firewall.
3. Refer to the **Timeout Configuration** field to define a timeout interval to terminate IP address translations.

**NAT Timeout**

*Network Address Translation (NAT)* converts an IP address in one network to a different IP address or set of IP addresses in a different network. Set a **NAT Timeout** interval (in minutes) the AP-5131 uses to terminate the IP address translation process if no translation activity is detected after the specified interval.

4. Refer to the **Configurable Firewall Filters** field to set the following firewall filters:

- **Disable Firewall**
  
  Select the **Disable Firewall** checkbox to disable all firewall functions on the AP-5131. This includes firewall filters, NAT, VPN, content filtering, and subnet access. Disabling the AP-5131 firewall makes the AP-5131 vulnerable to data attacks and is not recommended during normal operation if using the WAN port.

- **SYN Flood Attack Check**

  A SYN flood attack requests a connection and then fails to promptly acknowledge a destination host’s response, leaving the destination host vulnerable to a flood of connection requests.

- **Source Routing Check**

  A source routing attack specifies an exact route for a packet’s travel through a network, while exploiting the use of an intermediate host to gain access to a private host.

- **Winnuke Attack Check**

  A “Win-nuking” attack uses the IP address of a destination host to send junk packets to its receiving port.

- **FTP Bounce Attack Check**

  An FTP bounce attack uses the PORT command in FTP mode to gain access to arbitrary ports on machines other than the originating client.

- **IP Unaligned Timestamp Check**

  An IP unaligned timestamp attack uses a frame with the IP timestamp option, where the timestamp is not aligned on a 32-bit boundary.

- **Sequence Number Prediction Check**

  A sequence number prediction attack establishes a three-way TCP connection with a forged source address. The attacker guesses the sequence number of the destination host response.

- **Mime Flood Attack Check**

  A MIME flood attack uses an improperly formatted MIME header in “sendmail” to cause a buffer overflow on the destination host.
Configuring Access Point Security

5. Click **Apply** to save any changes to the Firewall screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Firewall screen to the last saved configuration.

7. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 6.10.1 Configuring LAN to WAN Access

The AP-5131 LAN can be configured to communicate with the WAN side of the AP-5131. Use the **LAN to WAN Access** screen to allow/deny access to the AP-5131 WAN protocols, specify names and properties for existing protocols and enable pre-configured protocols (FTP, TFTP, Telnet etc.).

To configure AP-5131 subnet access:

1. Select **Network Configuration -> Firewall -> LAN to WAN Access** from the AP-5131 menu tree.

---

**Max Header Length**

Use the Max Header Length field to set the maximum allowable header length (at least 256 bytes).

**Max Headers**

Use the Max Headers field to set the maximum number of headers allowed (12)
2. Configure the **LAN to WAN Access** screen as required to allow or deny access to selected (enabled) protocols.

**Allow or Deny all protocols, except**

Use the drop-down menu to select either **Allow** or **Deny**. The selected setting applies to all protocols except those with enabled checkboxes and any traffic that is added to the table. For example, if the adoption rule is to Deny access to all protocols except those listed, access is allowed only to those selected protocols.

**Add**

Click **Add** to create a new table entry.

**Del (Delete)**

Click **Del (Delete)** to remove a selected list entry.

**Name**

Specify a name for a newly configured protocol.

**Transport**

Select a protocol from the drop-down menu. For a detailed description of the protocols available, see *Available Protocols on page 6-30*.

**Start Port**

Enter the starting port number for a range of ports. If the protocol uses a single port, enter that port in this field.
End Port

Enter the ending port number for a port range. If the protocol uses a single port, leave the field blank. A new entry might use Web Traffic for its name, TCP for its protocol, and 80 for its port number.

Pre configured Rules

The following protocols are preconfigured with the AP-5131. To enable a protocol, check the box next to the protocol name.

- **HTTP** - Hypertext Transfer Protocol is the protocol for transferring files on the Web. HTTP is an application protocol running on top of the TCP/IP suite of protocols, the foundation protocols for the Internet. The HTTP protocol uses TCP port 80.

- **TELNET** - TELNET is the terminal emulation protocol of TCP/IP. TELNET uses TCP to achieve a virtual connection between server and client, then negotiates options on both sides of the connection. TELNET uses TCP port 23.

- **FTP** - File Transfer Protocol (FTP) is an application protocol using the Internet’s TCP/IP protocols. FTP provides an efficient way to exchange files between computers on the Internet. FTP uses TCP port 21.

- **SMTP** - Simple Mail Transfer Protocol is a TCP/IP protocol for sending and receiving email. Due to its limited ability to queue messages at the receiving end, SMTP is often used with POP3 or IMAP. SMTP sends the email, and POP3 or IMAP receives the email. SMTP uses TCP port 25.

- **POP** - Post Office Protocol is a TCP/IP protocol intended to permit a workstation to dynamically access a maildrop on a server host. A workstation uses POP3 to retrieve email that the server is holding for it.

- **DNS** - Domain Name Service protocol searches for resources using a database distributed among different name servers.

3. Click **Apply** to save any changes to the LAN to WAN Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

4. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LAN to WAN Access screen to the last saved configuration.

5. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.
6.10.1.1 Available Protocols

Protocols that are not pre-configured can be specified using the drop down list within the Transport column within the LAN to WAN Access and Advanced Subnet Access screens. They include:

- **ALL** - Enables all of the protocol options displayed in the drop-down menu (as described below).
- **TCP** - Transmission Control Protocol is a set of rules for sending data as message units over the Internet. TCP manages individual data packets. Messages are divided into packets for efficient routing through the Internet.
- **UDP** - User Datagram Protocol is used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides few error recovery services. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
- **ICMP** - Internet Control Message Protocol is tightly integrated with IP. ICMP messages are used for out-of-band messages related to network operation. ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.
- **AH** - Authentication Header is one of the two key components of IP Security Protocol (IPsec). The other key component is Encapsulating Security Protocol (ESP). AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
- **ESP** - Encapsulating Security Protocol is one of two key components of IP Security Protocol (IPsec). The other key component is Authentication Header (AH). ESP encrypts the packets and provides authentication services. ESP can be used in transport mode, providing security between two end points. ESP can also be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
- **GRE** - General Routing Encapsulation supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet using globally assigned IP addresses.

6.10.2 Configuring Advanced LAN Access

Use the Advanced LAN Access screen to configure complex access rules and filtering based on source port, destination port, and transport protocol. To enable advanced subnet access, the subnet
access rules must be overridden. However, the Advanced LAN Access screen allows you to import existing subnet access rules into the advanced subnet access rules.

To configure AP-5131 advanced LAN access:

1. Select **Network Configuration** -> **Firewall** -> **Advanced LAN Access** from the AP-5131 menu tree.

2. Configure the **Settings** field as needed to override the settings in the LAN to WAN Access screen and import firewall rules into the Advanced LAN Access screen.

   - **Override LAN to WAN Access settings**
     Select this checkbox to enable advanced subnet access rules and disable existing subnet access rules, port forwarding, and 1 to many mappings from the system. Only enable advanced subnet access rules if your configuration requires rules that cannot be configured within the **LAN to WAN Access** screen.

   - **Import rules from LAN to WAN Access**
     Select this checkbox to import existing access rules (NAT, packet forwarding, VPN rules etc.) into the **Firewall Rules** field. This rule import overrides any existing rules configured in the Advanced Subnet Access screen. A warning box displays stating the operation cannot be undone.
3. Configure the **Firewall Rules** field as required add, insert or delete firewall rules into the list of advanced rules.

**Inbound or Outbound**
Select **Inbound** or **Outbound** from the drop-down menu to specify if a firewall rule is intended for inbound traffic to an interface or outbound traffic from that interface.

**Add**
Click the **Add** button to insert a new rule at the bottom of the table. Click on a row to display a new window with configuration options for that field.

**Insert**
Click the **Insert** button to insert a new rule directly above a selected rule in the table. Clicking on a field in the row displays a new window with configuration options.

**Del (Delete)**
Click **Del** to remove the selected rule from the table. The index numbers for all the rows below the deleted row decrease by 1.

**Move Up**
Clicking the **Move Up** button moves the selected rule up by one row in the table. The index numbers for the affected rows adjust to reflect the new order.

**Move Down**
Clicking the **Move Down** button moves the selected rule down by one row in the table. The index numbers for the affected rows adjust to reflect the new order.

**Index**
The index number determines the order firewall rules are executed. Rules are executed from the lowest number to the highest number.

**Source IP**
The **Source IP** range defines the origin address or address range for the firewall rule. To configure the Source IP range, click on the field. A new window displays for entering the IP address and range.

**Destination IP**
The **Destination IP** range determines the target address or address range for the firewall rule. To configure the Destination IP range, click on the field. A new window displays for entering the IP address and range.

**Transport**
Select a protocol from the drop-down list. For a detailed description of the protocols available, see *Available Protocols on page 6-30.*
4. Click **Apply** to save any changes to the Advanced LAN Access screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Advanced LAN Access screen to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 6.11 Configuring VPN Tunnels

The AP-5131 allows up to 25 VPN tunnels to either a VPN endpoint or to another AP-5131. VPN tunnels allow all traffic on a local subnet to route securely through an IPSEC tunnel to a private network. A VPN port is a virtual port which handles tunneled traffic.

When connecting to another site using a VPN, the traffic is encrypted so if anyone intercepts the traffic, they cannot see what it is unless they can break the encryption. The traffic is encrypted from your computer through the network to the VPN. At that point the traffic is un-encrypted.

Use the **VPN** screen to add and remove VPN tunnels. To configure an existing VPN tunnel, select it from the list in the **VPN Tunnels** field. The selected tunnel’s configuration displays in a **VPN Tunnel Config** field.

To configure a VPN tunnel on the AP-5131:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the AP-5131 menu tree.

<table>
<thead>
<tr>
<th><strong>Src. Ports (Source Ports)</strong></th>
<th>The source port range determines which ports the firewall rule applies to on the source IP address. Click on the field to configure the source port range. A new window displays to enter the starting and ending port ranges. For rules where only a single port is necessary, enter the same port in the start and end port fields.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dst. Ports (Destination Ports)</strong></td>
<td>The destination port range determines which ports the firewall rule applies to on the destination IP address. Click on the field to configure the source port range. A new window displays to enter the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.</td>
</tr>
</tbody>
</table>
2. Use the **VPN Tunnels** field to add or delete a tunnel to the list of available tunnels, list tunnel network address information and display key exchange information for each tunnel.

- **Add**
  
  Click **Add** to add a VPN tunnel to the list. To configure a specific tunnel, select it from the list and use the parameters within the **VPN Tunnel Config** field to set its properties.

- **Del**
  
  Click **Del** to delete a highlighted VPN tunnel. There is no confirmation before deleting the tunnel.

- **Tunnel Name**
  
  The **Tunnel Name** column lists the name of each VPN tunnel on the AP-5131.

- **Remote Subnet**
  
  The **Remote Subnet** column lists the remote subnet mask for each tunnel. The remote subnet mask is the subnet setting for the remote network the tunnel connects to.

- **Remote Gateway**
  
  The **Remote Gateways** column lists a remote gateway IP address for each tunnel. The numeric remote gateway is the gateway IP address on the remote network the VPN tunnel connects to. Ensure the address is the same as the WAN port address of the target gateway AP or switch.
3. If a VPN tunnel has been added to the list of available AP-5131 tunnels, use the VPN Tunnel Config field to optionally modify the tunnel’s properties.

- **Key Exchange Type**: The Key Exchange Type column lists the key exchange type for passing keys between both ends of a VPN tunnel. If Manual Key Exchange is selected, this column displays Manual. If Auto (IKE) Key Exchange is selected, the field displays Automatic.

- **Default Gateway**: Displays the WAN interface’s default gateway IP address.

- **Tunnel Name**: Enter a name to define the VPN tunnel. The tunnel name is used to uniquely identify each tunnel. Select a name best suited to that tunnel’s function so it can be selected again in the future if required in a similar application.

- **Local WAN IP**: Enter the WAN’s numerical (non-DNS) IP address in order for the tunnel to pass traffic to a remote network.

- **Remote Subnet**: Specify the numerical (non-DNS) IP address for the Remote Subnet.

- **Remote Subnet Mask**: Enter the subnet mask for the tunnel’s remote network for the tunnel. The remote subnet mask is the subnet setting for the remote network the tunnel connects to.

- **Remote Gateway**: Enter a numerical (non-DNS) remote gateway IP address for the tunnel. The remote gateway IP address is the gateway address on the remote network the VPN tunnel connects to.

- **Remote Subnet Mask**: Enter a numerical (non-DNS) remote gateway IP address for the tunnel. The remote gateway IP address is the gateway address on the remote network the VPN tunnel connects to.

- **Manual Key Exchange**: Selecting Manual Key Exchange requires you to manually enter keys for AH and or ESP encryption and authentication. Click the Manual Key Settings button to configure the settings.

- **Manual Key Settings**: Select Manual Key Exchange and click the Manual Key Settings button to open a screen where AH authentication and ESP encryption/authentication can be configured and keys entered. For more information, see Configuring Manual Key Settings on page 6-36.
4. Click **Apply** to save any changes to the **VPN** screen as well as changes made to the Auto Key Settings, IKE Settings and Manual Key Settings screens. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

5. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the VPN, Auto Key Settings, IKE Settings and Manual Key Settings screens to the last saved configuration.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 6.11.1 Configuring Manual Key Settings

A transform set is a combination of security protocols and algorithms applied to IPSec protected traffic. During security association (SA) negotiation, both gateways agree to use a particular transform set to protect data flow.

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies the algorithms to use for the selected security protocol. If you specify an ESP protocol in a transform set, specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote end of the gateway.

Use the **Manual Key Settings** screen to specify the transform sets used for VPN access.
To configure manual key settings for the AP-5131:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the AP-5131 menu tree.
2. Refer to the **VPN Tunnel Config** field, select the **Manual Key Exchange** checkbox and click the **Manual Key Settings** button.

3. Configure the **Manual Key Settings** screen to modify the following:

   **AH Authentication**
   
   AH provides data authentication and anti-replay services for the VPN tunnel. Select the required authentication method from the drop-down menu:
   
   - **None** - Disables AH authentication. The rest of the fields are not active.
   - **MD5** - Enables the Message Digest 5 algorithm requiring 128-bit (32-character hexadecimal) keys.
   - **SHA1** - Enables Secure Hash Algorithm 1, requiring 160-bit (40-character hexadecimal) keys.
Inbound AH Authentication Key
Configure a key for computing the integrity check on inbound traffic with the selected authentication algorithm. The key must be 32/40 hexadecimal (0-9, A-E) characters in length. The key value must match the corresponding outbound key on the remote security gateway.

Outbound AH Authentication Key
Configure a key for computing the integrity check on outbound traffic with the selected authentication algorithm. The key must be 32/40 hexadecimal (0-9, A-E) characters in length. The key value must match the corresponding inbound key on the remote security gateway.

Inbound SPI (Hex)
Enter an eight-character hexadecimal value to identify the inbound security association created by the AH algorithm. The value must match the corresponding outbound SPI value configured on the remote security gateway.

Outbound SPI (Hex)
Provide an eight-character hexadecimal value to identify the outbound security association created by the AH algorithm. The value must match the corresponding inbound SPI value configured on the remote security gateway.

ESP Type
ESP provides packet encryption, optional data authentication and anti-replay services for the VPN tunnel. Use the drop-down menu to select the ESP type. Options include:
- None - Disables ESP. The rest of the fields are not be active.
- ESP - Enables ESP for the tunnel.
- ESP with Authentication - Enables ESP with authentication.
Configuring Access Point Security

ESP Encryption Algorithm
Select the encryption and authentication algorithms for the VPN tunnel using the drop-down menu.

- DES - Uses the DES encryption algorithm requiring 64-bit (16-character hexadecimal) keys.
- 3DES - Uses the 3DES encryption algorithm requiring 192-bit (64-character hexadecimal) keys.
- AES 256-bit: - Uses the Advanced Encryption Standard algorithm with 256-bit (64-character hexadecimal) keys.
- Inbound ESP Encryption Key

ESP Authentication Algorithm
Select the authentication algorithm to use with ESP. This option is available only when ESP with Authentication was selected for the ESP type. Options include:

- MD5 - Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) keys.
- SHA1 - Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

Inbound ESP Authentication Key
Define a key for computing the integrity check on the inbound traffic with the selected authentication algorithm. The key must be 32/40 hexadecimal (0-9, A-E) characters in length. The key must match the corresponding outbound key on the remote security gateway.

Outbound ESP Authentication Key
Enter a key for computing the integrity check on outbound traffic with the selected authentication algorithm. The key must be 32/40 hexadecimal (0-9, A-E) characters in length. The key must match the corresponding inbound key on the remote security gateway.
The Inbound and Outbound SPI settings are required to be interpolated to function correctly. For example:

AP1 Inbound SPI = 800
AP1 Outbound SPI = 801
AP2 Inbound SPI = 801
AP2 Outbound SPI = 800

4. Click **Ok** to return to the VPN screen. Click **Apply** to retain the settings made on the Manual Key Settings screen.

5. Click **Cancel** to return to the VPN screen without retaining the changes made to the Manual Key Settings screen.

### 6.11.2 Configuring Auto Key Settings

The AP-5131’s Network Management System can automatically set encryption and authentication keys for VPN access. Use the Auto Key Settings screen to specify the type of encryption and authentication, without specifying the keys. To manually specify keys, cancel out of the Auto Key Settings screen, select the Manual Key Exchange radio button, and set the keys within the Manual Key Setting screen.

To configure auto key settings for the AP-5131:

1. Select **Network Configuration** -&gt; **WAN** -&gt; **VPN** from the AP-5131 menu tree.
2. Refer to the VPN Tunnel Config field, select the Auto (IKE) Key Exchange checkbox and click the Auto Key Settings button.
3. Configure the **Auto Key Settings** screen to modify the following:

**Use Perfect Forward Secrecy**

Forward secrecy is a key-establishment protocol guaranteeing the discovery of a session key or long-term private key does not compromise the keys of other sessions. Select **Yes** to enable Perfect Forward Secrecy. Select **No** to disable Perfect Forward Secrecy.

**AH Authentication**

AH provides data authentication and anti-replay services for the VPN tunnel. Select the desired authentication method from the drop-down menu.

- **None** - Disables AH authentication and the rest of the fields in this area are not active.
- **MD5** - Enables the Message Digest 5 algorithm, requiring 128-bit (32-character hexadecimal) keys.
- **SHA1** - Enables Secure Hash Algorithm 1, requiring 160-bit (40-character hexadecimal) keys.
4. Click **Ok** to return to the VPN screen. Click Apply to retain the settings made on the Auto Key Settings screen.

5. Click **Cancel** to return to the VPN screen without retaining the changes made to this screen.

### 6.11.3 Configuring IKE Key Settings

The Internet Key Exchange (IKE) is an IPsec standard protocol used to ensure security for VPN negotiation and remote host or network access. IKE provides an automatic means of negotiation and authentication for communication between two or more parties. In essence, IKE manages IPsec keys automatically for the parties.
To configure IKE key settings for the AP-5131:

1. Select Network Configuration -> WAN -> VPN from the AP-5131 menu tree.
2. Refer to the VPN Tunnel Config field, select the Auto (IKE) Key Exchange checkbox and click the IKE Settings button.

3. Configure the IKE Key Settings screen to modify the following:

   **Operation Mode**

   The Phase I protocols of IKE are based on the ISAKMP identity-protection and aggressive exchanges. IKE main mode refers to the identity-protection exchange, and IKE aggressive mode refers to the aggressive exchange.

   - **Main** - Standard IKE mode for communication and key exchange.
   - **Aggressive** - Aggressive mode is faster, but less secure than Main mode. Identities are not encrypted unless public key encryption is used. The authentication method cannot be negotiated if the initiator chooses public key encryption.
<table>
<thead>
<tr>
<th><strong>Local ID Type</strong></th>
<th>Select the type of ID to be used for the AP-5131 end of the SA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP</td>
<td>Select IP if the local ID type is the IP address specified as part of the tunnel.</td>
</tr>
<tr>
<td>• FQDN</td>
<td>Use FQDN if the local ID is a fully qualified domain name (such as sj.symbol.com).</td>
</tr>
<tr>
<td>• UFQDN</td>
<td>Select UFQDN if the local ID is a user fully-qualified domain name (such as <a href="mailto:johndoe@symbol.com">johndoe@symbol.com</a>).</td>
</tr>
</tbody>
</table>

| **Local ID Data** | Specify the FQDN or UFQDN based on the Local ID type assigned. |
| **Remote ID Type** | Select the type of ID to be used for the AP-5131 end of the tunnel from the **Remote ID Type** drop-down menu. |
| • IP             | Select the IP option if the local ID type is the IP address specified as part of the tunnel. |
| • FQDN           | Select FQDN if the local ID type is a fully qualified domain name (such as sj.symbol.com). The setting for this field does not have to be fully qualified, however it must match the setting for the Certificate Authority. |
| • UFQDN          | Select this item if the local ID type is a user unqualified domain name (such as johndoe@symbol.com). The setting for this field does not have to be unqualified, it just must match the setting of the field of the Certificate Authority. |

| **Remote ID Data** | If FQDN or UFQDN is selected, specify the data (either the qualified domain name or the user name) in the **Remote ID Data** field. |
| **IKE Authentication Mode** | Select the appropriate IKE authentication mode: |
| • Pre-Shared Key (PSK) | Specify an authenticating algorithm and passcode used during authentication. |
| • RSA Certificates | Select this option to use RSA certificates for authentication purposes. See the CA Certificates and Self certificates screens to create and import certificates into the system. |
| • Digital Signature Standard (DSS) | Select DDS to use DSS certificates as the authentication mode. |
IKE Authentication Algorithm
IKE provides data authentication and anti-replay services for the VPN tunnel. Select an authentication method from the drop-down menu.
- MD5 - Enables the Message Digest 5 algorithm requiring 128-bit (32-character hexadecimal) keys.
- SHA1 - Enables Secure Hash Algorithm 1 requiring 160-bit (40-character hexadecimal) keys.

IKE Authentication Passphrase
If you selected **Pre-Shared Key** as the authentication mode, you must provide a key. If MD5 is the selected authentication algorithm, provide a 32-character hexadecimal key. If SHA1 is the selected algorithm, provide a 40-character hexadecimal key.

IKE Encryption Algorithm
Select the encryption and authentication algorithms for the VPN tunnel from the drop-down menu.
- DES - Uses the DES encryption algorithm requiring 64-bit (16-character hexadecimal) keys.
- 3DES - Enables the 3DES encryption algorithm requiring 192-bit (64-character hexadecimal) keys.
- AES 256-bit - Uses the Advanced Encryption Standard algorithm with 256-bit (64-character hexadecimal) keys.

Key Lifetime
The number of seconds the key is valid. At the end of the lifetime, the key is renegotiated.

The AP-5131 forces renegotiation every 3600 seconds. There is no way to change the renegotiation value. If the IKE Lifetime is greater than 3600, the keys still get renegotiated every 3600 seconds.
Diffie Hellman Group  
Select a Diffie-Hellman Group to use. The Diffie-Hellman key agreement protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Two algorithms exist, one 768-bit and one 1024-bit algorithm. Select one of the following options:

- Group 1 - 768 bit - Somewhat faster than the 1024-bit algorithm, but secure enough in most situations.
- Group 2 - 1024 bit - Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

4. Click Ok to return to the VPN screen. Click Apply to retain the settings made on the IKE Settings screen.

5. Click Cancel to return to the VPN screen without retaining the changes made to the IKE Settings screen.

6.11.4 Viewing VPN Status

Use the VPN Status screen to display the status of the tunnels configured on the AP-5131 as well as their lifetime, transmit and receive statistics. The VPN Status screen is read-only with no configurable parameters. To configure a VPN tunnel, use the VPN configuration screen in the WAN section of the AP-5131 menu tree.

To view VPN status or the AP-5131:

1. Select Network Configuration -> WAN -> VPN -> VPN Status from the AP-5131 menu tree.
2. Reference the Security Associations field to view the following:

- **Tunnel Name**: The Tunnel Name column lists the names of all the tunnels configured on the AP-5131. Clicking the Tunnel Name title bar enables you to sort by tunnel name. For information on configuring a tunnel, see Configuring VPN Tunnels on page 6-33.

- **Status**: The Status column lists the status of each configured tunnel. When the tunnel is not in use, the status reads **NOT_ACTIVE**. When the tunnel is connected, the status reads **ACTIVE**.

- **Outb SPI**: The Outb SPI column displays the outbound Security Parameter Index (SPI) for each tunnel. The SPI is used locally by the AP-5131 to identify a security association. There are unique outbound and inbound SPIs.

- **Inb SPI**: The Inb SPI column displays the inbound SPI Security Parameter Index (SPI) for each of the tunnels. The SPI is used locally by the AP-5131 to identify a security association. There are unique outbound and inbound SPIs.
3. Reference the **IKE Summary** field to view the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Name</strong></td>
<td>Displays the name of each of the tunnels configured to use IKE for automatic key exchange.</td>
</tr>
<tr>
<td><strong>IKE State</strong></td>
<td>Lists the state for each of the tunnels configured to use IKE for automatic key exchange. When the tunnel is not active, the IKE State field displays <strong>NOT_CONNECTED</strong>. When the tunnel is active, the IKE State field displays <strong>CONNECTED</strong>.</td>
</tr>
<tr>
<td><strong>Destination IP</strong></td>
<td>Displays the destination IP address for each tunnel configured to use IKE for automatic key exchange.</td>
</tr>
<tr>
<td><strong>Remaining Life</strong></td>
<td>Lists the remaining life of the current IKE key for each tunnel. When the remaining life on the IKE key reaches 0, IKE initiates a negotiation for a new key. IKE keys associated with a renegotiated tunnel.</td>
</tr>
</tbody>
</table>

4. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 6.12 Configuring Content Filtering Settings

Content filtering allows system administrators to block specific commands and URL extensions from going out through the AP-5131 WAN port. Therefore, content filtering affords system administrators selective control on the content proliferating the network and is a powerful data and network
screening tool. Content filtering allows the blocking of up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

To configure content filtering for the AP-5131:

1. Select **Network Configuration** -> **WAN** -> **Content Filtering** from the AP-5131 menu tree.

2. Configure the **HTTP** field to configure block Web proxies and URL extensions.

   **Block Outbound HTTP**  
   HyperText Transport Protocol (HTTP) is the protocol used to transfer information to and from Web sites. HTTP blocking allows for blocking of specific HTTP commands going outbound on the AP-5131 WAN port. HTTP blocks commands on port 80 only. The Block Outbound HTTP option allows blocking of the following (user selectable) outgoing HTTP requests:
   - Web Proxy: Blocks the use of Web proxies by clients
   - ActiveX: Blocks all outgoing ActiveX requests by clients. Selecting ActiveX only blocks traffic (scripting language) with an .ocx extension.
3. Configure the **SMTP** field to disable or restrict specific kinds of network mail traffic.

**Block Outbound URL Extensions**
Enter a URL extension or file name per line in the format of `filename.ext`. An asterisk (*) can be used as a wildcard in place of the filename to block all files with a specific extension.

**Block Outbound SMTP Commands**

*Simple Mail Transport Protocol (SMTP)* is the Internet standard for host-to-host mail transport. SMTP generally operates over TCP on port 25. SMTP filtering allows the blocking of any or all outgoing SMTP commands. Check the box next to the command to disable that command when using SMTP across the AP-5131’s WAN port.

- **HELO** - *(Hello)* Identifies the SMTP sender to the SMTP receiver.
- **MAIL** - Initiates a mail transaction where data is delivered to one or more mailboxes on the local server.
- **RCPT** - *(Recipient)* Identifies a recipient of mail data.
- **DATA** - Tells the SMTP receiver to treat the following information as mail data from the sender.
- **QUIT** - Tells the receiver to respond with an **OK** reply and terminate communication with the sender.
- **SEND** - Initiates a mail transaction where mail is sent to one or more remote terminals.
- **SAML** - *(Send and Mail)* Initiates a transaction where mail data is sent to one or more local mailboxes and remote terminals.
- **RESET** - Cancels mail transaction and informs the recipient to discard data sent during transaction.
- **VRFY** - Asks receiver to confirm the specified argument identifies a user. If argument does identify a user, the full name and qualified mailbox is returned.
- **EXPN** - *(Expand)* Asks receiver to confirm a specified argument identifies a mailing list. If the argument identifies a list, the membership list of the mailing list is returned.

4. Configure the **FTP** field to block or restrict various FTP traffic on the network.
5. Click **Apply** to save any changes to the Content Filtering screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.

6. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Content Filtering screen to the last saved configuration.

7. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 6.13 Configuring Rogue AP Detection

It is possible that not all of the devices identified by the AP-5131 are operating legitimately within the AP-5131’s radio coverage area. A rogue AP is a device located nearby an authorized Symbol AP-5131 but recognized as having properties rendering its operation illegal and threatening to the AP-5131 and the LAN. Rogue AP detection can be configured independently for both AP-5131 802.11a and 802.11b/g radios (if using a dual radio sku AP-5131). A rogue detection interval is the user-defined interval the AP-5131 waits to search for rogue APs. Additionally, the AP-5131 does not detect rogue APs on illegal channels (channels not allowed by the regulatory requirements of the country the AP-5131 is operating in).
The rogue detection interval is used in conjunction with Symbol MUs that identify themselves as rogue detection capable to the AP-5131. The detection interval defines how often the AP-5131 requests these MUs to scan for a rogue AP. A shorter interval can effect the performance of the MU, but it will also decrease the time it takes for the AP-5131 to scan for a rogue AP. A longer interval will have less of an impact to the MU’s, but it will increase the amount of time used to detect rogue APs. Therefore, the interval should be set according to the perceived risk of rogue devices and the criticality of MU performance.

**CAUTION** Using an antenna other than the Dual-Band Antenna (Part No. ML-2452-APA2-01) could render the AP-5131’s Rogue AP Detector Mode feature inoperable. Contact your Symbol sales associate for specific information.

To configure Rogue AP detection for the AP-5131:

1. Select **Network Configuration -> Wireless -> Rogue AP Detection** from the AP-5131 menu tree.

2. Configure the **Detection Method** field to set the detection method (MU or AP-5131) and define the 802.11a or 802.11b/g radio to conduct the rogue AP search.
3. Use the **Rule Management** field to restrict Symbol AP’s from Rogue AP detection and create a list of device MAC addresses and ESSID’s approved for interoperability with the AP-5131.

- **Authorize Any AP Having Symbol Defined MAC Address**
  Select this checkbox to enable all access points with a Symbol MAC address to interoperate with the AP-5131 conducting a scan for rogue devices.

- **Add**
  Click Add to display a single set of editable MAC address and ESS address values.

- **Delete**
  Click the Delete button to remove the highlighted line from the Rule Management field. The MAC and ESS address information previously defined is no longer applicable unless the previous configuration is restored.

- **Delete All**
  Click the Delete All button to remove all entries from the Rule Management field. All MAC and ESS address information previously defined is no longer applicable unless the previous configuration is restored.

- **Any MAC**
  Select the Any MAC checkbox to prevent a device’s MAC address (whether it is a known device MAC address or not) from being considered a rogue device.
MAC Address  
Click Add, and enter the device MAC address to be excluded from classification as a rogue device.

Any ESSID  
Select the Any ESSID checkbox to prevent a device’s ESSID (whether it is a known device ESSID or not) from being considered a rogue device.

ESSID  
Click Add, and enter the name of a device ESSID to be excluded from classification as a rogue device.

4. Click Apply to save any changes to the Rogue AP Detection screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

5. Click Undo Changes (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Rogue AP Detection screen to the last saved configuration.

6. Click Logout to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.13.1 Moving Rogue APs to the Allowed AP List

The AP-5131 Active APs screen enables the user to view the list of detected rogue APs and, if necessary, select and move an AP into a list of allowed devices. This is helpful when the settings defined within the Rogue AP Detection screen inadvertently detect and define a device as a rogue AP.

To move detected rogue APs into a list of allowed APs:

1. Select Network Configuration -> Wireless -> Rogue AP Detection -> Active APs from the AP-5131 menu tree.
Configuring Access Point Security

The Active APs screen displays with detected rogue devices displayed within the Rogue APs table.

2. Enter a value (in minutes) in the Allowed APs Age Out Time field to indicate the number of elapsed minutes before an AP will be removed from the approved list and reevaluated. A zero (0) for this value (default value) indicates an AP can remain on the approved AP list permanently.

3. Enter a value (in minutes) in the Rogue APs Age Out Time field to indicate the number of elapsed minutes before an AP will be removed from the rogue AP list and reevaluated. A zero (0) for this value (default value) indicates an AP can remain on the rogue AP list permanently.

4. Highlight an AP from within the Rogue APs table and click the Add to Allowed APs List button to move the device into the list of Allowed APs.

5. Click the Add All to Allowed APs List button to move each of the APs displayed within the Rogue APs table to the list of allowed APs.
6. Highlight a rogue AP and click the Details button to display a screen with device and detection information specific to that rogue device. This information is helpful in determining if a rogue AP should be moved to the Allowed APs table.

For more information on the displaying information on detected rogue APs, see Displaying Rogue AP Details on page 6-56.

7. Click Apply to save any changes to the Active APs screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

8. Click Undo Changes (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Active APs screen to the last saved configuration.

9. Click Logout to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

6.13.1.1 Displaying Rogue AP Details

Before moving a rogue AP into the list of allowed APs within the Active APs screen, the device address and rogue detection information for that AP should be evaluated.

To evaluate the properties of a rogue AP:

1. Select Network Configuration -> Wireless -> Rogue AP Detection -> Active APs from the AP-5131 menu tree.

2. Highlight a target rogue AP from within Rogue APs table and click the Details button.
The **Detail** screen displays for the rogue AP:

3. Refer to the **Rogue AP Detail** field for the following information:
   - **BSSID/MAC** Displays the MAC address of the rogue AP. This information could be useful if the MAC address is determined to be a Symbol MAC address and the device is interpreted as non-hostile and the device should be defined as an allowed AP.
   - **ESSID** Displays the ESSID of the rogue AP. This information could be useful if the ESSID is determined to be non-hostile and the device should be defined as an allowed AP.
   - **RSSI** Shows the Relative Signal Strength (RSSI) of the rogue AP. Use this information to assess how close the rogue AP is. The higher the RSSI, the closer the rogue AP. If multiple AP-5131’s have detected the same rogue AP, RSSI can be useful in triangulating the location of the rogue AP.

4. Refer to the **Rogue Detector Detail** field for the following information:
   - **Finder’s MAC** The MAC address of the AP-5131 detecting the rogue AP.
6.13.2 Using MUs to Detect Rogue Devices

The AP-5131 can use an associated MU that has its rogue AP detection feature enabled to scan for rogue APs. Once detected, the rogue AP(s) can be moved to the list of allowed devices (if appropriate) within the Active APs screen. When adding an MU’s detection capabilities with the AP-5131’s own rogue AP detection functionality, the rogue detection area can be significantly extended.

To use associated rogue AP enabled MUs to scan for rogue APs:

1. Select **Network Configuration -> Wireless -> Rogue AP Detection -> MU Scan** from the AP-5131 menu tree.

   The **On Demand MU Scan** screen displays with associated MUs with rogue AP detection enabled.
2. Highlight an MU from within the Rogue AP enabled MUs field and click the scan button. The target MU begins scanning for rogue devices using the detection parameters defined within the Rogue AP Detection screen. To modify the detection parameters, see Configuring Rogue AP Detection on page 6-51.

Those devices detected as rogue APs display within the Scan Result table. Use the displayed AP MAC, ESSID and RSSI values to determine the device listed in the table is truly a rogue device or one inadvertently detected as a rogue AP.

3. If necessary, highlight an individual MU from within the Scan Result field and click the Add to Allowed AP List button to move the AP into the Allowed APs table within the Active APs screen.

4. Additionally, if necessary, click the Add All to Allowed APs List button to move every device within the Scan Result table into the Allowed APs table within the Active APs screen. Only use this option if you are sure all of the devices detected and displayed within the Scan Results table are non-hostile APs.

5. Highlight a different MU from the Rogue AP enabled MUs field as needed to scan for additional rogue APs.
6. Click **Logout** to return to the Rogue AP Detection screen.
The AP-5131 has functionality to display robust transmit and receive statistics for its WAN and LAN port. Wireless Local Area Network (WLAN) stats can also be displayed collectively for each enabled WLAN as well as individually for up to 16 specific WLANs.

Transmit and receive statistics can also be displayed for the AP-5131’s 802.11a and 802.11b/g radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated MU stats can be displayed collectively for associated MUs and individually for specific MUs. An echo (ping) test is also available to ping specific MUs to assess the strength of the AP association.

Finally, the AP-5131 can detect and display the properties of other APs detected within the AP-5131 radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs.

See the following sections for more details on viewing statistics for the AP-5131:

- Viewing WAN Statistics
7.1 Viewing WAN Statistics

Use the AP-5131 **WAN Stats** screen to view real-time statistics for monitoring the AP-5131 activity through its *Wide Area Network (WAN)* port.

The **Information** field of the WAN Stats screen displays basic WAN information, generated from settings on the WAN screen. The **Received** and **Transmitted** fields display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface since it was last enabled or the AP was last rebooted. The AP-5131 **WAN Stats** screen is view-only with no configurable data fields.

To view AP-5131 WAN Statistics:

1. Select **Status and Statistics** -> **WAN Stats** from the AP-5131 menu tree.
2. Refer to the Information field to reference the following AP-5131 WAN data:

**Status**  
The **Status** field displays **Enabled** if the WAN interface is enabled on the **WAN** screen. If the WAN interface is disabled on the WAN screen, the WAN Stats screen displays no connection information and statistics. To enable the WAN connection, see *Configuring WAN Settings on page 5-13*.

**HW Address**  
The **Media Access Control (MAC)** address of the AP-5131 WAN port. The WAN port MAC address is hard coded at the factory and cannot be changed.

**IP Addresses**  
The displayed **Internet Protocol (IP)** addresses for the AP-5131 WAN port.

**Mask**  
The **Mask** field displays the subnet mask number for the AP-5131’s WAN connection. This value is set on the **WAN** screen. Refer to *Configuring WAN Settings on page 5-13* to change the subnet mask.

**Link**  
The **Link** field displays **Up** if the WAN connection is active between the AP-5131 and network, and **Down** if the WAN connection is interrupted or lost. Use this information to assess the current connection status of the WAN port.

**Speed**  
The WAN connection speed is displayed in Megabits per second (Mbps), for example, 54Mbps. If the throughput speed is not achieved, examine the number of transmit and receive errors, or consider increasing the supported data rate. To change the data rate of the 802.11a or 802.11b/g radio, see *Configuring the 802.11a or 802.11b/g Radio on page 5-38*.

3. Refer to the **Received** field to reference data received over the AP-5131 WAN port.

**RX Packets**  
RX packets are data packets received over the WAN port. The displayed number is a cumulative total since the WAN interface was last enabled or the AP-5131 was last restarted.

**RX Bytes**  
RX bytes are bytes of information received over the WAN port. The displayed number is a cumulative total since the WAN interface was last enabled or the AP-5131 was last restarted. To restart the AP-5131 to begin a new data collection, see *Configuring System Settings on page 4-2*. 
4. Refer to the **Transmitted** field to reference data received over the AP-5131 WAN port.

**RX Errors**

RX errors include dropped data packets, buffer overruns, and frame errors on inbound traffic. The number of RX errors is a total of *RX Dropped*, *RX Overruns* and *RX Carrier* errors. Use this information to determine performance quality of the current WAN connection.

**RX Dropped**

The *RX Dropped* field displays the number of data packets that fail to reach the WAN interface. If this number appears excessive, consider a new connection to the device.

**RX Overruns**

RX overruns are buffer overruns on the WAN connection. RX overruns occur when packets are received faster than the WAN port can handle them. If RX overruns are excessive, consider reducing the data rate, for more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-38*.

**RX Frame**

The *RX Frame* field displays the number of TCP/IP data frame errors received.

**TX Packets**

TX packets are data packets sent over the WAN connection. The displayed number is a cumulative total since the WAN interface was last enabled or the AP-5131 was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

**TX Bytes**

TX bytes are bytes of information sent over the WAN connection. The displayed number is a cumulative total since the WAN interface was last enabled or the AP-5131 was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

**TX Errors**

TX errors include dropped data packets, buffer overruns, and carrier errors on outbound traffic. The displayed number of TX errors is the total of *TX Dropped*, *TX Overruns* and *TX Carrier* errors. Use this information to re-assess AP-5131 location and transmit speed.

**TX Dropped**

The *TX Dropped* field displays the number of data packets that fail to get sent from the WAN interface.

**TX Overruns**

TX overruns are buffer overruns on the WAN connection. TX overruns occur when packets are sent faster than the WAN interface can handle. If TX overruns are excessive, consider reducing the data rate, for more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-38*.
5. Click the **Clear WAN Stats** button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared. Do not clear the WAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

6. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 7.2 Viewing LAN Statistics

Use the **LAN Stats** screen to monitor the activity of the AP-5131 LAN connection. The **Information** field of the LAN Stats screen displays network traffic information as monitored over the AP-5131 LAN port. The **Received** and **Transmitted** fields of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted over the LAN port since it was last enabled or the AP-5131 was last restarted. The **LAN Stats** screen is view-only with no user configurable data fields.

To view AP-5131 LAN connection stats:

1. Select **Status and Statistics** -> **LAN Stats** from the AP-5131 menu tree.
2. Refer to the **Information** field to view the following AP-5131 device address information:

   **HW Address**  
   The *Media Access Control (MAC)* address of the AP-5131. The MAC address is hard coded at the factory and cannot be changed.

   **IP Address**  
   The *Internet Protocol (IP)* addresses for the AP-5131 LAN port.

3. Refer to the **Received** field to view data received over the AP-5131 LAN port.

   **RX Packets**  
   RX packets are data packets received over the AP-5131 LAN port. The number is a cumulative total since the LAN connection was last enabled or the AP-5131 was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

   **RX Bytes**  
   RX bytes are bytes of information received over the LAN port. The value is a cumulative total since the LAN connection was last enabled or the AP-5131 was last restarted. To begin a new data collection, see *Configuring System Settings on page 4-2*.

   **RX Errors**  
   RX errors include dropped data packets, buffer overruns, and frame errors on inbound traffic. The number of RX errors is a total of *RX Dropped, RX Overruns* and *RX Carrier* errors. Use this information to determine performance quality of the current LAN connection.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Dropped</td>
<td>The RX Dropped field displays the number of data packets failing to reach the LAN port. If this number appears excessive, consider a new connection to the device.</td>
</tr>
<tr>
<td>RX Overruns</td>
<td>RX overruns are buffer overruns on the AP-5131 LAN port. RX overruns occur when packets are received faster than the LAN connection can handle them. If RX overruns are excessive, consider reducing the data rate, for more information, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.</td>
</tr>
<tr>
<td>RX Frame</td>
<td>The RX Frame field displays the number of TCP/IP data frame errors received.</td>
</tr>
</tbody>
</table>

4. Refer to the Transmitted field to view statistics transmitted over the AP-5131 LAN port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets</td>
<td>TX packets are data packets sent over the AP-5131 LAN port. The displayed number is a cumulative total since the LAN connection was last enabled or the AP-5131 was last restarted. To begin a new data collection, see Configuring System Settings on page 4-2.</td>
</tr>
<tr>
<td>TX Bytes</td>
<td>TX bytes are bytes of information sent over the LAN port. The displayed number is a cumulative total since the LAN Connection was last enabled or the AP-5131 was last restarted. To begin a new data collection, see Configuring System Settings on page 4-2.</td>
</tr>
<tr>
<td>TX Errors</td>
<td>TX errors include dropped data packets, buffer overruns, and carrier errors on outbound traffic. The displayed number of TX errors is a total of TX Dropped, TX Overruns and TX Carrier errors. Use this information to re-assess AP location and transmit speed.</td>
</tr>
<tr>
<td>TX Dropped</td>
<td>The TX Dropped field displays the number of data packets that fail to get sent from the AP-5131 LAN port.</td>
</tr>
<tr>
<td>TX Overruns</td>
<td>TX overruns are buffer overruns on the LAN port. TX overruns occur when packets are sent faster than the LAN connection can handle. If TX overruns are excessive, consider reducing the data rate, for more information, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.</td>
</tr>
<tr>
<td>TX Carrier</td>
<td>The TX Carrier field displays the number of TCP/IP data carrier errors.</td>
</tr>
</tbody>
</table>
5. Click the **Clear LAN Stats** button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared.

6. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet. There will be a prompt confirming logout before the applet is closed.

### 7.3 Viewing Wireless Statistics

Use the **WLAN Stats Summary** screen to view overview statistics for active (enabled) WLANs on the AP-5131. The **WLAN Summary** field displays basic information such as number of Mobile Units (MUs) and total throughput for each of the active WLANs. The **Total RF Traffic** section displays basic throughput information for all RF activity on the AP-5131. The WLAN Stats Summary screen is view-only with no user configurable data fields.

If a WLAN is not displayed within the **Wireless Stats Summary** screen, see *Enabling Wireless LANs (WLANs) on page 5-22* to enable the WLAN. For information on configuring the properties of individual WLANs, see *Creating/Editing Individual WLANs on page 5-24*.

To view AP-5131 WLAN Statistics:

1. Select **Status and Statistics -> Wireless Stats** from the AP-5131 menu tree.
2. Refer to the **WLAN Summary** field to reference high-level data for each enabled WLAN.

   **Name**
   Displays the names of all the enabled WLANs on the AP-5131. For information on enabling a WLAN, see *Enabling Wireless LANs (WLANs)* on page 5-22.

   **MUs**
   Displays the total number of MUs currently associated with each enabled WLAN. Use this information to assess if the MUs are properly grouped by function within each enabled WLAN. To adjust the maximum number of MUs permissible per WLAN, see *Creating/Editing Individual WLANs* on page 5-24.

   **T-put**
   Displays the total throughput in Megabits per second (Mbps) for each active WLAN.

   **ABS**
   Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each active WLAN displayed.

   **% NU**
   Displays a percentage of the total packets for each active WLAN that are non-unicast. Non-unicast packets include broadcast and multicast packets.
3. Refer to the **Total AP RF Traffic** field to view throughput information for the AP-5131 and WLAN.

- **Retries**: Displays the average number of retries per packet. An excessive number could indicate possible network or hardware problems.

- **Clear All WLAN Stats**: Click this button to reset each of the data collection counters to zero in order to begin new data collections.
  - Do not clear the WLAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

4. Click the **Clear RF Stats** button to reset each of the data collection counters to zero in order to begin new data collections.

5. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 7.3.1 Viewing WLAN Statistics

Use the **WLAN Stats** screen to view detailed statistics for individual WLANs. The WLAN Stats screen is separated into four fields; **Information**, **Traffic**, **RF Status**, and **Errors**. The **Information** field displays basic information such as number of associated Mobile Units, ESSID and security...
information. The Traffic field displays statistics on RF traffic and throughput. The RF Status field displays information on RF signal averages from the associated MUs. The Error field displays RF traffic errors based on retries, dropped packets, and undecryptable packets. The WLAN Stats screen is view-only with no user configurable data fields.

To view statistics for an individual WLAN:

1. Select Status and Statistics -> Wireless Stats -> WLANx Stats (x = target WLAN) from the AP-5131 menu tree.

2. Refer to the Information field to view specific WLAN address, MU and security scheme information for the WLAN selected from the AP-5131 menu tree.

**ESSID**
Displays the Extended Service Set ID (ESSID) for the target WLAN.

**Radio/s**
Displays the name of the 802.11a or 802.11b/g radio the target WLAN is using for AP-5131 transmissions.

**Authentication Type**
Displays the authentication type (802.1x EAP or Kerberos) defined for the WLAN. If the authentication type does not match the desired scheme for the WLAN or needs to be enabled, see Enabling Authentication and Encryption Schemes on page 6-5.
3. Refer to the **Traffic** field to view performance and throughput information for the WLAN selected from the AP-5131 menu tree.

- **Encryption Type**
  Displays the encryption method defined for the WLAN. If the encryption type does not match the desired scheme for the WLAN or needs to be enabled, see *Enabling Authentication and Encryption Schemes on page 6-5*.

- **Num. Associated MUs**
  Displays the total number of MUs currently associated with the WLAN. If this number seems excessive, consider segregating MU’s to other WLANs if appropriate.

- **Pkts per second**
  The **Total** column displays the average total packets per second crossing the selected WLAN. The **Rx** column displays the average total packets per second received on the selected WLAN. The **Tx** column displays the average total packets per second sent on the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **Throughput**
  The **Total** column displays average throughput in Mbps for a given time period on the selected WLAN. The **Rx** column displays average throughput in Mbps for packets received on the selected WLAN. The **Tx** column displays average throughput for packets sent on the selected WLAN. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. Use this information to assess whether the current AP-5131 data rate is sufficient to support required network traffic.

- **Avg. Bit Speed**
  The **Total** column displays the average bit speed in Mbps for a given time period on the selected WLAN. This includes all packets that are sent and received. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. If the bit speed is significantly slower than the selected data rate, refer to the **RF Statistics** and **Errors** fields to troubleshoot.

- **% Non-unicast pkt**
  Displays the percentage of the total packets that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.
4. Refer to the **RF Status** field to view the following MU signal, noise and performance information for the WLAN selected from the AP-5131 menu tree.

   * **Avg MU Signal**
     Displays the average RF signal strength in dBm for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour. If the signal is low, consider mapping the MU to a different WLAN if a better functional grouping of MUs can be determined.

   * **Avg MU Noise**
     Displays the average RF noise for all MUs associated with the selected WLAN. The number in black represents MU noise for the last 30 seconds and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the AP-5131, or in area with less conflicting network traffic.

   * **Avg MU SNR**
     Displays the average **Signal to Noise Ratio (SNR)** for all MUs associated with the selected WLAN. The Signal to Noise Ratio is an indicator of overall RF performance on your wireless networks.

5. Refer to the **Errors** field to view MU association error statistics for the WLAN selected from the AP-5131 menu tree.

   * **Avg Num of Retries**
     Displays the average number of retries for all MUs associated with the selected WLAN. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.

   * **Dropped Packets**
     Displays the percentage of packets which the AP gave up on for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

   * **% of Undecryptable Pkts**
     Displays the percentage of undecryptable packets for all MUs associated with the selected WLAN. The number in black represents undecryptable pkts for the last 30 seconds and the number in blue represents undecryptable pkts for the last hour.

**NOTE** The **Apply** and **Undo Changes** buttons are not available on the **WLAN Statistics** screen as this screen is view only with no configurable data fields.
6. Click the **Clear WLAN Stats** button to reset each of the data collection counters to zero in order to begin new data collections.
   Do not clear the WLAN stats if currently in an important data gathering activity or risk losing all data calculations to that point.

7. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 7.4 Viewing Radio Statistics Summary

Select the **Radio Stats Summary** screen to view high-level information (radio name, type, number of associated MUs, etc.) for the radio(s) enabled on an AP-5131. Individual radio statistics can be displayed as well by selecting a specific radio from within the AP-5131 menu tree.

To view high-level AP-5131 radio statistics:

1. Select **Status and Statistics -> Radio Summary** from the AP-5131 menu tree.

2. Refer to the **Radio Summary** field to reference AP-5131 radio information.
3. Click the **Clear All Radio Stats** button to reset each of the data collection counters to zero in order to begin new data collections. Do not clear the radio stats if currently in an important data gathering activity or risk losing all data calculations to that point. For information on viewing radio statistics particular to the AP-5131 radio type displayed within the AP Stats Summary screen, see **Viewing Radio Statistics on page 7-15**.

4. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet.

### 7.4.1 Viewing Radio Statistics

Refer to the **Radio Stats** screen to view detailed information for the AP-5131 radio (either 802.11a or 802.11b/g) displayed within the Radio Summary screen. There are four fields within the screen. The **Information** field displays device address and location information, as well as channel and power information. The **Traffic** field displays statistics for cumulative packets, bytes, and errors received and transmitted. The Traffic field does not add retry information to the stats displayed. Refer to the **RF Status** field for an average MU signal, noise and signal to noise ratio information. Finally, the **Errors** field displays retry information as well as data transmissions the AP-5131 radio either
dropped or could not decrypt. The information within the 802.11a Radio Statistics screen is view-only with no configurable data fields.

To view detailed radio statistics:

1. Select **Status and Statistics -> Radio Summary -> Radio Statistics** from the AP-5131 menu tree.

2. Refer to the **Information** field to view the AP-5131 802.11a or 802.11b/g radio’s MAC address, placement and transmission information.

   **HW Address**
   The Media Access Control (MAC) address of the AP-5131 housing the 802.11a radio. The MAC address is set at the factory and can be found on the bottom of the AP.

   **Radio Type**
   Displays the radio type (either 802.11a or 802.11b/g).

   **Power**
   The power level in milliwatts (mW) for RF signal strength. To change the power setting for the radio, see **Configuring the 802.11a or 802.11b/g Radio** on page 5-38.

   **Adopted by**
   Lists the AP-5131 WLANs adopted by the 802.11a or 802.11b/g radio.
### Monitoring Statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placement</td>
<td>Lists whether the AP-5131 radio is indoors or outdoors. To change the placement setting, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.</td>
</tr>
<tr>
<td>Current Channel</td>
<td>Indicates the channel for communications between the AP-5131 radio and its associated MUs. To change the channel setting, see Configuring the 802.11a or 802.11b/g Radio on page 5-38.</td>
</tr>
<tr>
<td>Num Associated MUs</td>
<td>Lists the number of mobile units (MUs) currently associated with the AP-5131 802.11a or 802.11b/g radio.</td>
</tr>
</tbody>
</table>

3. Refer to the Traffic field to view performance and throughput information for the target AP-5131 802.11a or 802.11b/g radio.

<table>
<thead>
<tr>
<th>Pkts per second</th>
<th>The Total column displays the average total packets per second crossing the radio. The Rx column displays the average total packets per second received. The Tx column displays the average total packets per second transmitted. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>The Total column displays average throughput on the radio. The Rx column displays average throughput in Mbps for packets received. The Tx column displays average throughput for packets transmitted. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour. Use this information to assess whether the current throughput is sufficient to support required network traffic.</td>
</tr>
<tr>
<td>Avg. Bit Speed</td>
<td>The Total column displays the average bit speed in Mbps for the radio. This includes all packets transmitted and received. The number in black represents statistics for the last 30 seconds and the number in blue represents statistics for the last hour.</td>
</tr>
<tr>
<td>Approximate RF Utilization</td>
<td>The approximate RF utilization of the AP-5131 radio. This value is calculated as throughput divided by average bit speed. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</td>
</tr>
<tr>
<td>% Non-unicast pkts</td>
<td>Displays the percentage of total radio packets that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.</td>
</tr>
</tbody>
</table>
4. Refer to the **RF Status** field to view the following MU signal, noise and performance information for the target AP-5131 802.11a or 802.11b/g radio.

   **Avg MU Signal** Displays the average RF signal strength in dBm for all MUs associated with the radio. The number in black represents the average signal for the last 30 seconds and the number in blue represents the average signal for the last hour. If the signal is low, consider mapping the MU to a different WLAN, if a better functional grouping of MUs can be determined.

   **Avg MU Noise** Displays the average RF noise for all MUs associated with the AP-5131 radio. The number in black represents MU noise for the last 30 seconds and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the AP-5131, or in an area with less conflicting network traffic.

   **Avg MU SNR** Displays the average **Signal to Noise Ratio (SNR)** for all MUs associated with the AP-5131 radio. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

5. Refer to the **Errors** field to reference retry information as well as data transmissions the target AP-5131 802.11a or 802.11 b/g radio either gave up on could not decrypt.

   **Avg Num. of Retries** Displays the average number of retries for all MUs associated with the AP-5131 802.11a or 802.11b/g radio. The number in black represents retries for the last 30 seconds and the number in blue represents retries for the last hour.

   **Dropped Packets** Displays the percentage of packets the AP gave up on for all MUs associated with the AP-5131 802.11a or 802.11b/g radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

   **% of Undecryptable Pkts** Displays the percentage of undecryptable packets for all MUs associated with the 802.11a or 802.11b/g radio. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

6. Click the **Clear Radio Stats** button to reset each of the data collection counters to zero in order to begin new data collections.

7. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet.
7.4.1.1 Retry Histogram

Refer to the Retry Histogram screen for an overview of the retries transmitted by an AP-5131 radio and whether those retries contained any data packets. Use this information in combination with the error fields within a Radio Stats screen to assess overall radio performance.

To display a Retry Histogram screen for an AP-5131 radio:


A Radio Histogram screen is available for each AP-5131 radio (regardless of single or dual-radio model).

The table’s first column shows 0 under Retries. The value under the Packets column directly to the right shows the number of packets transmitted by this AP-5131 radio that required 0 retries (delivered on the first attempt). As you go down the table you can see the number of packets requiring 1 retry, 2 retries etc. Use this information to assess whether an abundance of retries warrants reconfiguring the AP-5131 radio to achieve better performance.
2. Click **Apply** to save any changes to the Radio Histogram screen. Navigating away from the screen without clicking Apply results in changes to the screens being lost.

3. Click **Undo Changes** (if necessary) to undo any changes made to the screen. Undo Changes reverts the settings to the last saved configuration.

4. Click **Logout** to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 7.5 Viewing MU Statistics Summary

Use the **MU Stats Summary** screen to display overview statistics for mobile units (MUs) associated with the AP-5131. The **MU List** field displays basic information such as IP Address and total throughput for each associated MU. The MU Stats screen is view-only with no user configurable data fields. However, individual MUs can be selected from within the MU Stats Summary screen to either ping to assess interoperability or display authentication statistics.

To view AP-5131 overview statistics for all of the MUs associated to the AP-5131:

1. Select **Status and Statistics** -> **MU Stats** from the AP-5131 menu tree.
2. Refer to the **MU List** field to reference associated MU address, throughput and retry information.

   - **IP Address**
     - Displays the IP address of each of the associated MU.

   - **MAC Address**
     - Displays the MAC address of each of the associated MU.

   - **WLAN**
     - Displays the WLAN name each MU is interoperating with.

   - **Radio**
     - Displays the name of the 802.11a or 802.11b/g radio each MU is associated with.

   - **T-put**
     - Displays the total throughput in Megabits per second (Mbps) for each associated MU.

   - **ABS**
     - Displays the **Average Bit Speed (ABS)** in Megabits per second (Mbps) for each associated MU.

   - **Retries**
     - Displays the average number of retries per packet. A high number of retries could indicate possible network or hardware problems.

3. Click the **Refresh** button to update the data collections displayed without resetting the data collections to zero.

4. Click the **Echo Test** button to display a screen for verifying the link with an associated MU.
   
   For detailed information on conducting a ping test for an MUs, see *Pinging Individual MUs on page 7-24*.

5. Click the **MU Authentication Statistics** button to display a screen with detailed authentication statistics for the an MU.
   
   For information on individual MU authentication statistics, see *MU Authentication Statistics on page 7-25*.

6. Click the **MU Details** button to display a screen with detailed statistics for a selected MU.
   
   For detailed information on individual MU authentication statistics, see *Viewing MU Details on page 7-22*.

7. Click the **Clear All MU Stats** button to reset each of the data collection counters to zero in order to begin new data collections.

---

**NOTE**

An echo test initiated from the AP-5131 **MU Stats Summary** screen uses WNMP pings. Therefore, target clients that are not Symbol MUs are unable to respond to the echo test.
8. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### 7.5.1 Viewing MU Details

Use the **MU Details** screen to display throughput, signal strength and transmit error information for a specific MU associated with the AP-5131.

The MU Details screen is separated into four fields; **MU Properties**, **MU Traffic**, **MU Signal**, and **MU Errors**. The **MU Properties** field displays basic information such as hardware address, IP address, and associated WLAN and AP. Reference the **MU Traffic** field for MU RF traffic and throughput data. Use the **RF Status** field to reference information on RF signal averages from the target MU. The **Error** field displays RF traffic errors based on retries, dropped packets and undecryptable packets. The MU Details screen is view-only with no user configurable data fields.

To view details specific to an individual MU:

1. Select **Status and Statistics -> MU Stats** from the AP-5131 menu tree.
2. Highlight a specific MU.
3. Select the **MU Details** button.
4. Refer to the **MU Properties** field to view MU address information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>Displays the IP address of the MU.</td>
</tr>
<tr>
<td><strong>WLAN Association</strong></td>
<td>Displays the name of the WLAN the MU is associated with. Use this information to assess whether the MU is properly grouped within that specific WLAN.</td>
</tr>
<tr>
<td><strong>PSP State</strong></td>
<td>Displays the current PSP state of the MU. The <strong>PSP Mode</strong> field has two potential settings. PSP indicates the MU is operating in Power Save Protocol mode. In PSP, the MU runs enough power to check for beacons and is otherwise inactive. CAM indicates the MU is continuously aware of all radio traffic. Symbol recommends CAM for those MUs transmitting with the AP frequently and for periods of time of two hours.</td>
</tr>
<tr>
<td><strong>HW Address</strong></td>
<td>Displays the Media Access Control (MAC) address for the MU.</td>
</tr>
<tr>
<td><strong>Radio Association</strong></td>
<td>Displays the name of the AP MU is currently associated with. If the name of the AP-5131 requires modification, see Configuring System Settings on page 4-2.</td>
</tr>
</tbody>
</table>
5. Refer to the **Traffic** field to view individual MU RF throughput information.

**Packets per second**

The **Total** column displays average total packets per second crossing the MU. The **Rx** column displays the average total packets per second received on the MU. The **Tx** column displays the average total packets per second sent on the MU. The number in black represents Pkts per second for the last 30 seconds and the number in blue represents Pkts per second for the last hour.

**Throughput**

The **Total** column displays the average total packets per second crossing the selected MU. The **Rx** column displays the average total packets per second received on the MU. The **Tx** column displays the average total packets per second sent on the MU. The number in black represents throughput for the last 30 seconds, the number in blue represents throughput for the last hour.

**Avg. Bit Speed**

The **Total** column displays the average bit speed in Mbps for a given time period on the MU. This includes all packets sent and received. The number in black represents average bit speed for the last 30 seconds and the number in blue represents average bit speed for the last hour. Consider increasing the data rate of the AP if the current bit speed does not meet network requirements. For more information, see *Configuring the 802.11a or 802.11b/g Radio on page 5-38*. The associated MU must also be set to the higher rate to interoperate with the AP-5131 at that data rate.

**% of Non-unicast pkts**

Displays the percentage of the total packets for the selected mobile unit that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents packets for the last 30 seconds and the number in blue represents packets for the last hour.

6. Refer to the **RF Status** field to view MU signal and signal disturbance information.
7. Refer to the Errors field to view MU retry information and statistics on packets not transmitted.

- Avg MU Signal: Displays RF signal strength in dBm for the target MU. The number in black represents signal information for the last 30 seconds and the number in blue represents signal information for the last hour.
- Avg MU Noise: Displays RF noise for the target MU. The number in black represents noise for the last 30 seconds, the number in blue represents noise for the last hour.
- Avg MU SNR: Displays the Signal to Noise Ratio (SNR) for the target MU. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.
- Avg Num of Retries: Displays the average number of retries for the MU. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.
- Dropped Packets: Displays the percentage of packets the AP gave up as not received on for the selected MU. The number in black represents the percentage of packets for the last 30 seconds and the number in blue represents the percentage of packets for the last hour.
- % of Undecryptable Pkts: Displays the percentage of undecryptable packets for the MU. The number in black represents the percentage of undecryptable packets for the last 30 seconds and the number in blue represents the percentage of undecryptable packets for the last hour.

8. Click OK to exit the screen.

### 7.5.2 Pinging Individual MUs

The AP-5131 can verify its link with an MU by sending WNMP ping packets to the associated MU. Use the Echo Test screen to specify a target MU and configure the parameters of the ping test.

**NOTE** An echo test initiated from the AP-5131 MU Stats Summary screen uses WNMP pings. Therefore, target clients that are not Symbol MUs are unable to respond to the echo test.
To ping a specific MU to assess its connection with an AP-5131:

1. Select Status and Statistics -> MU Stats from the AP-5131 menu tree.
2. Select the Echo Test button from within the MU Stats Summary screen.
3. Specify the following ping test parameters.
   - Station Address: The IP address of the target MU. Refer to the MU Stats Summary screen for associated MU IP address information.
   - Number of ping: Specify the number of ping packets to transmit to the target MU. The default is 100.
   - Packet Length: Specify the length of each data packet transmitted to the target MU during the ping test. The default is 100 bytes.
   - Packet Data: Defines the data to be transmitted as part of the test.
4. Click the Ping button to begin transmitting ping packets to the station address specified.
   - Refer to the Number of Responses parameter to assess the number of responses from the target MU versus the number of pings transmitted by the AP-5131. Use the ratio of packets sent versus packets received to assess the link quality between MU and the AP-5131.
   - Click the Ok button to exit the Echo Test screen and return to the MU Stats Summary screen.

### 7.5.3 MU Authentication Statistics

The AP-5131 can access and display authentication statistics for individual MUs.

To view AP-5131 authentication statistics for a specific MU:

1. Select Status and Statistics -> MU Stats from the AP-5131 menu tree.
2. Highlight a target MU from within the MU List field.
3. Click the MU Authentication Statistics button.
   - Use the displayed statistics to determine if the target MU would be better served with a different AP-5131 WLAN or AP-5131 radio.
4. Click Ok to return to the MU Stats Summary screen.
7.6 Viewing Known Access Point Statistics

The AP-5131 has the capability of detecting and displaying the properties of other access points (both Symbol and those from other manufacturers) located within its coverage area. Detected AP-5131’s transmit a WNMP message indicating their channel, IP address, firmware version, etc. This information is used to create a known AP list. The list has field indicating the properties of the access point discovered.

To view detected access point statistics:

1. Select Status and Statistics -> Known AP from the AP-5131 menu tree.

The Known AP Statistics screen displays the following information:

- **IP Address**: The network-assigned Internet Protocol address of the located AP.
- **MAC Address**: The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.
- **MUs**: The number MUs associated with the located AP-5131.
2. Click the **Clear Known AP Stats** button to reset each of the data collection counters to zero in order to begin new data collections.

3. Click the **Details** button to display AP address and radio information.

4. Click the **Ping** button to display a screen for verifying the link with a highlighted Symbol access point.

5. Click the **Send Cfg to APs** button to send the your AP-5131’s configuration to other AP-5131’s with same ESSID. Recipient AP-5131 must be the same single or dual-radio model as the AP-5131 sending the configuration. The sending and recipient AP-5131’s must also be running the same major firmware version (i.e., 1.0 to 1.0).

6. Click the **Start Flash** button to flash the LEDs of other AP-5131s detected and displayed within the Known AP Statistics screen.

   Use the **Start Flash** button to determine the location of the devices displayed within the Known AP Statistics screen. When an AP-5131 is highlighted and the Start Flash button is selected, the LEDs on the selected AP-5131 flash. When the **Stop Flash** button is selected, the LEDs on the selected AP-5131 go back to normal operation.

7. Click the **Logout** button to securely exit the AP-5131 Symbol Access Point applet. A prompt displays confirming the logout before the applet is closed.

### **NOTE**

A ping test initiated from the AP-5131 Known AP Statistics screen uses WNMP pings. Therefore, target devices that are not Symbol access points are unable to respond to the ping test.
The AP-5131 Command Line Interface (CLI) is accessed through the serial port or a Telnet session. The AP-5131 CLI follows the same conventions as the Web-based user interface. The CLI does, however, provide an “escape sequence” to provide diagnostics for problem identification and resolution.

The AP-5131 CLI treats the following as invalid characters:

| ' " & , \ ' < > |

In order to avoid problems when using the AP-5131 CLI, these characters should be avoided.

8.1 Connecting to the CLI

8.1.1 Accessing the CLI through the Serial Port

To connect to the AP-5131 CLI through the serial port:

1. Connect one end of a null modem serial cable to the AP-5131’s serial connector.
2. Attach the other end of the null modem serial cable to the serial port of a PC running HyperTerminal or a similar emulation program.
3. Set the HyperTerminal program to use 19200 baud, 8 data bits, 1 stop bit, no parity, no flow control, and auto-detect for terminal emulation.
4. Press <ESC> or <Enter> to enter into the CLI.
5. Enter the default username of admin and the default password of symbol. If this is your first time logging into the AP-5131, you are unable to access any of the AP-5131’s commands until the country code is set. A new password will also need to be created.
**8.1.2 Accessing the CLI via Telnet**

To connect to the AP-5131 CLI through a Telnet connection:

1. Telnet into the AP-5131 using an IP address of 192.168.0.1
2. Enter the default username of **admin** and the default password of **symbol**. If this is your first time logging into the AP-5131, you are unable to access any of the AP-5131’s commands until the country code is set. A new password will also need to be created.
8.2 Admin and Common Commands

AP5131>admin>

Description:
Displays admin configuration options. The items available under this command are shown below.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Accesses admin configuration. This requires an administration login.</td>
</tr>
<tr>
<td>help</td>
<td>Displays general user interface help.</td>
</tr>
<tr>
<td>passwd</td>
<td>Changes the admin password.</td>
</tr>
<tr>
<td>summary</td>
<td>Shows a system summary containing network address information (IP address, network mask, DHCP mode, default gateway and WLAN information) for the AP-5131.</td>
</tr>
<tr>
<td>network</td>
<td>Goes to the network submenu</td>
</tr>
<tr>
<td>system</td>
<td>Goes to the system submenu.</td>
</tr>
<tr>
<td>stats</td>
<td>Goes to the stats submenu.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>
AP5131>admin>

**Description:**
Displays admin configuration options.

**Syntax:**

`admin`  
Accesses admin configuration. Admin configuration requires an administration login.

**Example:**

```
admin>admin

Admin Password:******
```
**AP5131>admin>help**

**Description:**
Displays general CLI user interface help.

**Syntax:**

`help` Displays command line help using combinations of function keys for navigation.

**Example:**

```
admin>help

? : display command help - Eg. ?, show ?, s?
* Restriction of "?": "?" after a function argument is treated as an argument
: Eg. admin<network.lan> set lan enable?
: (Here "?" is an invalid extra argument,
: because it is after the argument
: "enable")

<ctrl-q> : go backwards in command history
<ctrl-p> : go forwards in command history

* Note : 1) commands can be incomplete
: - Eg. sh = sho = show
: 2) "//" introduces a comment and gets no response from CLI.
```

admin>
AP5131>admin>passwd

Description:
Changes the password for the admin login.

Syntax:

```
passwd
```

Changes the admin password for AP-5131 access. This requires typing the old admin password and entering a new password and confirming it. Passwords can be up to 11 characters. The AP-5131 CLI treats the following as invalid characters:

```
| " & , \ ' < >
```

In order to avoid problems when using the AP-5131 CLI, these characters should be avoided.

Example:

```
admin>passwd

Old Admin Password:******
New Admin Password:******
Verify Admin Password:******
```

For information on configuring passwords using the applet (GUI), see Setting Passwords on page 6-3.
AP5131>admin>summary

Description:
Displays the AP-5131’s system summary.

Syntax:

```
summary
```

Displays a summary of high-level characteristics and settings for the WAN, LAN and WLAN.

Example:

```
admin>summary
```

```
AP-5131 firmware version 1.0.0.0-xxx
country code us
serial number 00A0F8716A74
```

<table>
<thead>
<tr>
<th>WLAN Name</th>
<th>ESSID</th>
<th>Radio</th>
<th>VLAN</th>
<th>Security Policy</th>
<th>QOS Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lobby</td>
<td>101</td>
<td>11a</td>
<td>2</td>
<td>Open</td>
<td>Voice</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Interface</th>
<th>IP Address</th>
<th>Network Mask</th>
<th>LAN DHCP Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WAN Interface</th>
<th>IP Address</th>
<th>Network Mask</th>
<th>LAN Default Gateway</th>
<th>DHCP Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>157.235.91.63</td>
<td>255.255.255.0</td>
<td>157.235.91.2</td>
<td>enable</td>
</tr>
</tbody>
</table>

For information on displaying a system summary using the applet (GUI), see Basic Device Configuration on page 3-3.
AP5131>admin>..

Description:
Displays the parent menu of the current menu.

This command appears in all of the submenus under admin. In each case, it has the same function, to move up one level in the directory structure.

Example:

admin(network.lan)>..
admin(network)>
admin(network)>
**AP5131>admin> /**

**Description:**
Displays the root menu, that is, the top-level CLI menu.

This command appears in all of the submenus under admin. In each case, it has the same function, to move up to the top level in the directory structure.

**Example:**
```
admin(network.lan)>/
admin>
```
**AP5131>admin>save**

**Description:**
Saves the configuration to system flash.

The save command appears in all of the submenus under admin. In each case, it has the same function, to save the current configuration.

**Syntax:**

```
save
```

Saves configuration settings. The save command works at all levels of the CLI. The save command must be issued before leaving the CLI for updated settings to be retained.

**Example:**

```
admin>save
admin>
```
**AP5131>admin>quit**

**Description:**

Exits the command line interface session and terminates the session.

The quit command appears in all of the submenus under admin. In each case, it has the same function, to exit out of the CLI. Once the quit command is executed, the login prompt displays again.

**Example:**

```
admin>quit
```
8.3 Network Commands

AP5131>admin(network)>

Description:
Displays the network submenu. The items available under this command are shown below.

- **lan**: Goes to the LAN submenu.
- **wan**: Goes to the WAN submenu.
- **wireless**: Goes to the Wireless Configuration submenu.
- **firewall**: Goes to the firewall submenu.
- **router**: Goes to the router submenu.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the current configuration to the system flash.
- **quit**: Quits the CLI and exits the current session.
8.3.1 Network LAN Commands

AP5131>admin(network.lan)>

Description:
Displays the LAN submenu. The items available under this command are shown below.

- **show** Shows current AP-5131 LAN port parameters.
- **set** Sets LAN parameters.
- **vlan** Defines LAN VLAN configuration values.
- **dhcp** Goes to the LAN DHCP submenu.
- **type-filter** Goes to the type-filter submenu to specify data types allowed or denied access to the AP-5131 WLAN traffic
- .. Goes to the parent menu.
- / Goes to the root menu.
- **save** Saves the configuration to system flash.
- **quit** Quits the CLI.

For an overview of the AP-5131’s LAN configuration options using the applet (GUI), see Configuring the LAN Interface on page 5-1.
AP5131>admin(network.lan)> show

**Description:**
Displays the AP-5131 LAN settings.

**Syntax:**

*show*  Shows the settings for the AP-5131 LAN interface.

**Example:**

```
admin(network.lan)> show

LAN Interface : enable
LAN Timeout   : 45 sec.
802.11q Trunking : disable

802.1x Port Authentication:
  Username      : admin
  Password      : ********

LAN IP mode   : DHCP server
IP Address    : 192.168.0.1
Network Mask  : 255.255.255.255
Default Gateway: 192.168.0.1
Domain Name   :
Primary DNS Server : 192.168.0.1
Secondary DNS Server : 192.168.0.2
WINS Server   : 192.168.0.254

admin(network.lan)> 
```

For information on displaying LAN information using the applet (GUI), see *Configuring the LAN Interface on page 5-1.*
**AP5131>admin(network.lan)> set**

**Description:**
Sets the LAN parameters for the LAN port.

**Syntax:**

- `set lan <mode>`: Enables or disables the AP-5131 LAN interface.
- `timeout <seconds>`: Sets the interval (in seconds) the AP-5131 uses to terminate its LAN interface if no activity is detected for the specified interval.
- `trunking <mode>`: Enables or disables 802.11q Trunking over the AP-5131 LAN port.
- `username <name>`: Specifies the user name for 802.1x port authentication over the LAN interface.
- `password <password>`: The 0-32 character password for the username for the 802.1x port.
- `ip-mode <ip>`: Defines the AP-5131 LAN port IP mode.
- `ipadr <ip>`: Sets the IP address used by the LAN port.
- `mask <ip>`: Defines the IP address used for AP-5131 LAN port network mask.
- `dgw <ip>`: Sets the Gateway IP address used by the LAN port.
- `domain <name>`: Specifies the domain name used by the AP-5131 LAN port.
- `dns <ip>`: Defines the IP address of the primary and secondary DNS servers used by the LAN port.
- `wins <ip>`: Defines the IP address of the WINS server used by the LAN port.

**Example:**

```
admin(network.lan)>

admin(network.lan)>set lan enable
admin(network.lan)>set timeout 45
admin(network.lan)>set trunking disable
admin(network.lan)>set dns 1 192.168.0.1
admin(network.lan)>set dns 2 192.168.0.2
admin(network.lan)>set wins 192.168.0.254
admin(network.lan)>set trunking disable
admin(network.lan)>set username phil
admin(network.lan)>set password ea0258c1
```

**Related Commands:**

- `show`  Shows the current settings for the AP-5131 LAN port.

For information on configuring the AP-5131 LAN using the applet (GUI), see *Configuring the LAN Interface on page 5-1*. 
8.3.1.1 Network LAN, VLAN Commands

AP5131>admin(network.lan.vlan)>

Description:
Displays the AP-5131 VLAN submenu.

show          Displays the VLAN list currently defined for the AP-5131.
set           Sets the AP-5131 VLAN configuration.
create        Creates a new AP-5131 VLAN.
edit          Edits the properties of an existing AP-5131 VLAN.
delete        Deletes a VLAN.
mapping       Maps AP-5131 WLANs to VLANs.
..            Moves to the parent menu.
/             Goes to the root menu.
save          Saves the configuration to system flash.
quit          Quits the CLI and exits the session.

For an overview of the AP-5131’s VLAN configuration options using the applet (GUI), see Configuring VLAN Support on page 5-5.
**AP5131>admin(network.lan.vlan)> show**

**Description:**
Displays current VLAN parameter settings the AP-5131. These parameters are defined with the set command.

**Syntax:**
- `show name` Displays the existing list of AP-5131 VLAN names.
- `show config` Shows the target VLAN configuration.
- `show wlan` Displays the WLAN summary list.

**Example:**
```
admin(network.lan.vlan)> show name

<table>
<thead>
<tr>
<th>Index</th>
<th>VLAN ID</th>
<th>VLAN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>VLAN_1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>VLAN_2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>VLAN_3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>VLAN_4</td>
</tr>
</tbody>
</table>
```

```
admin(network.lan.vlan)> show config

Management VLAN Tag : 1
Native VLAN Tag : 2
WLAN : Lobby
mapped to VLAN : VLAN 2
VLAN Mode : static
```

```
admin(network.lan.vlan)> show wlan

<table>
<thead>
<tr>
<th>WLAN Name</th>
<th>ESSID</th>
<th>Radio</th>
<th>VLAN</th>
<th>Security Policy</th>
<th>QOS Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lobby</td>
<td>101</td>
<td>11a</td>
<td>2</td>
<td>Open</td>
<td>Voice</td>
</tr>
</tbody>
</table>
```

For information on displaying the AP-5131 VLAN screens using the applet (GUI), see [Configuring VLAN Support on page 5-5](#).
AP5131>admin(network.lan.vlan)> set

Description:
Sets VLAN parameters for the AP-5131.

Syntax:
```
set mgmt-tag <id>     Defines the Management VLAN tag (1-4095).
native-tag <id>       Sets the Native VLAN tag (1-4095).
mode <id>             Sets WLAN VLAN mode (WLAN 1-16) to either dynamic or static.
```

Example:
```
admin(network.lan.vlan)>set mgmt-tag 1
admin(network.lan.vlan)>set native-tag 1

admin(network.lan.vlan)>show config

Management VLAN Tag  :1
Native VLAN Tag       :2
WLAN                  :Lobby
mapped to VLAN       :2
VLAN Mode             :static
```

For information on configuring VLANs using the applet (GUI), see Configuring VLAN Support on page 5-5.
**AP5131>admin(network.lan.vlan)> create**

**Description:**
Creates a VLAN for the AP-5131.

**Syntax:**
```
create vlan-id <id>    Defines the VLAN ID (1-4095).
vlan-name <name>      Specifies the name of the VLAN (1-31 characters in length).
```

**Example:**
```
admin(network.lan.vlan)>
admin(network.lan.vlan)>create 5 VLAN-5
```

For information on creating VLANs using the applet (GUI), see Configuring VLAN Support on page 5-5.
AP5131>admin(network.lan.vlan)> edit

Description:
Modifies a VLAN's name and ID.

Syntax:
edit name <name> Modifies an existing VLAN name (1-31 characters in length)
id <id> Modifies an existing VLAN ID (1-4095) characters in length).

For information on editing VLANs using the applet (GUI), see Configuring VLAN Support on page 5-5.
AP5131>admin(network.lan.vlan)> delete

**Description:**

Deletes a specific VLAN or all VLANs.

**Syntax:**

- `delete <VLANid>` Deletes a specific VLAN ID (1-16).
- `all` Deletes all defined VLANs.

For information on deleting VLANs using the applet (GUI), see *Configuring VLAN Support on page 5-5.*
**AP5131>admin(network.lan.vlan)> mapping**

**Description:**
Maps an AP-5131 VLAN to a WLAN.

**Syntax:**

```
wlan <wlan name> <vlan name>
```
Maps an AP-5131 WLAN to an existing VLAN name, and maps an AP-5131 VLAN to an existing WLAN name. All names and IDs are case-sensitive.

For information on mapping VLANs using the applet (GUI), see *Configuring VLAN Support on page 5-5.*
8.3.1.2 Network LAN, DHCP Commands

AP5131>admin(network.lan.dhcp)>

Description:
Displays the AP-5131 DHCP submenu. The items available are displayed below.

- **show**: Displays DHCP parameters.
- **set**: Sets DHCP parameters.
- **add**: Adds static DHCP address assignments.
- **delete**: Deletes static DHCP address assignments.
- **list**: Lists static DHCP address assignments.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI and exits the session.
AP5131>admin(network.lan.dhcp)> show

**Description:**
Shows DHCP parameter settings.

**Syntax:**

```
show
```

Displays DHCP parameter settings for the AP-5131. These parameters are defined with the set command.

**Example:**

```
admin(network.lan.dhcp)> show

DHCP Address Assignment Range:
  Starting IP Address : 192.168.0.100
  Ending IP Address   : 192.168.0.254
  Lease Time          : 86400
```

For information on configuring DHCP using the applet (GUI), see *Configuring the LAN Interface on page 5-1*. 
**AP5131>admin(network.lan.dhcp)> set**

**Description:**
Sets DHCP parameters for the LAN port.

**Syntax:**

```
set range <ip1> <ip2>  Sets the DHCP assignment range from IP address <ip1> to IP address <ip2>.
lease <lease>       Sets the DHCP lease time <lease> in seconds (1-999999).
```

**Example:**

```
admin(network.lan.dhcp)>set range 192.168.0.100 192.168.0.254
admin(network.lan.dhcp)>set lease 86400

admin(network.lan.dhcp)>show
DHCP Address Assignment Range:
  Starting IP Address : 192.168.0.100
  Ending IP Address   : 192.168.0.254
  Lease Time          : 86400
```

For information on configuring DHCP using the applet (GUI), see *Configuring the LAN Interface on page 5-1*. 


**AP5131**>admin(network.lan.dhcp)> add

**Description:**

Adds static DHCP address assignments.

**Syntax:**

```
add <mac> <ip>  Adds a reserved static IP address to a MAC address.
```

**Example:**

```
admin(network.lan.dhcp)>add 00A0F8112233 192.160.24.6
admin(network.lan.dhcp)>add 00A0F1112234 192.169.24.7
admin(network.lan.dhcp)>list
```

<table>
<thead>
<tr>
<th>Index</th>
<th>MAC Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00A0F8112233</td>
<td>192.160.24.6</td>
</tr>
<tr>
<td>2</td>
<td>00A0F8112234</td>
<td>192.169.24.7</td>
</tr>
</tbody>
</table>

For information on adding client MAC and IP address information using the applet (GUI), see Configuring Advanced DHCP Server Settings on page 5-10.
**AP5131>admin(network.lan.dhcp)> delete**

**Description:**
Deletes static DHCP address assignments.

**Syntax:**
```
delete <idx> <entry> Deletes the static DHCP address entry <entry>.
<idx> all Deletes all static DHCP addresses.
```

**Example:**
```
admin(network.lan.dhcp)>list

------------------------------------------------------------------------------
Index   MAC Address     IP Address
------------------------------------------------------------------------------
1 00A0F8112233  10.1.2.4
2 00A0F8102030  10.10.1.2
3 00A0F8112234  10.1.2.3
4 00A0F8112235  192.160.24.6
5 00A0F8112236  192.169.24.7

admin(network.lan.dhcp)>delete 1

------------------------------------------------------------------------------
index   mac address     ip address
------------------------------------------------------------------------------
1 00A0F8102030  10.10.1.2
2 00A0F8112234  10.1.2.3
3 00A0F8112235  192.160.24.6
4 00A0F8112236  192.169.24.7

admin(network.lan.dhcp)>delete all

------------------------------------------------------------------------------
index   mac address     ip address
------------------------------------------------------------------------------
```

For information on deleting client MAC and IP address information using the applet (GUI), see *Configuring Advanced DHCP Server Settings on page 5-10.*
AP5131>admin(network.lan.dhcp)> list

Description:
Lists static DHCP address assignments.

Syntax:
list <idx> Lists the static DHCP address assignments.

Example:
admin(network.lan.dhcp)> list

-------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Index</th>
<th>MAC Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00A0F8112233</td>
<td>10.1.2.4</td>
</tr>
<tr>
<td>2</td>
<td>00A0F8102030</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>3</td>
<td>00A0F8112234</td>
<td>10.1.2.3</td>
</tr>
<tr>
<td>4</td>
<td>00A0F8112235</td>
<td>192.160.24.6</td>
</tr>
<tr>
<td>5</td>
<td>00A0F8112236</td>
<td>192.169.24.7</td>
</tr>
</tbody>
</table>

admin(network.lan.dhcp)>

For information on listing client MAC and IP address information using the applet (GUI), see Configuring Advanced DHCP Server Settings on page 5-10.
8.3.1.3 Network Type Filter Commands

AP5131>admin(network.lan.type-filter)>

Description:
Displays the AP-5131 Type Filter submenu. The items available under this command include:

- **show**: Displays the current Ethernet Type exception list.
- **set**: Defines Ethernet Type Filter parameters.
- **add**: Adds an Ethernet Type Filter entry.
- **delete**: Removes an Ethernet Type Filter entry.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
AP5131>admin(network.lan.type-filter)> show

Description:
Displays the AP-5131’s current Ethernet Type Filter configuration.

Syntax:
show Displays the existing AP-5131 Type-Filter configuration.

Example:

admin(network.lan.type-filter)> show

Ethernet Type Filter mode : allow

index ethernet type
-----------------------------------------------
1 8137

For information on displaying the AP-5131’s type filter configuration using the applet (GUI), see Setting the Type Filter Configuration on page 5-11.
**AP5131>admin(network.lan.type-filter)> set**

**Description:**
Defines the AP-5131 Ethernet Type Filter configuration.

**Syntax:**

```
set mode allow or deny
```

Allows or denies the AP-5131 from processing a specified Ethernet data type.

**Example:**

```
admin(network.lan.type-filter)>set mode allow
```

For information on configuring the AP-5131’s type filter settings using the applet (GUI), see *Setting the Type Filter Configuration on page 5-11.*
**AP5131>admin(network.lan.type-filter)> add**

**Description:**

Adds an Ethernet Type Filter entry.

**Syntax:**

```
add <type>
```

Adds entered Ethernet Type to list of data types either allowed or denied AP-5131 processing permissions.

**Example:**

```
admin(network.lan.type-filter)>

admin(network.wireless.type-filter)>add 2 8137
admin(network.wireless.type-filter)>add 3 0806
admin(network.wireless.type-filter)>add 4 0800
admin(network.wireless.type-filter)>add 5 8782
admin(network.wireless.type-filter)>show
```

<table>
<thead>
<tr>
<th>index</th>
<th>ethernet type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8137</td>
</tr>
<tr>
<td>2</td>
<td>0806</td>
</tr>
<tr>
<td>3</td>
<td>0800</td>
</tr>
<tr>
<td>4</td>
<td>8782</td>
</tr>
</tbody>
</table>

Ethernet Type Filter mode : allow

For information on configuring the AP-5131’s type filter settings using the applet (GUI), see *Setting the Type Filter Configuration on page 5-11.*
AP5131> admin(network.lan.type-filter)> delete

Description:
Removes an Ethernet Type Filter entry individually or the entire Type Filter list.

Syntax:

```
delete <index>   Deletes the specified Ethernet Type index entry (1 through 16).
    all          Deletes all Ethernet Type entries currently in list.
```

Example:

```
admin(network.lan.type-filter)> delete 1
admin(network.lan.type-filter)> show

Ethernet Type Filter mode : allow
-----------------------------------------------
index      ethernet type
-----------------------------------------------
1          0806
2          0800
3          8782

admin(network.lan.type-filter)> delete all
admin(network.lan.type-filter)> show

Ethernet Type Filter mode : allow
-----------------------------------------------
index      ethernet type
-----------------------------------------------
```

For information on configuring the AP-5131’s type filter settings using the applet (GUI), see Setting the Type Filter Configuration on page 5-11.
8.3.2 Network WAN Commands

AP5131>admin(network.wan)>

Description:
Displays the WAN submenu. The items available under this command are shown below.

- **show**: Displays the AP-5131 WAN configuration and the AP-5131’s current PPPoE configuration.
- **set**: Defines the AP-5131’s WAN and PPPoE configuration.
- **nat**: Displays the NAT submenu, wherein Network Address Translations (NAT) can be defined.
- **vpn**: Goes to the VPN submenu, where the AP-5131 VPN tunnel configuration can be set.
- **app**: Displays the Outbound Content Filtering submenu, where data types can be included/excluded from AP-5131 throughput.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the current configuration to the AP-5131 system flash.
- **quit**: Quits the CLI and exits the current session.

For an overview of the AP-5131’s WAN configuration options using the applet (GUI), see *Configuring WAN Settings on page 5-13*. 
AP5131>admin(network.wan)> show

Description:
Displays the AP-5131 WAN port parameters.

Syntax:

show   Shows the general IP parameters for the WAN port along with settings for the WAN interface.

Example:

```
admin(network.wan)>show

WAN Interface : enable
WAN DHCP Client Mode : disable
IP address : 0.0.0.0
Network Mask : 0.0.0.0
Default Gateway : 10.10.1.1
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0
WAN IP 2 : disable
WAN IP 3 : disable
WAN IP 4 : disable
WAN IP 5 : disable
WAN IP 6 : disable
WAN IP 7 : disable
WAN IP 8 : disable
PPPoE Mode : enable
PPPoE User Name : JohnDoe
PPPoE Password : *******
PPPoE keepalive mode : enable
PPPoE Idle Time : 600
PPPoE Authentication Type : chap
```

For an overview of the AP-5131 WAN configuration options available using the applet (GUI), see Configuring WAN Settings on page 5-13.
AP5131>admin(network.wan)> set

Description:
Defines the configuration of the AP-5131 WAN port.

Syntax:

```
set wan enable/disable
set dhcp enable/disable
set ipadr <indx> <a.b.c.d>
set mask <a.b.c.d>
set dgw <a.b.c.d>
set dns <indx> <a.b.c.d>
set pppoe mode enable/disable
```

Enables or disables the AP-5131 WAN port.
Enables or disables WAN DHCP Client mode.
Sets up to 8 (using <indx> from 1 to 8) IP addresses <a.b.c.d> for the AP-5131 WAN interface.
Sets the subnet mask for the AP-5131 WAN interface.
Sets the default gateway IP address to <a.b.c.d>.
Sets the IP address of one or two DNS servers, where <indx> indicates either the primary (1) or secondary (2) server, and <a.b.c.d> is the IP address of the server.
Enables or disables PPPoE.

Example:

```
admin(network.wan)>
admin(network.wan)>set dhcp disable
admin(network.wan)>set ipadr 157.169.22.5
admin(network.wan)>set dgw 157.169.22.1
admin(network.wan)>set dns 1 157.169.22.2
admin(network.wan)>set mask 255.255.255.000
admin(network.wan)>set pppoe mode enable
admin(network.wan)>set pppoe type chap
admin(network.wan)>set pppoe user JohnDoe
admin(network.wan)>set pppoe passwd @#$goodpassword%$#
admin(network.wan)>set pppoe ka enable
admin(network.wan)>set pppoe idle 600
```

For an overview of the AP-5131 WAN configuration options available using the applet (GUI), see Configuring WAN Settings on page 5-13.
8.3.2.1 Network WAN NAT Commands

AP5131>admin(network.wan.nat)>

Description:
Displays the NAT submenu. The items available under this command are shown below.

show  Displays the AP-5131’s current NAT parameters for the specified index.
set   Defines the AP-5131 NAT settings.
add   Adds NAT entries.
delete Deletes NAT entries.
list  Lists NAT entries.
..    Goes to the parent menu.
/     Goes to the root menu.
save  Saves the configuration to system flash.
quit  Quits the CLI.

For an overview of the AP-5131 NAT configuration options available using the applet (GUI), see Configuring Network Address Translation (NAT) Settings on page 5-18.
AP5131>admin(network.wan.nat)> show

Description:
Displays AP-5131 NAT parameters.

Syntax:

show <idx>       Displays AP-5131 NAT parameters for the specified NAT index.

Example:

    admin(network.wan.nat)> show 2

    WAN IP Mode                     : disable
    WAN IP Address                  : 157.235.91.2
    NAT Type                        : 1-to-many
    1 to 1 Outbound Mappings        : 0.0.0.0
    Inbound Mappings                : Port Forwarding

    unspecified port forwarding mode : enable
    unspecified port fwd. ip address : 111.223.222.1

    admin(network.wan.nat)>

For an overview of the AP-5131 NAT options available using the applet (GUI), see Configuring Network Address Translation (NAT) Settings on page 5-18.
**AP5131>admin(network.wan.nat)> set**

**Description:**
Sets NAT inbound and outbound parameters.

**Syntax:**

- `set type <index> <type>` Sets the type of NAT translation for WAN address index `<idx>` (1-8) to `<type>` (none, 1-to-1, or 1-to-many).
- `ip <index> <ip>` Sets NAT IP mapping associated with WAN address `<idx>` to the specified IP address `<ip>`.
- `mode <index> enable/disable` Enable or disable the AP-5131’s Unspecified Port Forwarding mode for the designated NAT index.
- `unspec-ip <index> <ip>` Forward unspecified ports for the defined NAT index to the defined IP address.

**Example:**

```
admin(network.wan.nat)> set type 1-to-1
admin(network.wan.nat)> set ip 157.235.91.2
admin(network.wan.nat)> set mode 2 disable
admin(network.wan.nat)> set unspec-ip 2 111.223.222.1
```

```
admin(network.wan.nat)> show 2

WAN IP Mode : disable
WAN IP Address : 157.235.91.2
NAT Type : 1-to-many
1 to 1 Outbound Mappings : LAN
Inbound Mappings : Port Forwarding

unspecified port forwarding mode : disable
unspecified port fwd. ip address : 111.223.222.1
```

For an overview of the AP-5131 NAT options available using the applet (GUI), see *Configuring Network Address Translation (NAT) Settings* on page 5-18.
**AP5131>admin(network.wan.nat)> add**

**Description:**
Adds NAT entries.

**Syntax:**

```
add <idx> <name> <tran> <port1> <port2> <ip> <dst_port>
```

Sets an inbound network address translation (NAT) for WAN address `<idx>`, where `<name>` is the name of the entry (1 to 7 characters), `<tran>` is the transport protocol (one of `tcp`, `udp`, `icmp`, `ah`, `esp`, `gre`, or `all`), `<port1>` is the starting port number in a port range, `<port2>` is the ending port number in a port range, `<ip>` is the internal IP address, and `<dst_port>` is the (optional) internal translation port.

**Example:**

```
admin(network.wan.nat)>add 1 indoors udp 20 29 10.10.2.2
```

```
admin(network.wan.nat)>list 1
```

```
---------------------------------------------------------------------
index  name  prot  start port  end port  internal ip  translation port
---------------------------------------------------------------------
 1  indoor  udp   20      29  10.10.2.2   0

**Related Commands:**

- **delete** Deletes one of the inbound NAT entries from the list.
- **list** Displays the list of inbound NAT entries.

For an overview of the AP-5131 NAT options available using the applet (GUI), see *Configuring Network Address Translation (NAT) Settings on page 5-18.*
**AP5131>admin(network.wan.nat)> delete**

**Description:**
Deletes NAT entries.

**Syntax:**

`delete <idx> <entry>` Deletes a specified NAT index entry `<entry>` associated with the WAN.

`<idx> all` Deletes all NAT entries associated with the WAN.

**Example:**

```
admin(network.wan.nat)> list 1

-------------------------------------------------------------------------------
index  name  prot  start port  end port  internal ip  translation port
-------------------------------------------------------------------------------
1  special  tcp  20  21  192.168.42.16  21

admin(network.wan.nat)> delete all
^  
admin(network.wan.nat)> list 1

-------------------------------------------------------------------------------
index  name  prot  start port  end port  internal ip  translation port
-------------------------------------------------------------------------------
```

**Related Commands:**

- **add** Adds entries to the list of inbound NAT entries.
- **list** Displays the list of inbound NAT entries.

For an overview of the AP-5131 NAT options available using the applet (GUI), see *Configuring Network Address Translation (NAT) Settings* on page 5-18.
AP5131>admin(network.wan.nat)> list

Description:
Lists AP-5131 NAT entries for the specified index.

Syntax:
list <idx> Lists the inbound NAT entries associated with WAN port.

Example:

admin(network.wan.nat)>list 1

-----------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>index</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
<th>internal ip</th>
<th>translation port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>special</td>
<td>tcp</td>
<td>20</td>
<td>21</td>
<td>192.168.42.16</td>
<td>21</td>
</tr>
</tbody>
</table>

Related Commands:

delete  Deletes inbound NAT entries from the list.
add  Adds entries to the list of inbound NAT entries.

For an overview of the AP-5131 NAT options available using the applet (GUI), see Configuring Network Address Translation (NAT) Settings on page 5-18.
8.3.2.2 Network WAN, VLAN Commands

AP5131>admin(network.wan.vpn)>

Description:
Displays the VPN submenu. The items available under this command include:

- **add**: Adds VPN tunnel entries.
- **set**: Sets key exchange parameters.
- **delete**: Deletes VPN tunnel entries.
- **list**: Lists VPN tunnel entries
- **reset**: Resets all VPN tunnels.
- **stats**: Lists security association status for the VPN tunnels.
- **ikestate**: Displays an Internet Key Exchange (IKE) summary.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.

For an overview of the AP-5131 VPN options available using the applet (GUI), see Configuring VPN Tunnels on page 6-33.
AP5131>admin(network.wan.vpn)> add

Description:
Adds a VPN tunnel entry.

Syntax:
```
add <name> <LWanIP> <RSubnetIP> <RSubnetMask> <RGatewayIP>
```

Creates a tunnel <name> (1 to 13 characters) to gain access through local WAN IP <LWanIP> from the remote subnet with address <RSubnetIP> and subnet mask <RSubnetMask> using the remote gateway <RGatewayIP>.

Example:
```
admin(network.wan.vpn)> add SJSharkey 209.235.44.31 206.107.22.46 255.255.255.224 206.107.22.1

If tunnel type is Manual, proper SPI values and Keys must be configured after adding the tunnel
```

```
admin(network.wan.vpn)> list

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Type</th>
<th>Remote IP/Mask</th>
<th>Remote Gateway</th>
<th>Local WAN IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SJSharkey</td>
<td>Manual</td>
<td>206.107.22.46/27</td>
<td>255.255.255.224</td>
<td>209.235.44.31</td>
</tr>
</tbody>
</table>
```

For information on configuring VPN using the applet (GUI), see Configuring VPN Tunnels on page 6-33.
AP5131>admin(network.wan.vpn)> set

Description:
Sets VPN entry parameters.

Syntax:

```
set type <name> <tunnel type>
authalgo <name> <authalgo>
authkey <name> <dir> <authkey>
esp-type <name> <esptype>
esp-encalgo <name> <escalgo>
esp-enckey <name> <dir> <enckey>
esp-authalgo <name> <authalgo>
esp-authkey <name> <dir> <authkey>
spi <name> <algo> <dir> <value>
usepfs <name> <mode>
```

- **set type**
  - Sets the tunnel type `<name>` to **Auto** or **Manual** for the specified tunnel name.

- **authalgo**
  - Sets the authentication algorithm for `<name>` to **(None, MD5, or SHA1)**.

- **authkey**
  - Sets the AH authentication key (if type is Manual) for tunnel `<name>` with the direction set to **IN** or **OUT**, and the manual authentication key set to `<authkey>`. (The key size is **32** hex characters for MD5, and **40** hex characters for SHA1).

- **esp-type**
  - Sets the Encapsulating Security Payload (ESP) type. Options include **None**, **ESP**, or **ESP-AUTH**.

- **esp-encalgo**
  - Sets the ESP encryption algorithm. Options include **DES, 3DES, AES128, AES192,** or **AES256**.

- **esp-enckey**
  - Sets the Manual Encryption Key in ASCII for tunnel `<name>` and direction **IN** or **OUT** to the key `<esc-key>`. The size of the key depends on the encryption algorithm:
    - **16** hex characters for DES
    - **48** hex characters for 3DES
    - **32** hex characters for AES128
    - **48** hex characters for AES192
    - **64** hex characters for AES256

- **esp-authalgo**
  - Sets the ESP authentication algorithm. Options include **MD5** or **SHA1**.

- **esp-authkey**
  - Sets ESP Authentication key `<name>` either for **IN** or **OUT** direction to `<auth-key>`, an ASCII string of hex characters. If authalgo is set to **MD5**, the provide 32 hex characters. If authalgo is set to **SHA1**, provide 40 hex characters.

- **spi**
  - Sets **IN**(bound) or **OUT**(bound) for **AUTH** (Manual Authentication) or **ESP** for `<name>` to `<spi>` (a hex value more than 0xFF) `<value>`.

- **usepfs**
  - Enables or disables Perfect Forward Secrecy for `<name>`.
salife <name> <lifetime> Defines the name of the tunnel <name> the Security Association Life Time <300-65535> applies to in seconds.

ike opmode <name> <opmode> Sets the Operation Mode of IKE for <name> to Main or Aggressive.

myidtype <name> <idtype> Sets the Local ID type for IKE authentication for <name> (1 to 13 characters) to <idtype> (IP, FQDN, or UFQDN).

remidtype <name> <idtype> Sets the Remote ID type for IKE authentication for <name> (1 to 13 characters) to <idtype> (IP, FQDN, or UFQDN).

myiddata <name> <idtype> Sets the Local ID data for IKE authentication for <name> to <idtype>. This value is not required when the ID type is set to IP.

remiddata <name> <idtype> Sets the Local ID data for IKE authentication for <name> to <idtype>. This value is not required when the ID type is set to IP.

authtype <name> <authtype> Sets the IKE Authentication type for <name> to <authtype> (one of PSK, RSA, or DSS).

authalgo <name> <authalgo> Sets the IKE Authentication Algorithm for <name> to MD5 or SHA1.

phrase <name> <phrase> Sets the IKE Authentication passphrases for <name> to <phrase>.

encalgo <name> <encalgo> Sets the IKE Encryption Algorithm for <name> to <encalgo> (one of DES, 3DES, AES128, AES192, or AES256).

lifetime <name> <lifetime> Sets the IKE Key lifetime in seconds for <name> to <lifetime>.

group <name> <group> Sets the IKE Diffie-Hellman Group for <name> to either G768 or G1024.

For information on configuring VPN using the applet (GUI), see Configuring VPN Tunnels on page 6-33.
AP5131>admin(network.wan.vpn)> delete

**Description:**

Deletes VPN tunnel entries.

**Syntax:**

```
delete  *          Deletes all VPN entries.
<name>      Deletes VPN entries <name>.
```

**Example:**

```
admin(network.wan.vpn)>list

+-----------------+--------+-----------------+-----------------+-------------------+
| Tunnel Name     | Type   | Remote IP/Mask  | Remote Gateway  | Local WAN IP      |
|-----------------+--------+-----------------+-----------------+-------------------+

admin(network.wan.vpn)>delete Eng2EngAnnex

admin(network.wan.vpn)>list

+-----------------+--------+-----------------+-----------------+-------------------+
| Tunnel Name     | Type   | Remote IP/Mask  | Remote Gateway  | Local WAN IP      |
|-----------------+--------+-----------------+-----------------+-------------------+

admin(network.wan.vpn)>
```

For information on configuring VPN using the applet (GUI), see *Configuring VPN Tunnels on page 6-33.*
**AP5131>admin(network.wan.vpn)> list**

**Description:**
Lists VPN tunnel entries.

**Syntax:**

```
list               Lists all tunnel entries.
<name>            Lists detailed information about tunnel named <name>. Note that the <name> must match case with the name of the VPN tunnel entry
```

**Example:**

```
admin(network.wan.vpn)>list

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Type</th>
<th>Remote IP/Mask</th>
<th>Remote Gateway</th>
<th>Local WAN IP</th>
</tr>
</thead>
</table>
```

```
admin(network.wan.vpn)>list SJSharkey

Detail listing of VPN entry:

<table>
<thead>
<tr>
<th>Name</th>
<th>SJSharkey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Subnet</td>
<td>1</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>Manual</td>
</tr>
<tr>
<td>Remote IP</td>
<td>206.107.22.45</td>
</tr>
<tr>
<td>Remote IP Mask</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>Remote Security Gateway</td>
<td>206.107.22.2</td>
</tr>
<tr>
<td>Local Security Gateway</td>
<td>209.239.160.55</td>
</tr>
<tr>
<td>AH Algorithm</td>
<td>None</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>ESP</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>DES</td>
</tr>
<tr>
<td>ESP Inbound SPI</td>
<td>0x000000100</td>
</tr>
<tr>
<td>ESP Outbound SPI</td>
<td>0x000000100</td>
</tr>
</tbody>
</table>
```

For information on displaying VPN information using the applet (GUI), see [Viewing VPN Status on page 6-46](#).
**AP5131>admin(network.wan.vpn)> reset**

**Description:**
Resets all of the AP-5131’s VPN tunnels.

**Syntax:**
```
reset
```
Resets all VPN tunnels.

**Example:**
```
admin(network.wan.vpn)> reset

VPN tunnels reset.

admin(network.wan.vpn)> 
```

For information on configuring VPN using the applet (GUI), see *Configuring VPN Tunnels on page 6-33*. 
AP5131>admin(network.wan.vpn)> stats

**Description:**
Lists statistics for all active tunnels.

**Syntax:**

```
stats
```

Display statistics for all VPN tunnels.

**Example:**
```
admin(network.wan.vpn)>stats
-------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Status</th>
<th>SPI(OUT/IN)</th>
<th>Life Time</th>
<th>Bytes(Tx/Rx)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eng2EngAnnex</td>
<td>Not Active</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SJSharkey</td>
<td>Not Active</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
-------------------------------------------------------------------------------
```

For information on displaying VPN information using the applet (GUI), see *Viewing VPN Status on page 6-46*. 
**AP5131>admin(network.wan.vpn)> ikestate**

**Description:**
Displays statistics for all active tunnels using Internet Key Exchange (IKE).

**Syntax:**
ikestate

Displays status about Internet Key Exchange (IKE) for all tunnels. In particular, the table indicates whether IKE is connected for any of the tunnels, it provides the destination IP address, and the remaining lifetime of the IKE key.

**Example:**

```
admin(network.wan.vpn)> ikestate
-----------------------------------------------------------------------
Tunnel Name  IKE State  Dest IP  Remaining Life
-----------------------------------------------------------------------
Eng2EngAnnex  Not Connected  ----  ---
SJSharkey    Not Connected  ----  ---
-----------------------------------------------------------------------
admin(network.wan.vpn)> 
```

For information on configuring IKE using the applet (GUI), see *Configuring IKE Key Settings on page 6-42*. 
### 8.3.2.3 Network WAN App Commands

**AP5131>admin(network.wan.app)>**

**Description:**
Displays the outbound content filtering submenu. The items available under this command are shown below.

- **addcmd**: Adds app control commands to the deny list.
- **delcmd**: Deletes app control commands from the deny list.
- **list**: Lists app control entries.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
AP5131>admin(network.wan.app)> addcmd

Description:
Adds app control commands to the deny list.

Syntax:
```
addcmd  web  file  <filename>.<ext>
```
Denies specified web file name. `<filename>` can be up to 15 characters and `*` can be used to match any string. `<ext>` can be up to 10 characters (such as htm, html, or java). Up to 10 files can be specified.

```
proxy
activex
ftp  put
get
ls
mkdir
cd
pasv
smtp  helo
mail
rcpt
data
quit
send
saml
reset
vrfy
expn
```
Denies web proxies.
Denies ActiveX files.
Adds put command to the deny list.
Adds get command to the deny list.
Adds list directory command to the deny list.
Adds make directory command to the deny list.
Adds connect directory command to the deny list.
Adds passive mode command to the deny list.
Adds helo SMTP command to the deny list.
Adds mail SMTP command to the deny list.
Adds rcpt SMTP command to the deny list.
Adds data SMTP command to the deny list.
Adds quit SMTP command to the deny list.
Adds send SMTP command to the deny list.
Adds saml SMTP command to the deny list.
Adds reset SMTP command to the deny list.
Adds vrfy SMTP command to the deny list.
Adds expn SMTP command to the deny list.

For information on configuring Content Filtering using the applet (GUI), see Configuring Content Filtering Settings on page 6-48.
**AP5131>admin(network.wan.app)> delcmd**

**Description:**
Deletes application control commands from the deny list.

**Syntax:**

```
delcmd web file <filename><ext>
```

- **proxy**
  - Allows web proxies.
- **activex**
  - Allows ActiveX files.
- **ftp put**
  - Deletes put command from the deny list.
- **get**
  - Deletes get command from the deny list.
- **ls**
  - Deletes list directory command from the deny list.
- **mkdir**
  - Deletes make directory command from the deny list.
- **cd**
  - Deletes connect directory command from the deny list.
- **pasv**
  - Deletes passive mode command from the deny list.
- **smtp helo**
  - Deletes helo SMTP command from the deny list.
- **mail**
  - Deletes mail SMTP command from the deny list.
- **rcpt**
  - Deletes rcpt SMTP command from the deny list.
- **data**
  - Deletes data SMTP command from the deny list.
- **quit**
  - Deletes quit SMTP command from the deny list.
- **send**
  - Deletes send SMTP command from the deny list.
- **saml**
  - Deletes saml SMTP command from the deny list.
- **reset**
  - Deletes reset SMTP command from the deny list.
- **vrfy**
  - Deletes vrfy SMTP command from the deny list.
- **expn**
  - Deletes expn SMTP command from the deny list.

*<filename>* can be up to 15 characters and **{*}** can be used to match any string. *<ext>* can be up to 10 characters (such as htm, html, or java). Up to 10 files can be specified.

For information on configuring Content Filtering using the applet (GUI), see *Configuring Content Filtering Settings on page 6-48.*
AP5131>admin(network.wan.app)> list

Description:
Lists the app control records.

Syntax:

```
list web     Lists Web/HTTP app control settings.
ftp          Lists FTP app control settings.
smtp         Lists SMTP app control record.
```

Example:

```
admin(network.wan.app)>list web

HTTP Files/Commands

  Web Proxy    : deny
  ActiveX      : deny
  filename     :

admin(network.wan.app)>list ftp

FTP Commands

  Storing Files   : allow
  Retrieving Files: allow
  Directory List  : allow
  Create Directory: deny
  Change Directory: deny
  Passive Operation: deny

admin(network.wan.app)>list smtp

SMTP Commands

  HELO          : deny
  MAIL          : allow
  RCPT          : allow
  DATA          : allow
  QUIT          : allow
  SEND          : allow
  SAML          : allow
  RESET         : allow
  VRFY          : deny
  EXPN          : allow
```

For information on configuring Content Filtering using the applet (GUI), see Configuring Content Filtering Settings on page 6-48.
8.3.3 Network Wireless Commands

AP5131>admin(network.wireless)

Description:
Displays the AP-5131 wireless submenu. The items available under this command include:

- **wlan**: Displays the WLAN submenu used to create and configure up to 16 WLANs per AP-5131.
- **security**: Displays the security submenu used to create encryption and authentication based security policies for use with AP-5131 WLANs.
- **acl**: Displays to the Access Control List (ACL) submenu to restrict or allow MU access to AP-5131 WLANs.
- **radio**: Displays the radio configuration submenu used to specify how the 802.11a or 802.11b/g radio is used with specific WLANs.
- **qos**: Displays the Quality of Service (QoS) submenu to prioritize specific kinds of data traffic within a WLAN.
- **bandwidth**: Displays the Bandwidth Management submenu used to configure the order data is processed by an AP-5131 radio.
- **rogue-ap**: Displays the Rogue-AP submenu to configure devices located by the AP-5131 as friendly or threatening for interoperability.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
8.3.3.1 Network WLAN Commands

AP5131>admin(network.wireless.wlan)>

Description:
Displays the AP-5131 wireless LAN (WLAN) submenu. The items available under this command include:

- show: Displays the AP-5131’s current WLAN configuration.
- create: Defines the parameters of a new WLAN.
- edit: Modifies the properties of an existing WLAN.
- delete: Deletes an existing WLAN.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
- save: Saves the configuration to system flash.
- quit: Quits the CLI.

For an overview of the Wireless configuration options available to the AP-5131 using the applet (GUI), see Enabling Wireless LANs (WLANs) on page 5-22.
**AP5131>admin(network.wireless.wlan)> show**

**Description:**
Displays the AP-5131’s current WLAN configuration.

**Syntax:**
- `show`                  Displays the current configuration for existing WLANs.
- `wlan <number>`        Displays the configuration for the requested WLAN (WLAN 1 through 16).

**Example:**
```
admin(network.wireless.wlan)> show wlan 1
```

ESS Identifier : 101
WLAN Name : Lobby
802.11a Radio : available
802.11b/g Radio : not available
Maximum MUs : 127
Security Policy : Default
MU Access Control : Default
Kerberos User Name : Default
Kerberos Password : *******
Disallow MU to MU Communication : disable
Use Secure Beacon : disable
Accept Broadcast ESSID : disable
QoS Policy : Default

For information on displaying WLAN information using the applet (GUI), see *Enabling Wireless LANs (WLANs) on page 5-22*. 
AP5131>admin(network.wireless.wlan)> create

**Description:**
Defines the parameters of a new AP-5131 WLAN.

**Syntax:**
```
create set ess <essid>  Defines the ESSID for a target WLAN.
wlan-name <name> Determines the name of this particular WLAN (1-32).
11a <mode> Enables or disables access to the AP-5131 802.11a radio.
11bg <mode> Enables or disables access to the AP-5131 802.11b/g radio.
max-mu <number> Defines the maximum number of MU able to operate within the WLAN (default = 127 MUs).
security <name> Sets the security policy to the WLAN (1-32).
acl <name> Sets the MU ACL policy to the WLAN (1-32).
passwd <ascii string> Defines a Kerberos password used if the WLAN's security policy uses a Kerberos server-based authentication scheme.
no-mu-mu <mode> Enables or disables MUs associated to the same WLAN to not communicate with each other.
sbeacon <mode> Enables or disables the AP-5131 from transmitting the ESSID in the beacon.
bcast <mode> Enables or disables the AP-5131 from accepting broadcast IDs from MUs. Broadcast IDs are transmitted without security.
qos <name> Defines the index name representing the QoS policy used with this WLAN.
```

**Example:**
```
admin(network.wireless.wlan.create)>show wlan
```

```
ESS Identifier : 101
WLAN Name     : WLAN1
802.11a Radio  : available
802.11b/g Radio: not available
Maximum MUs    : 127
Security Policy: Default
MU Access Control: Default
Kerberos User Name: Default
Kerberos Password: *********
Disallow MU to MU Communication: disable
Use Secure Beacon: disable
Accept Broadcast ESSID: disable
QoS Policy: Default
```
admin(network.wireless.wlan.create)>show security

<table>
<thead>
<tr>
<th>Secu Policy Name</th>
<th>Authen</th>
<th>Encryption</th>
<th>Associated WLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Default</td>
<td>Manual</td>
<td>no encrypt</td>
<td>Front Lobby</td>
</tr>
<tr>
<td>2 WEP Demo</td>
<td>Manual</td>
<td>WEP 64</td>
<td>2nd Floor</td>
</tr>
<tr>
<td>3 Open</td>
<td>Manual</td>
<td>no encrypt</td>
<td>1st Floor</td>
</tr>
</tbody>
</table>

admin(network.wireless.wlan.create)>show acl

<table>
<thead>
<tr>
<th>ACL Policy Name</th>
<th>Associated WLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Default</td>
<td>Front Lobby</td>
</tr>
<tr>
<td>2 Admin</td>
<td>3rd Floor</td>
</tr>
<tr>
<td>3 Demo Room</td>
<td>5th Floor</td>
</tr>
</tbody>
</table>

admin(network.wireless.wlan.create)>show qos

<table>
<thead>
<tr>
<th>QOS Policy Name</th>
<th>Associated WLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Default</td>
<td>Front Lobby</td>
</tr>
<tr>
<td>2 Voice</td>
<td>Audio Dept</td>
</tr>
<tr>
<td>3 Video</td>
<td>Video Dept</td>
</tr>
</tbody>
</table>

For information on creating a WLAN using the applet (GUI), see Creating/Editing Individual WLANs on page 5-24.
AP5131>admin(network.wireless.wlan)> edit

Description:
Edits the properties of an existing WLAN policy.

Syntax:
edit <index> Edits the properties of an existing WLAN policy.

For information on editing a WLAN using the applet (GUI), see Creating/Editing Individual WLANs on page 5-24.
8.3.3.2 Network Security Commands

AP5131>admin(network.wireless.security)>

Description:
Displays the AP-5131 wireless security submenu. The items available under this command include:

- **show**: Displays the AP-5131’s current security configuration.
- **create**: Defines the parameters of a security policy.
- **edit**: Edits the properties of an existing security policy.
- **delete**: Removes a specific security policy.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.

For information the security configuration options available to the AP-5131 using the applet (GUI), see Configuring Security Options on page 6-2.
**AP5131>admin(network.wireless.security)> show**

**Description:**
Displays the AP-5131's current security configuration.

**Syntax:**
```
show summary
policy <id>   Displays list of existing security policies (1-16).
             Displays the specified security policy <id>.
```

**Example:**
```
admin(network.wireless.security)> show summary

Secu Policy Name  Authen  Encryption  Associated WLANs
------------------------------------------------------------------
   1 Default    Manual  no encrypt   Lobby
   2 WEP Demo    Manual  WEP 64      2nd Floor
   3 Open       Manual  no encrypt   1st Floor

admin(network.wireless.security)> show policy 1

Security Policy 1
Policy Name : Default
Authentication : Manual Pre-shared key/No Authentication

Encryption type : no encryption
```

**Related Commands:**
```
create       Defines security parameters for the specified WLAN.
```

For information displaying existing WLAN security settings using the applet (GUI), see *Enabling Authentication and Encryption Schemes on page 6-5.*
AP5131>admin(network.wireless.security)> create

Description:
Defines the parameter of AP-5131 security policies.
### Syntax:

**create**

Defines the parameters of a security policy.

**show**

Displays new or existing security policy parameters.

**set sec-name <name>**

Sets the name of the security policy.

**auth <authtype>**

Sets the authentication type for WLAN <idx> to <type> (none, eap, or kerberos).

*Note: Kerberos parameters are only in affect if "kerberos" is specified for the authentication method (set auth <type>).*

**kerb realm <name>**

Sets the Kerberos realm.

**server <sidx> <ip>**

Sets the Kerberos server <sidx> (1-primary, 2-backup, or 3-remote) to KDC IP address.

**port <sidx> <port>**

Sets the Kerberos port to <port> (KDC port) for server <ksidx> (1-primary, 2-backup, or 3-remote).

*Note: EAP parameters are only in affect if "eap" is specified for the authentication method (set auth <type>).*

**eap server <sidx> <ip>**

Sets the radius server (1-primary or as 2-secondary) IP address <ip>.

**port <sidx> <port>**

Sets the radius server <sidx> (1-primary or 2-secondary) <port> (1-65535).

**secret <sidx> <secret>**

Sets the EAP shared secret <secret> (1-63 characters) for server <sidx> (1-primary or 2-secondary).

**reauth mode <mode>**

Enables or disables EAP reauthentication.

**period <time>**

Sets the reauthentication period <period> in seconds (30-9999).
retry <number> Sets the maximum number of reauthentication retries <retry> (1-99).

accounting mode <mode> Enable or disable Radius accounting.

timeout <period> Defines MU timeout period in seconds (1-255).

retry <number> Sets the maximum number of MU retries to <retry> (1-10).

syslog <mode> Enable or disable syslog messages.

ip <ip> Defines syslog server IP address.

adv mu-quiet <time> Set the EAP MU/supplicant quiet period to <time> seconds (1-65535).

mu-timeout <timeout> Sets the EAP MU/supplicant timeout in seconds (1-255).

mu-tx <time> Sets the EAP MU/supplicant TX period <time> in seconds (1-65535).

mu-retry <count> Sets the EAP maximum number of MU retries to <count> (1-10).

svr-timeout <time> Sets the server timeout <time> in seconds (1-255).

svr-retry <count> Sets the maximum number of server retries to <count> (1-255).

Note: The WEP authentication mechanism saves up to four different keys (one for each WLAN). It is not requirement to set all keys, but you must associate a WLAN with the same keys.

enc <idx> <type> Sets the encryption type to <type> (one of none, wep40, wep104, keyguard, tkip, or ccmp) for WLAN <idx>.

wep-keyguard passkey The passkey used as a text abbreviation for the entire key length (4-32).
index <key index> Selects the WEP/KeyGuard key (from one of the four potential values of <key index> (1-4).

hex-key <kidx> <key string> Sets the WEP/KeyGuard key for key index <kidx> (1-4) for WLAN <kidx> to <key string>.

ascii-key <kidx> <key string> Sets the WEP/KeyGuard key for key index <kidx> (1-4) for WLAN <kidx> to <key string>.

Note: TKIP parameters are only affected if "tkip" is selected as the encryption type.

tkip rotate-mode <mode> Enables or disabled the broadcast key.

interval <time> Sets the broadcast key rotation interval to <time> in seconds (300-604800).

type <key type> Sets the TKIP key type.

key <256 bit key> Sets the TKIP key to <256 bit key>.

phrase <ascii phrase> Sets the TKIP ASCII pass phrase to <ascii phrase> (8-63 characters).

ccmp rotate-mode <mode> Enables or disabled the broadcast key.

interval <time> Sets the broadcast key rotation interval to <time> in seconds (300-604800).

type <key type> Sets the CCMP key type.

key <256 bit key> Sets the CCMP key to <256 bit key>.

phrase <ascii phrase> Sets the CCMP ASCII pass phrase to <ascii phrase> (8-63 characters).

mixed-mode <mode> Enables or disables mixed mode (allowing WPA-TKIP clients).

preauth <mode> Enables or disables preauthentication (fast roaming).
For information on configuring the encryption and authentication options available to the AP-5131 using the applet (GUI), see Configuring Security Options on page 6-2.
**AP5131>admin(network.wireless.security.edit)>**

**Description:**
Edits the properties of a specific security policy.

**Syntax:**

- `show` Displays the new or modified security policy parameters.
- `set <index>` Edits security policy parameters.
- `change` Completes policy changes and exits the session.
- `..` Cancels the changes made and exits the session.

**Example:**

```plaintext
admin(network.wireless.security.edit)>
admin(network.wireless.security.edit)>show

Policy Name : Default
Authentication : Manual Pre-shared key/No Authentication
Encrypted connections : no encryption
```

For information on configuring the encryption and authentication options available to the AP-5131 using the applet (GUI), see *Configuring Security Options on page 6-2.*
AP5131>admin(network.wireless.security)> delete

Description:
Deletes a specific security policy.

Syntax:
delete <sec-name>  Removes the specified security policy for the list supported.
<all>               Removes all security policies except the default policy.

For information on configuring the encryption and authentication options available to the AP-5131 using the applet (GUI), see Configuring Security Options on page 6-2.
8.3.3.3 Network ACL Commands

AP5131>admin(network.wireless.acl)>

Description:
Displays the AP-5131 Mobile Unit Access Control List (ACL) submenu. The items available under this command include:

- **show**: Displays the AP-5131’s current ACL configuration.
- **create**: Creates an MU ACL policy.
- **edit**: Edits the properties of an existing MU ACL policy.
- **delete**: Removes an MU ACL policy.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
AP5131>admin(network.wireless.acl)> show

Description:
Displays the AP-5131’s current ACL configuration.

Syntax:

show                      summary       Displays the list of existing MU ACL policies.
            policy  <index>       Displays the requested MU ACL index policy.

Example:

admin(network.wireless.acl)>show summary
------------------------------------------------------------------
ACL Policy Name               Associated WLANs
------------------------------------------------------------------
  1 Default               Front Lobby
  2 Admin                 Administration
  3 Demo Room            Customers
------------------------------------------------------------------

admin(network.wireless.acl)>show policy 1

Policy Name               : Front Lobby
Policy Mode               : allow

------------------------------------------------------------------
index                         start mac      end mac
------------------------------------------------------------------
  1  00A0F8348787              00A0F8348798

For information on configuring the ACL options available to the AP-5131 using the applet (GUI), see Configuring a WLAN Access Control List (ACL) on page 5-29.
AP5131>admin(network.wireless.acl)> create

Description:
Creates an MU ACL policy.

Syntax:
create <acl-name> Displays the parameters of a new ACL policy.
set acl-name <index> Sets the MU ACL policy name.
mode <acl-mode> Sets the ACL mode for the defined index (1-16). Allowed MUs can access
the AP-5131 managed LAN. Options are deny and allow.
add-addr <mac1> or <mac1> <mac2> Adds specified MAC address to list of ACL MAC addresses.
delete <index> <all> Removes either a specified ACL index or all ACL entries.
add-policy Completes the policy creation and exits the CLI.
.. Cancels the creation of the ACL and exits the CLI.

Example:

admin(network.wireless.acl.create)>show

Policy Name : Front Lobby
Policy Mode : allow

<table>
<thead>
<tr>
<th>index</th>
<th>start mac</th>
<th>end mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00A0F8334455</td>
<td>00A0F8334455</td>
</tr>
<tr>
<td>2</td>
<td>00A0F8400000</td>
<td>00A0F8402001</td>
</tr>
</tbody>
</table>

admin(network.wireless.acl.create)>set name engineering
admin(network.wireless.acl.create)>set mode deny
admin(network.wireless.acl.create)>add addr 00A0F843AABB
admin(network.wireless.acl.create)>add-policy

For information on configuring the ACL options available to the AP-5131 using the applet (GUI), see Configuring a WLAN Access Control List (ACL) on page 5-29.
AP5131>admin(network.wireless.acl.edit)>

**Description:**
Edits the properties of an existing MU ACL policy.

**Syntax:**

- **show**  
  Displays MU ACL policy and its parameters.
- **set**  
  Modifies the properties of an existing MU ACL policy.
- **add**  
  Adds an MU ACL table entry.
- **delete**  
  Deletes an MU ACL table entry, including starting and ending MAC address ranges.
- **change**  
  Completes the changes made and exits the session.
- **..**  
  Cancels the changes made and exits the session.

For information on configuring the ACL options available to the AP-5131 using the applet (GUI), see *Configuring a WLAN Access Control List (ACL)* on page 5-29.
AP5131>admin(network.wireless.acl)> delete

**Description:**
Removes an MU ACL policy.

**Syntax:**

```
delete       <acl name>   <index>  Deletes a particular MU ACL policy.
all               Deletes all MU ACL policies.
```

For information on configuring the ACL options available to the AP-5131 using the applet (GUI), see *Configuring a WLAN Access Control List (ACL) on page 5-29.*
8.3.3.4 Network Radio Configuration Commands

AP5131>admin(network.wireless.radio)>

Description:

Displays the AP-5131 Radio submenu. The items available under this command include:

- **show** Summarizes AP-5131 radio parameters at a high-level.
- **set** Defines the AP-5131 radio configuration.
- **radio1** Displays the 802.11b/g radio submenu.
- **radio2** Displays the 802.11a radio submenu.
- **..** Goes to the parent menu.
- **/** Goes to the root menu.
- **save** Saves the configuration to system flash.
- **quit** Quits the CLI.
**AP5131>admin(network.wireless.radio)> show**

**Description:**
Displays the AP-5131’s current radio configuration.

**Syntax:**
```
show
```
Displays the AP-5131’s current radio configuration.

**Example:**
```
admin(network.wireless.radio)>show

Radio Configuration

Radio 1
Name : Radio 1
Radio Mode : enable
RF Band of Operation : 802.11b/g (2.4 GHz)

Radio 2
Name : Radio 2
Radio Mode : enable
RF Band of Operation : 802.11a (5 GHz)
```

For information on configuring the Radio Configuration options available to the AP-5131 using the applet (GUI), see *Setting the WLAN's Radio Configuration on page 5-36.*
AP5131>admin(network.wireless.radio)> set

Description:
Enables an AP-5131 Radio and defines the RF band of operation.

Syntax:

```
set 11a <mode> Enables or disables the AP-5131’s 802.11a radio.
set 11bg <mode> Enables or disables the AP-5131’s 802.11b/g radio.
```

Example:

```
admin(network.wireless.radio)>set 11a disable
admin(network.wireless.radio)>set 11bg enable
admin(network.wireless.radio)>show
```

```
Radio Configuration
Radio 1
  Name : Radio 1
  Radio Mode : enable
  RF Band of Operation : 802.11b/g (2.4 GHz)

Radio 2
  Name : Radio 2
  Radio Mode : disable
  RF Band of Operation : 802.11a (5 GHz)
```

For information on configuring the Radio Configuration options available to the AP-5131 using the applet (GUI), see Setting the WLAN’s Radio Configuration on page 5-36.
**Description:**
Displays a specific 802.11b/g radio submenu. The items available under this command include:

**Syntax:**
- **show**  Displays 802.11b/g radio settings.
- **set**  Defines specific 802.11b/g radio parameters.
- **advanced**  Displays the Advanced radio settings submenu.
- **..**  Goes to the parent menu.
- **/**  Goes to the root menu.
- **save**  Saves the configuration to system flash.
- **quit**  Quits the CLI.

For information on configuring Radio 1 Configuration options available to the AP-5131 using the applet (GUI), see *Setting the WLAN's Radio Configuration on page 5-36.*
AP5131>admin(network.wireless.radio.radio1)> show

Description:
Displays specific 802.11b/g radio settings.

Syntax:
show radio
qos

Example:
admin(network.wireless.radio.radio1)> show radio

Radio Setting Information

Placement : indoor
MAC Address : 00A0F8715920
Radio Type : 802.11b/g

Channel Setting : user selection
Channel : 1
Antenna Diversity : full
Power Level : 5 dbm (4 mW)

802.11b/g mode : B-Only
Basic Rates : 1 2 5.5 11
Supported Rates : 1 2 5.5 11

Beacon Interval : 100
DTIM Interval : 10

short preamble : disable
RTS Threshold : 2341
**Command Line Interface Reference**

```
admin(network.wireless.radio.radio1)>show qos

----------------------------------------------
| Access Category | CWMin | CWMax | AIFSN | TXOPs |
----------------------------------------------
| Background      | 15    | 1023  | 7     | 0     |
| Best Effort     | 15    | 63    | 3     | 31    |
| Video           | 7     | 15    | 1     | 94    |
| Voice           | 3     | 7     | 1     | 47    |
----------------------------------------------
```

For information on configuring the Radio 1 Configuration options available to the AP-5131 using the applet (GUI), see *Configuring the 802.11a or 802.11b/g Radio on page 5-38*. 
**AP5131>admin(network.wireless.radio.802-11bg)> set**

**Description:**
Defines specific 802.11b/g radio parameters.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set placement</td>
<td>Defines the AP-5131 radio placement as indoors or outdoors.</td>
</tr>
<tr>
<td>ch-mode</td>
<td>Determines how the radio channel is selected.</td>
</tr>
<tr>
<td>channel</td>
<td>Defines the actual channel used by the radio.</td>
</tr>
<tr>
<td>antenna</td>
<td>Sets the radio antenna power</td>
</tr>
<tr>
<td>power</td>
<td>Defines the radio antenna power transmit level.</td>
</tr>
<tr>
<td>bg-mode</td>
<td>Enables or disables 802-11bg radio mode support.</td>
</tr>
<tr>
<td>rates</td>
<td>Sets the supported radio transmit rates.</td>
</tr>
<tr>
<td>beacon</td>
<td>Sets the beacon interval used by the radio.</td>
</tr>
<tr>
<td>dtim</td>
<td>Defines the DTIM interval used by the radio.</td>
</tr>
<tr>
<td>preamble</td>
<td>Enables or disables support for short preamble for the radio.</td>
</tr>
<tr>
<td>rts</td>
<td>Defines the RTS Threshold value for the radio.</td>
</tr>
<tr>
<td>qos</td>
<td>Defines the cwmin, cwmax, aifsn and txops levels for the QoS policy used for the radio.</td>
</tr>
</tbody>
</table>

**Example:**

```
admin(network.wireless.radio.802-11bg)>set placement indoor
admin(network.wireless.radio.802-11bg)>set ch-mode user
admin(network.wireless.radio.802-11bg)>set channel 1
admin(network.wireless.radio.802-11bg)>set antenna full
admin(network.wireless.radio.802-11bg)>set power 4
admin(network.wireless.radio.802-11bg)>set bg-mode enable
admin(network.wireless.radio.802-11bg)>set rates
admin(network.wireless.radio.802-11bg)>set beacon 100
admin(network.wireless.radio.802-11bg)>set dtim 10
admin(network.wireless.radio.802-11bg)>set preamble disable
admin(network.wireless.radio.802-11bg)>set rts 2341
admin(network.wireless.radio.802-11bg)>set qos cwmin 125
admin(network.wireless.radio.802-11bg)>set qos cwxmax 255
admin(network.wireless.radio.802-11bg)>set qos aifsn 7
admin(network.wireless.radio.802-11bg)>set qos txops 0
```

For information on configuring the Radio 1 Configuration options available to the AP-5131 using the applet (GUI), see *Configuring the 802.11a or 802.11b/g Radio on page 5-38.*
**AP5131>admin(network.wireless.radio.802-11bg.advanced)>**

**Description:**
Displays the advanced submenu for the 802.11b/g radio. The items available under this command include:

**Syntax:**
- **show** Displays advanced radio settings for the 802.11b/g radio.
- **set** Defines advanced parameters for the 802.11b/g radio.
- **..** Goes to the parent menu.
- **/** Goes to the root menu.
- **save** Saves the configuration to system flash.
- **quit** Quits the CLI.
AP5131>admin(network.wireless.radio.802-11bg.advanced)> show

Description:
Displays the BSSID to WLAN mapping for the 802.11b/g radio.

Syntax:

show advanced wlan
Displays advanced settings for the 802.11b/g radio.
Displays WLAN summary list for the 802.11b/g radio.

Example:

admin(network.wireless.radio.802-11bg.advanced)> show advanced

-------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>WLAN</th>
<th>BSS ID</th>
<th>BC/MC Cipher</th>
<th>Status</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lobby</td>
<td>1</td>
<td>Open</td>
<td>good</td>
<td>configuration is ok</td>
</tr>
<tr>
<td>HR</td>
<td>2</td>
<td>Open</td>
<td>good</td>
<td>configuration is ok</td>
</tr>
<tr>
<td>Office</td>
<td>3</td>
<td>Open</td>
<td>good</td>
<td>configuration is ok</td>
</tr>
</tbody>
</table>
-------------------------------------------------------------------------------

BSSID Primary WLAN

| 1   | Lobby |
| 2   | HR    |
| 3   | Office |

For information on configuring Radio 1 Configuration options available to the AP-5131 using the applet (GUI), see Configuring the 802.11a or 802.11b/g Radio on page 5-38.
**AP5131>admin(network.wireless.radio.802-11bg.advanced)> set**

**Description:**
Defines advanced parameters for the target 802.11b/g radio.

**Syntax:**

```plaintext
set wlan <wlan-name> <bssid>  Defines advanced WLAN to BSSID mapping for the target radio.
set bss <bssid> <wlan name> Sets the BSSID to primary WLAN definition.
```

**Example:**

```
admin(network.wireless.radio.802-11bg.advanced)>set wlan demoroom 1
admin(network.wireless.radio.802-11bg.advanced)>set bss 1 demoroom
```

For information on configuring Radio 1 Configuration options available to the AP-5131 using the applet (GUI), see *Configuring the 802.11a or 802.11b/g Radio on page 5-38.*
AP5131>admin(network.wireless.radio.802-11a)>

Description:
Displays a specific 802.11a radio submenu. The items available under this command include:

Syntax:

- **show**: Displays 802.11a radio settings
- **set**: Defines specific 802.11a radio parameters.
- **advanced**: Displays the Advanced radio settings submenu.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
AP5131>admin(network.wireless.radio.802-11a)> show

Description:
Displays specific 802.11a radio settings.

Syntax:

```
show  radio  qos
```

Displays specific 802.11a radio settings.
Displays specific 802.11a radio WMM QoS settings.

Example:

```
admin(network.wireless.radio.802-11a)> show radio
```

Radio Setting Information

<table>
<thead>
<tr>
<th>Placement</th>
<th>indoor</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>00A0F8715920</td>
</tr>
<tr>
<td>Radio Type</td>
<td>802.11a</td>
</tr>
<tr>
<td>Channel Setting</td>
<td>user selection</td>
</tr>
<tr>
<td>Channel</td>
<td>1</td>
</tr>
<tr>
<td>Antenna Diversity</td>
<td>full</td>
</tr>
<tr>
<td>Power Level</td>
<td>5 dbm (4 mW)</td>
</tr>
<tr>
<td>Basic Rates</td>
<td>1 2 5.5 11</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>1 2 5.5 11</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>100</td>
</tr>
<tr>
<td>DTIM Interval</td>
<td>10</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>2341</td>
</tr>
</tbody>
</table>
admin(network.wireless.radio.802-11a)>show qos

<table>
<thead>
<tr>
<th>Access Category</th>
<th>CWMin</th>
<th>CWMax</th>
<th>AIFSN</th>
<th>TXOPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>15</td>
<td>1023</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Best Effort</td>
<td>15</td>
<td>63</td>
<td>3</td>
<td>31</td>
</tr>
<tr>
<td>Video</td>
<td>7</td>
<td>15</td>
<td>1</td>
<td>94</td>
</tr>
<tr>
<td>Voice</td>
<td>3</td>
<td>7</td>
<td>1</td>
<td>47</td>
</tr>
</tbody>
</table>

For information on configuring Radio 2 Configuration options available to the AP-5131 using the applet (GUI), see Configuring the 802.11a or 802.11b/g Radio on page 5-38.
AP5131 > admin(network.wireless.radio.802-11a) > set

Description:
Defines specific 802.11a radio parameters.

Syntax:

```
set placement          Defines the AP-5131 radio placement as indoors or outdoors.
ch-mode                Determines how the radio channel is selected.
channel                Defines the actual channel used by the radio.
antenna                 Sets the radio antenna power.
power                  Defines the radio antenna power transmit level.
rates                  Sets the supported radio transmit rates.
beacon                 Sets the beacon interval used by the radio.
dtim                   Defines the DTIM interval used by the radio.
rts                    Defines the RTS Threshold value for the radio.
qos                    Defines the cwmin, cwmax, aifsn and txops levels for the QoS policy used for the radio.
```

Example:

```
admin(network.wireless.radio.802-11a) >

admin(network.wireless.radio.802-11a) > set placement indoor
admin(network.wireless.radio.802-11a) > set ch-mode user
admin(network.wireless.radio.802-11a) > set channel 1
admin(network.wireless.radio.802-11a) > set antenna full
admin(network.wireless.radio.802-11a) > set power 4
admin(network.wireless.radio.802-11a) > set rates
admin(network.wireless.radio.802-11a) > set beacon 100
admin(network.wireless.radio.802-11a) > set dtim 10
admin(network.wireless.radio.802-11a) > set rts 2341
admin(network.wireless.radio.802-11a) > set qos cwmin 125
admin(network.wireless.radio.802-11a) > set qos cwmax 255
admin(network.wireless.radio.802-11a) > set qos aifsn 7
admin(network.wireless.radio.802-11a) > set qos txops 0
```

For information on configuring the Radio 2 Configuration options available to the AP-5131 using the applet (GUI), see Configuring the 802.11a or 802.11b/g Radio on page 5-38.
AP5131>admin(network.wireless.radio.802-11a.advanced)>

Description:
Displays the advanced submenu for the 802-11a radio. The items available under this command include:

Syntax:

- **show**: Displays advanced radio settings for the 802-11a radio.
- **set**: Defines advanced parameters for the 802-11a radio.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
**AP5131>admin(network.wireless.radio.802-11a.advanced)> show**

**Description:**
Displays the BSSID to WLAN mapping for the 802.11a radio.

**Syntax:**

```
show advanced
wlan
```

Displays advanced settings for the 802.11a radio.

Displays WLAN summary list for 802.11a radio.

**Example:**

```
admin(network.wireless.radio.802-11a.advanced)> show advanced
```

<table>
<thead>
<tr>
<th>WLAN</th>
<th>BSSID</th>
<th>BC/MC Cipher</th>
<th>Status</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lobby</td>
<td>1</td>
<td>Open</td>
<td>good</td>
<td>configuration is ok</td>
</tr>
<tr>
<td>HR</td>
<td>2</td>
<td>Open</td>
<td>good</td>
<td>configuration is ok</td>
</tr>
<tr>
<td>Office</td>
<td>3</td>
<td>Open</td>
<td>good</td>
<td>configuration is ok</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Primary WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lobby</td>
</tr>
<tr>
<td>2</td>
<td>HR</td>
</tr>
<tr>
<td>3</td>
<td>Office</td>
</tr>
</tbody>
</table>

For information on configuring the Radio 2 Configuration options available to the AP-5131 using the applet (GUI), see Configuring the 802.11a or 802.11b/g Radio on page 5-38.
AP5131>admin(network.wireless.radio.802-11a.advanced)> set

Description:
Defines advanced parameters for the target 802..11a radio.

Syntax:

```
set wlan <wlan-name> <bssid> Defines advanced WLAN to BSSID mapping for the target radio.
bss <bssid-id> <wlan-name> Sets the BSSID to primary WLAN definition.
```

Example:

```
admin(network.wireless.radio.802-11a.advanced)>set wlan demoroom 1
admin(network.wireless.radio.802-11a.advanced)>set bss 1 demoroom
```

For information on configuring Radio 2 Configuration options available to the AP-5131 using the applet (GUI), see Configuring the 802.11a or 802.11b/g Radio on page 5-38.
8.3.3.5 Network Quality of Service (QoS) Commands

AP5131>admin(network.wireless.qos)>

Description:
Displays the AP-5131 Quality of Service (QoS) submenu. The items available under this command include:

- **show** Displays AP-5131 QoS policy information.
- **create** Defines the parameters of the QoS policy.
- **edit** Edits the settings of an existing QoS policy.
- **delete** Removes an existing QoS policy.
- .. Goes to the parent menu.
- / Goes to the root menu.
- save Saves the configuration to system flash.
- quit Quits the CLI.
**AP1531>admin(network.wireless.qos)> show**

**Description:**
Displays the AP-5131’s current QoS policy by summary or individual policy.

**Syntax:**
- `show`             Displays all existing QoS policies that have been defined.
- `summary`          Displays the configuration for the requested QoS policy.
- `policy <index>`

**Example:**

```
admin(network.wireless.qos)> show summary

+----------------+---------------+
| QoS Policy Name| Associated WLANs |
+----------------+---------------+
| 1 Default      | 101           |
| 2 IP Phones    | Audio Dept    |
| 3 Video        | Vido Dept     |
```

```
admin(network.wireless.qos)> show policy 1

Policy Name   IP Phones
Support Legacy Voice Mode disable
Multicast address 1 01005E000000
Multicast address 2 09000E000000
WMM QOS Extension Mode disable
```

For information on configuring the WLAN QoS options available to the AP-5131 using the applet (GUI), see *Setting the WLAN Quality of Service (QoS) Policy* on page 5-31.
AP5131>admin(network.wireless.qos.create)>

Description:
Defines an AP-5131 QoS policy.

Syntax:

- **show**  Displays new QoS policy parameters.
- **set**  Sets QoS policy parameters.
- **add-policy**  Completes the policy creation and exits the CLI session.
- ..  Cancels the QoS policy creation and exits the CLI session.

For information on configuring the WLAN QoS options available to the AP-5131 using the applet (GUI), see Setting the WLAN Quality of Service (QoS) Policy on page 5-31.
**AP5131 > admin(network.wireless.qos.edit)>**

**Description:**
Edits the properties of an existing QoS policy.

**Syntax:**

- `show` Displays QoS policy parameters.
- `set qos-name <index>` Sets the QoS name for the specified index entry.
- `set vop <index>` Enables or disables support (by index) for legacy VOIP devices.
- `set mcast <mac>` Defines primary and secondary Multicast MAC address.
- `set wmm-qos <index>` Enables or disables the QoS policy index specified.
- `set cwmin <access category> <index>` Defines Minimum Contention Window (CW-Min) for specified access category and index.
- `set cwmax <access category> <index>` Defines Maximum Contention Window (CW-Max) for specified access category and index.
- `set aifsn <access category> <index>` Sets Arbitrary Inter-Frame Space Number (AIFSN) for specified access category and index.
- `set txops <access category> <index>` Configures Opportunity to Transmit Time (TXOPs Time) for specified access category and index.
- `set default <index>` Defines CWMIN, CWMAX, AIFSN and TXOPs default values.
- `change` Completes the policy edit and exits the session.
- `..` Cancels the changes and exits.

For information on configuring the WLAN QoS options available to the AP-5131 using the applet (GUI), see *Setting the WLAN Quality of Service (QoS) Policy on page 5-31*. 
**AP5131>admin(network.wireless.qos)> delete**

**Description:**
Removes a QoS policy.

**Syntax:**

```
delete <qos-name>                      Deletes the specified QoS policy index, or all of the policies.
  <all>
```

For information on configuring the WLAN QoS options available to the AP-5131 using the applet (GUI), see *Setting the WLAN Quality of Service (QoS) Policy on page 5-31.*
8.3.3.6 Network Bandwidth Management Commands

AP5131>admin(network.wireless.bandwidth)>

Description:
Displays the AP-5131 Bandwidth Management submenu. The items available under this command include:

- `show` Displays Bandwidth Management information for how data is processed by the AP-5131.
- `set` Defines Bandwidth Management parameters for the AP-5131.
- `..` Goes to the parent menu.
- `/` Goes to the root menu.
- `save` Saves the configuration to system flash.
- `quit` Quits the CLI.
**AP5131>admin(network.wireless.bandwidth)> show**

**Description:**
Displays the AP-5131’s current Bandwidth Management configuration.

**Syntax:**
```
show
```
Displays the current Bandwidth Management configuration for defined WLANs and how they are weighted.

**Example:**
```
admin(network.wireless.bandwidth)>show
```

| Bandwidth Share Mode | : First In First Out |

For information on configuring the Bandwidth Management options available to the AP-5131 using the applet (GUI), see Configuring Bandwidth Management Settings on page 5-45.
AP5131>admin(network.wireless.bandwidth)> set

**Description:**
Defines the AP-5131 Bandwidth Management configuration.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set mode</td>
<td>Defines bandwidth share mode of First In First Out &lt;fifo&gt;, Round Robin &lt;rr&gt; or Weighted Round Robin &lt;wrr&gt;</td>
</tr>
<tr>
<td>weight</td>
<td>Assigns a bandwidth share allocation for the WLAN &lt;index 1-16&gt; when Weighted Round Robin &lt;wrr&gt; is selected. The weighting is from 1-10.</td>
</tr>
</tbody>
</table>

For information on configuring the Bandwidth Management options available to the AP-5131 using the applet (GUI), see Configuring Bandwidth Management Settings on page 5-45.
8.3.3.7 Network Rogue-AP Commands

AP5131>admin(network.wireless.rogue-ap)>

Description:
Displays the Rogue AP submenu. The items available under this command include:

- **show**: Displays the current AP-5131 Rogue AP detection configuration.
- **set**: Defines the Rogue AP detection method.
- **mu-scan**: Goes to the Rogue AP mu-scan submenu.
- **allowed-list**: Goes to the Rogue AP Allowed List submenu.
- **active-list**: Goes the Rogue AP Active List submenu.
- **rogue-list**: Goes the Rogue AP List submenu.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
**AP5131>admin(network.wireless.rogue-ap)> show**

**Description:**
Displays the current AP-5131 Rogue AP detection configuration.

**Syntax:**
`show` Displays the current AP-5131 Rogue AP detection configuration.

**Example:**
```
admin(network.wireless.rogue-ap)> show

 MU Scan : disable
 MU Scan Interval : 60 minutes
 On Channel : disable
 Detector Radio Scan : enable
 Detector Radio Band : 11bg

 Auto Authorize Symbol APs : disable

 Approved APs age out : 0
 Rogue APs age out : 0
```

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see *Configuring Rogue AP Detection on page 6-51*. 
**AP5131>admin(network.wireless.rogue-ap)> set**

**Description:**
Defines the AP-5131 ACL rogue AP method.

**Syntax:**

```plaintext
set mu-scan <mode>       Enables or disables to permit MUs to scan for rogue APs.
interval <minutes>       Define an interval for associated MUs to beacon in attempting to locate rogue APs.
                        Value not available unless mu-scan is enabled.
on-channel <mode>       Enables or disables on-channel detection.
detector-scan <mode>    Enables or disables AP detector scan (dual-radio model only).
symbol-ap <mode>        Enables or disables the Authorize Any AP with a Symbol MAC address option.
applst-ageout <minutes> Sets the approved AP age out time.
roglst-ageout <minutes> Sets the rogue AP age out time.
```

**Example:**

```
admin(network.wireless.rogue-ap)>

admin(network.wireless.rogue-ap)>set mu-scan enable
admin(network.wireless.rogue-ap)>set interval 10
admin(network.wireless.rogue-ap)>set on-channel disable
admin(network.wireless.rogue-ap)>set detector-scan disable
admin(network.wireless.rogue-ap)>set symbol-ap enable
admin(network.wireless.rogue-ap)>set applst-ageout 10
admin(network.wireless.rogue-ap)>set roglst-ageout 10

admin(network.wireless.rogue-ap)>show

MU Scan                 : enable
MU Scan Interval        : 10 minutes
On Channel             : disable
Detector Radio Scan    : disable
Detector Radio Band    : none

Auto Authorize Symbol APs : enable

Approved AP age out    : 10
Rogue AP age out       : 10
```

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see *Configuring Rogue AP Detection on page 6-51*. 
AP5131>admin(network.wireless.rogue-ap.mu-scan)>

Description:
Displays the Rogue-AP mu-scan submenu.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Initiates scan immediately by the MU.</td>
</tr>
<tr>
<td>show</td>
<td>Displays all APs located by the MU scan.</td>
</tr>
<tr>
<td>.</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>
**AP5131>admin(network.wireless.rogue-ap.mu-scan)> start**

**Description:**
Initiates an MU scan from a user provided MAC address.

**Syntax:**

```
start <mu-mac> Initiates MU scan from user provided MAC address.
```

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see *Configuring Rogue AP Detection on page 6-51.*
**AP5131>admin(network.wireless.rogue-ap.mu-scan)> show**

**Description:**
Displays the results of an MU scan.

**Syntax:**

```
show
```

Initiates MU scan from user provided MAC address.

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see Configuring Rogue AP Detection on page 6-51.
**AP5131>admin(network.wireless.rogue-ap.allowed-list)>**

**Description:**
Displays the Rogue-AP allowed-list submenu.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays the rogue AP allowed list</td>
</tr>
<tr>
<td>add</td>
<td>Adds an AP MAC address and ESSID to the allowed list.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes an entry or all entries from the allowed list.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>
AP5131>admin(network.wireless.rogue-ap.allowed-list)> show

Description:
Displays the Rogue AP allowed List.

Syntax:
show
Displays the rogue-AP allowed list.

Example:
admin(network.wireless.rogue-ap.allowed-list)>show

--------------------------------------------------------------------------
index  ap               essid
--------------------------------------------------------------------------
 1  00:A0:F8:71:59:20 *
 2  00:A0:F8:33:44:55  101
 3  00:A0:F8:40:20:01  Marketing

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see Configuring Rogue AP Detection on page 6-51.
**AP5131>admin(network.wireless.rogue-ap.allowed-list)> add**

**Description:**
Adds an AP MAC address and ESSID to existing allowed list.

**Syntax:**
```
add <mac-addr> <ess-id>
```
Add an AP MAC address and ESSID to existing allowed list. Use a "*" for any ESSID.

**Example:**
```
admin(network.wireless.rogue-ap.allowed-list)>add 00A0F83161BB 103
admin(network.wireless.rogue-ap.allowed-list)>show

<table>
<thead>
<tr>
<th>index</th>
<th>ap</th>
<th>essid</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:A0:F8:71:59:20</td>
<td>*</td>
</tr>
<tr>
<td>2</td>
<td>00:A0:F8:33:44:55</td>
<td>101</td>
</tr>
<tr>
<td>3</td>
<td>00:A0:F8:40:20:01</td>
<td>Marketing</td>
</tr>
<tr>
<td>4</td>
<td>00:A0:F8:31:61:BB</td>
<td>103</td>
</tr>
</tbody>
</table>
```

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see [Configuring Rogue AP Detection on page 6-51](#).
AP5131>admin(network.wireless.rogue-ap.allowed-list)> delete

Description:
Deletes an AP MAC address and ESSID to existing allowed list.

Syntax:

```
delete <idx> <all>
```

Deletes an AP MAC address and ESSID (or all addresses) from the allowed list.

For information on configuring the Rogue AP options available to the AP-5131 using the applet (GUI), see Configuring Rogue AP Detection on page 6-51.
8.3.4 Network Firewall Commands

AP5131>admin(network.firewall)>

Description:
Displays the AP-5131 firewall submenu. The items available under this command include:

- **show**: Displays the AP-5131’s current firewall configuration.
- **set**: Defines the AP-5131’s firewall parameters.
- **access**: Enables/disables firewall permissions through the LAN and WAN ports.
- **advanced**: Displays interoperability rules between the LAN and WAN ports.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
AP5131>admin(network.firewall)> show

Description:
Displays the AP-5131 firewall parameters.

Syntax:
show

Example:

    admin(network.firewall)> show

    Firewall Status : disable
    Override LAN to WAN Access : disable

    Configurable Firewall Filters:

    ftp bounce attack filter : enable
    syn flood attack filter : enable
    unaligned ip timestamp filter : enable
    source routing attack filter : enable
    winnuke attack filter : enable
    seq num prediction attack filter : enable
    mime flood attack filter : enable
    max mime header length : 8192
    max mime headers : 16

For information on configuring the Firewall options available to the AP-5131 using the applet (GUI), see Configuring Firewall Settings on page 6-25.
AP5131>admin(network.firewall)> set

Description:
Defines the AP-5131 firewall parameters.

Syntax:

set mode <mode> Enables or disables the firewall.
nat-timeout <interval> Defines the NAT interval.
override <mode> Enables or disables subnet access override.
syn <mode> Enables or disables SYN flood attack check.
src <mode> Enables or disables source routing check.
win <mode> Enables or disables Winnuke attack check.
ftp <mode> Enables or disables FTP bounce attack check.
in <mode> Enables or disables IP unaligned timestamp check.
seq <mode> Enables or disables sequence number prediction check.
mime filter Enables or disables MIME flood attack check.
len <length> Sets the max header length in bytes as specified by <length>
(hdr <count> Sets the max number of headers as specified in <count>}

Example:

admin(network.firewall)>set mode enable
admin(network.firewall)>set override enable
admin(network.firewall)>set ftp enable
admin(network.firewall)>set ip enable
admin(network.firewall)>set seq enable
admin(network.firewall)>set src enable
admin(network.firewall)>set syn enable
admin(network.firewall)>set win enable
admin(network.firewall)>show

Firewall Status : enable
Override LAN to WAN Access : disable

Configurable Firewall Filters

ftp bounce attack filter : enable
syn flood attack filter : enable
unaligned ip timestamp filter : enable
source routing attack filter : enable
winnuke attack filter : enable
seq num prediction attack filter : enable
mime flood attack filter : enable
max mime header length : 8192
max mime headers : 16
AP5131>admin(network.firewall)> access

Description:
Enables or disables firewall permissions through LAN to WAN ports.

Syntax:

- **show**: Displays LAN to WAN access rules.
- **set**: Sets LAN to WAN access rules.
- **add**: Adds LAN to WAN exception rules.
- **delete**: Deletes LAN to WAN access exception rules.
- **list**: Displays LAN to WAN access exception rules.
- **..**: Goes to parent menu
- **/**: Goes to root menu.
- **save**: Saves configuration to system flash.
- **quit**: Quits and exits the CLI session.

Example:

```
admin(network.firewall)>set override disable
admin(network.firewall)>access
admin(network.firewall.lan-wan-access)>set rule allow
admin(network.firewall.lan-wan-access)>list
```

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>lan</td>
<td>wan</td>
<td>HTTP</td>
<td>tcp</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>2</td>
<td>lan</td>
<td>wan</td>
<td>abc</td>
<td>udp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>lan</td>
<td>wan</td>
<td>123456</td>
<td>ah</td>
<td>1440</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>lan</td>
<td>wan</td>
<td>654321</td>
<td>tcp</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>5</td>
<td>lan</td>
<td>wan</td>
<td>abc</td>
<td>ah</td>
<td>100</td>
<td>1000</td>
</tr>
</tbody>
</table>

For information on configuring the Firewall options available to the AP-5131 using the applet (GUI), see Configuring Firewall Settings on page 6-25.
**AP5131>admin(network.firewall)> advanced**

**Description:**
Displays whether an AP-5131 firewall rule is intended for inbound traffic to an interface or outbound traffic from that interface.

**Syntax:**

import Imports rules from LAN to WAN access.
inbound Goes to the Inbound Firewall Rules submenu.
outbound Goes to the Outbound Firewall Rules submenu.
.. Goes to the parent menu.
/ Goes to the root menu.
save Saves the configuration to flash memory.
quit Quits and exits the CLI session.

**Example:**

```
admin(network.firewall)> set override enable
admin(network.firewall)> advanced
admin(network.firewall.rules)> inbound
admin(network.firewall.rules.inb)> list
```

<table>
<thead>
<tr>
<th>Idx</th>
<th>SCR IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>TP</th>
<th>SPorts</th>
<th>DPorts</th>
<th>Rev</th>
<th>NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.2.3.4</td>
<td>2.2.2.2</td>
<td>all</td>
<td>1:</td>
<td>1:</td>
<td>0.0.0.0</td>
<td>deny</td>
<td></td>
</tr>
<tr>
<td></td>
<td>255.0.0.0</td>
<td>255.0.0.0</td>
<td></td>
<td>65535</td>
<td>65535</td>
<td>nat</td>
<td>port 33</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>33.3.0.0</td>
<td>10.10.1.1</td>
<td>tcp</td>
<td>1:</td>
<td>1:</td>
<td>11.11.1.0</td>
<td>allow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td></td>
<td>65535</td>
<td>65535</td>
<td>nat</td>
<td>port 0</td>
<td></td>
</tr>
</tbody>
</table>
```

For information on configuring the Firewall options available to the AP-5131 using the applet (GUI), see [Configuring Firewall Settings on page 6-25](#).
### 8.3.5 Network Router Commands

**AP5131>admin(network.router)>**

**Description:**
Displays the router submenu. The items available under this command are:

- **add**  
  Adds user-defined routes.
- **delete**  
  Deletes user-defined routes.
- **list**  
  Lists user-defined routes.
- **show**  
  Displays the existing AP-5131 router configuration.
- ..  
  Goes to the parent menu.
- /  
  Goes to the root menu.
- **save**  
  Saves the configuration to system flash.
- **quit**  
  Quits the CLI.
**AP5131>admin(network.router)> show**

**Description:**
Shows the AP-5131 route table.

**Syntax:**

`show`  
Shows the AP-5131 route table.

**Example:**

```
admin(network.router)> show
----------------------------------------------------------------------------
 index  destination  netmask  gateway  interface  metric
----------------------------------------------------------------------------
   1  192.168.2.0  255.255.255.0  0.0.0.0  lan  0
   2  192.168.1.0  255.255.255.0  0.0.0.0  lan  0
   3  192.168.0.0  255.255.255.0  0.0.0.0  lan  0
   4  192.168.24.0  255.255.255.0  0.0.0.0  wan  0
   5  157.235.19.5  255.255.255.0  192.168.24.1  wan  0
```

For information on configuring the Router options available to the AP-5131 using the applet (GUI), see *Configuring Router Settings on page 5-47*. 


AP5131>admin(network.router)> add

Description:
Adds user-defined routes.

Syntax:
add <dest> <netmask> <gw> <iface> <metric>  Adds a route with destination IP address <dest>, IP netmask <netmask>, destination gateway IP address <gw>, interface LAN or WAN <iface>, and metric set to <metric> (1-15).

Example:

admin(network.router)> add 192.168.2.100 255.255.255.0 192.168.2.1 LAN 1

admin(network.router)> list

<table>
<thead>
<tr>
<th>index</th>
<th>destination</th>
<th>netmask</th>
<th>gateway</th>
<th>interface</th>
<th>metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.2.100</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
<td>lan</td>
<td>1</td>
</tr>
</tbody>
</table>

For information on configuring the Router options available to the AP-5131 using the applet (GUI), see Configuring Router Settings on page 5-47.
AP5131>admin(network.router)> delete

Description:
Deletes user-defined routes.

Syntax:

\texttt{delete <idx>} Deletes the user-defined route <idx> (1-20) from list.
\texttt{all} Deletes all user-defined routes.

Example:

\begin{verbatim}
admin(network.router)>list
------------------------------------------------------------------
index destination  netmask  gateway  interface  metric
------------------------------------------------------------------
1  192.168.2.0  255.255.255.0  0.0.0.0  lan  0
2  192.168.1.0  255.255.255.0  0.0.0.0  lan  0
3  192.168.0.0  255.255.255.0  0.0.0.0  lan  0

admin(network.router)>delete 2
admin(network.router)>list
------------------------------------------------------------------
index destination  netmask  gateway  interface  metric
------------------------------------------------------------------
1  192.168.2.0  255.255.255.0  0.0.0.0  lan  0
2  192.168.0.0  255.255.255.0  0.0.0.0  lan  0

admin(network.router)>
\end{verbatim}

For information on configuring the Router options available to the AP-5131 using the applet (GUI), see Configuring Router Settings on page 5-47.
**AP5131>admin(network.router)> list**

**Description:**
Lists user-defined routes.

**Syntax:**

```
list
```

Displays a list of user-defined routes.

**Example:**

```
admin(network.router)>list
```

<table>
<thead>
<tr>
<th>index</th>
<th>destination</th>
<th>netmask</th>
<th>gateway</th>
<th>interface</th>
<th>metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.2.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>lan</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>lan</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>lan</td>
<td>0</td>
</tr>
</tbody>
</table>

For information on configuring the Router options available to the AP-5131 using the applet (GUI), see Configuring Router Settings on page 5-47.
8.4 System Commands

**AP5131>admin(system)>**

**Description:**
Displays the System submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restart</td>
<td>Restarts the AP-5131.</td>
</tr>
<tr>
<td>show</td>
<td>Shows AP-5131 system parameter settings.</td>
</tr>
<tr>
<td>set</td>
<td>Defines AP-5131 system parameter settings.</td>
</tr>
<tr>
<td>debug</td>
<td>Accesses AP-5131 password-protected debug information.</td>
</tr>
<tr>
<td>lastpw</td>
<td>Displays last debug password.</td>
</tr>
<tr>
<td>exec</td>
<td>Goes to a Linux command menu.</td>
</tr>
<tr>
<td>access</td>
<td>Goes to the AP-5131 access submenu where AP-5131 access methods can be enabled.</td>
</tr>
<tr>
<td>cmgr</td>
<td>Goes the Certificate Manager submenu.</td>
</tr>
<tr>
<td>snmp</td>
<td>Goes to the SNMP submenu.</td>
</tr>
<tr>
<td>ntp</td>
<td>Goes to the Network Time Protocol submenu.</td>
</tr>
<tr>
<td>logs</td>
<td>Displays the log file submenu.</td>
</tr>
<tr>
<td>cfg-update</td>
<td>Goes to the configuration file update submenu.</td>
</tr>
<tr>
<td>fw-update</td>
<td>Goes to the firmware update submenu.</td>
</tr>
<tr>
<td>test</td>
<td>Goes to the test group sub menu.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>
**AP5131>admin(system)>restart**

**Description:**
Restarts the AP-5131 access point.

**Syntax:**

```
restart
```

Restarts the AP-5131.

**Example:**

```
admin(system)>restart
```

**************************************************************************
** Unsaved configuration changes will be lost when the AP-5131 is reset.
** Please be sure to save changes before resetting.
**************************************************************************

Are you sure you want to restart the AP-5131? (yes/no):

AP-5131 Boot Firmware Version 1.0.0.0-xxx
Copyright(c) Symbol Technologies Inc. 2005. All rights reserved.

Press escape key to run boot firmware ........

Power On Self Test

```
testing ram : pass
testing nor flash : pass
testing nand flash : pass
testing ethernet : pass
```

For information on restarting the AP-5131 using the applet (GUI), see *Configuring System Settings on page 4-2*. 
**AP5131>admin(system)>show**

**Description:**
Displays high-level AP-5131 system information.

**Syntax:**

```
show
```
Displays AP-5131 system information.

**Example:**

```
admin(system)>show

system name            : BldgC
system location        : Atlanta Field Office
admin email address    : johndoe@mycompany.com
system uptime          : 0 days 4 hours 41 minutes
AP-5131 firmware version: 1.0.0.0-xxx
country code           : us

admin(system)>
```

For information on displaying System Settings using the applet (GUI), see *Configuring System Settings on page 4-2*.
AP5131>admin(system)>set

Description:
Sets AP-5131 system parameters.

Syntax:

set name <name> Sets the AP-5131 system name to <name> (1 to 59 characters).
loc <loc> Sets the AP-5131 system location to <loc> (1 to 59 characters).
email <email> Sets the AP-5131 admin email address to <email> (1 to 59 characters).
cc <code> Sets the AP-5131 country code using two-letters <code>.

Example:

    admin(system)>show

    system name : AP5131
    system location : San Jose Engineering
    admin email address : SJSharkey@symbol.com
    system uptime : 0 days 4 hours 33 minutes
    AP-5131 firmware version : 1.0.0.0-xxx
    country code : us

For information on configuring System Settings using the applet (GUI), see Configuring System Settings on page 4-2. Refer to Appendix A for information on the two-character country codes.
8.4.1 System Debug and Last Password Commands

**AP5131>admin(system)>debug**

**Description:**
Accesses AP-5131 debug information. This information is designed for field service use only, and should not be used by unqualified personnel.

**Example:**

```
admin(system)>debug

Debug Password:

AP-5131 MAC Address is 00:A0:F8:71:6A:74
Last Password was symbol12
```

**AP5131>admin(system)>lastpw**

**Description:**
Displays the last debug password.

```
admin(system)>lastpw

AP-5131 MAC Address is 00:A0:F8:71:6A:74
Last Password was symbol12
Current password used 0 times, valid 4 more time(s)
```
8.4.2 System Access Commands

AP5131>admin(system)>access

Description:
Displays the AP-5131 access submenu.

- **show**: Displays AP-5131 system access capabilities.
- **set**: Goes to the AP-5131 system access submenu.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the current configuration to the AP-5131 system flash.
- **quit**: Quits the CLI and exits the current session.
AP5131>admin(system.access)>set

Description:
Defines the permissions to access the AP-5131 applet, CLI, SNMP as well as defining their timeout values.

Syntax:

```
set applet lan
applet wan
app-timeout <minutes>
cli wan
cli lan
ssh wan
ssh lan
auth-timeout <seconds>
inactive-timeout <minutes>
smtp wan
smtp lan
admin-auth local/
               RADIUS
server <ip>
port <port#>
secret <pw>
```

- `set applet lan` defines the applet HTTP/HTTPS access parameters for the LAN port.
- `applet wan` defines the applet HTTP/HTTPS access parameters for the WAN port.
- `app-timeout <minutes>` sets the radio interface timeout interval if no activity is detected over Applet HTTPS (port 443) after the defined interval. Default is 300 Mins.
- `cli wan` defines CLI Telnet access parameters for the AP-5131 WAN port.
- `cli lan` defines CLI Telnet access parameters for the AP-5131 LAN port.
- `ssh wan` sets the WAN access to the CLI using the SSH (Secure Shell) protocol.
- `ssh lan` sets the LAN access to the CLI using the SSH (Secure Shell) protocol.
- `auth-timeout <seconds>` disables the radio interface if no data activity is detected after the interval defined. Default is 120 seconds.
- `inactive-timeout <minutes>` inactivity interval resulting in the AP terminating its connection. Default is 120 minutes.
- `smtp wan` sets SNMP interface values through the WAN port.
- `smtp lan` sets SNMP interface values through the LAN port.
- `admin-auth local/ RADIUS` designates a Radius server is used in the authentication verification.
- `server <ip>` specifies the IP address the Remote Dial-In User Service (RADIUS) server.
- `port <port#>` specifies the port on which the RADIUS server is listening. Default is 1812.
- `secret <pw>` defines the shared secret password for RADIUS server authentication.

For information on configuring AP-5131 access settings using the applet (GUI), see Configuring Data Access on page 4-5.
AP5131>admin(system.access)>show

**Description:**
Displays the current AP-5131 access permissions and timeout values.

**Syntax:**

`show`  
Shows all of the current system access settings for the AP-5131.

**Example:**

```
admin(system.access)>show

applet http access from lan : enable
applet http access from wan : enable
applet https access from lan : enable
applet https access from wan : enable
http/s timeout : 100
cli telnet access from lan : enable
cli telnet access from wan : enable
cli ssh access from lan : enable
cli ssh access from wan : enable
ssh server authentication timeout : 120
ssh server inactive timeout : 120
snmp access from lan : enable
snmp access from wan : enable
admin authentication mode : local
```

**Related Commands:**

- `set`  
  Defines the AP-5131 system access capabilities and timeout values.

For information on configuring AP-5131 access settings using the applet (GUI), see *Configuring Data Access on page 4-5.*
8.4.3 System Certificate Management Commands

AP5131>admin(system)>cmgr

Description:
Displays the Certificate Manager submenu. The items available under this command include:

genreq      Generates a Certificate Request.
delsef      Deletes a Self Certificate.
loadself    Loads a Self Certificate signed by CA.
listself    Lists the self certificate loaded.
loadca      Loads trusted certificate from CA.
delca       Deletes the trusted certificate.
listca      Lists the trusted certificate loaded.
showreq     Displays a certificate request in PEM format.
delprivkey  Deletes the private key.
listprivkey Lists names of private keys.
impcert     Imports the target certificate file.
..           Goes to the parent menu.
/            Goes to the root menu.
save        Saves the configuration to system flash.
quit         Quits the CLI.
**AP5131>admin(system.cmgr)> genreq**

**Description:**
Generates a certificate request.

**Syntax:**

```
<table>
<thead>
<tr>
<th>genreq</th>
<th>&lt;IDname&gt;</th>
<th>&lt;Subject&gt;</th>
<th>[ -ou &lt;OrgUnit&gt;]</th>
<th>[ -on &lt;OrgName&gt;]</th>
<th>[ -cn &lt;City&gt;]</th>
<th>[ -st &lt;State&gt;]</th>
<th>. . .</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[-sa &lt;SAalgo&gt;]</td>
</tr>
</tbody>
</table>

Generates a self-certificate request for a Certification Authority (CA), where:

- `<IDname>` The private key ID Name (up to 7 chars)
- `<Subject>` Subject Name (up to 49 chars)
- `-ou <OrgUnit>` Organization Unit (up to 49 chars)
- `-on <OrgName>` Organization Name (up to 49 chars)
- `-cn <City>` City Name of Organization (up to 49 chars)
- `-st <State>` State Name (up to 49 chars)
- `-p <PostCode>` Postal code (9 digits)
- `-cc <CCode>` Country code (2 chars)
- `-e <Email>` E-mail Address (up to 49 chars)
- `-d <Domain>` Domain Name (up to 49 chars)
- `-i <IP>` IP Address (a.b.c.d)
- `-sa <SAalgo>` Signature Algorithm (one of MD5-RSA, SHA1-RSA, or SHA1-DSS)
- `-k <KSize>` Key size in bits (one of 512, 1024, or 2048)
```

**Note:** The parameters in [square brackets] are optional. Check with the CA to determine what fields are necessary. For example, most CAs require an email address and an IP address, but not the address of the organization.

**Example:**

```
admin(system.cmgr)> genreq MyCert2 MySubject -ou MyDept -on MyCompany

Please wait. It may take some time...
Generating the certificate request
Retrieving the certificate request
The certificate request is

-----BEGIN CERTIFICATE REQUEST-----
MIHzM1GeAgEAMDkxExjAQBgNVBAoTCU15Q29tcGFueTEPA0GA1UECwMTcGZ1EZXB0
MRkwEAYDVQQDEw1Nym1Y3QwXDA1NBygkqkhkiG9w0BQExFAANLADBIAkEAtKcX
p1KFCFAJymTFx71yuxY1fdS7UEhKjsH7pdqnJnsASK6ZQGAqerjpRScWV1mzYn4
1q2+mgNcvaZU1Io7wIDAQABoAAwDQYJKoZIhvcNAQEEBQADQCCCl5LHdbGC1f
Bj8AszttSo/bA4dcX3vHvhhJcmuuWO9LHS2imPA3xhX/d6+Q1SMbs+tG4RP0lRSr
iWDyuww

-----END CERTIFICATE REQUEST-----
```

For information on configuring certificate management settings using the applet (GUI), see Managing Certificate Authority (CA) Certificates on page 4-8.
AP5131>admin(system.cmgr)> delself

**Description:**
Deletes a self certificate.

**Syntax:**

\[
\text{delsel} \quad \text{<IDname>} \quad \text{Deletes the self certificate named <IDname>}. \\
\]

**Example:**

\[
\text{admin(system.cmgr)}>\text{delsel MyCert2} \\
\]

For information on configuring self certificate settings using the applet (GUI), see *Creating Self Certificates on page 4-9.*
AP5131>admin(system.cmgr)> loadself

**Description:**
Loads a self certificate signed by the Certificate Authority.

**Syntax:**

```
loadself  <IDname>  Load the self certificate signed by the CA with name <IDname>.
```

For information on configuring self certificate settings using the applet (GUI), see *Creating Self Certificates on page 4-9*. 

AP5131>admin(system.cmgr)> listself

**Description:**
Lists the loaded self certificates.

**Syntax:**

```
listself          Lists all self certificates that are loaded.
```

For information on configuring self certificate settings using the applet (GUI), see *Creating Self Certificates on page 4-9*. 
**AP5131>admin(system.cmgr)> loadca**

**Description:**
Loads a trusted certificate from the Certificate Authority.

**Syntax:**

```
loadca
```

Loads the trusted certificate (in PEM format) that is pasted into the command line.

For information on configuring certificate settings using the applet (GUI), see *Importing a CA Certificate on page 4-8*. 


AP5131>admin(system.cmgr)> delca

Description:
Deletes a trusted certificate.

Syntax:

`delca <IDname>` Deletes the trusted certificate.

For information on configuring certificate settings using the applet (GUI), see Importing a CA Certificate on page 4-8.
AP5131>admin(system.cmgr)> listca

Description:
Lists the loaded trusted certificate.

Syntax:

listca          Lists the loaded trusted certificates.

For information on configuring certificate settings using the applet (GUI), see *Importing a CA Certificate on page 4-8.*
AP5131>admin(system.cmgr)> showreq

**Description:**
Displays a certificate request in PEM format.

**Syntax:**
```
showreq <IDname>
```
Displays a certificate request named `<IDname>` generated from the `genreq` command.

For information on configuring certificate settings using the applet (GUI), see *Importing a CA Certificate on page 4-8.*
**AP5131>admin(system.cmgr)> delprivkey**

**Description:**
Deletes a private key.

**Syntax:**

```
delprivkey <IDname>  Deletes private key named <IDname>.
```

For information on configuring certificate settings using the applet (GUI), see *Creating Self Certificates on page 4-9*. 
AP5131>admin(system.cmgr)> listprivkey

Description:
Lists the names of private keys.

Syntax:

listprivkey  Lists all private keys.

For information on configuring certificate settings using the applet (GUI), see Importing a CA Certificate on page 4-8.
8.4.4 System SNMP Commands

AP5131>admin(system)> snmp

Description:
Displays the SNMP submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>Goes to the SNMP access submenu.</td>
</tr>
<tr>
<td>traps</td>
<td>Goes to the SNMP traps submenu.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>


8.4.4.1 System SNMP Access Commands

AP5131>admin(system.snmp.access)

Description:
Displays the SNMP Access menu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Shows SNMP v3 engine ID.</td>
</tr>
<tr>
<td>add</td>
<td>Adds SNMP access entries.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes SNMP access entries.</td>
</tr>
<tr>
<td>list</td>
<td>Lists SNMP access entries.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>
AP5131>admin(system.snmp.access)> show

Description:
Shows the SNMP v3 engine ID.

Syntax:

show eid  Shows the SNMP v3 Engine ID.

Example:

admin(system.snmp.access)>show eid

AP-5131  snmp v3 engine id  : 000001846B8B4567F871AC68

admin(system.snmp.access)>

For information on configuring SNMP access settings using the applet (GUI), see Configuring SNMP Access Control on page 4-17.
**AP5131>admin(system.snmp.access)> add**

**Description:**
Adds SNMP access entries for specific v1v2 and v3 user definitions.

**Syntax:**

```plaintext
add acl <ip1> <ip2>     Adds an entry to the SNMP access control list with <ip1> as the starting IP address and <ip2> as the ending IP address.

v1v2c <comm> <access> <oid>

v3 <user> <access> <oid> <sec>
        <auth> <pass1> <priv> <pass2>
```

v1v2c: Adds an SNMP v1/v2c configuration with <comm> as the community (1-31 characters), the read/write access set to ro (read only) or rw (read/write), and the Object Identifier <oid> (a string of 1-127 numbers separated by dot, such as 2.3.4.5.6).

v3: Adds an SNMP v3 user definition with the username <user> (1 to 31 characters), access set to ro (read only) or rw (read/write), the object ID set to <oid> (1 to 127 chars in dot notation, such as 1.3.6.1), the security type <sec> set to one of none, auth, or auth/priv.

The following parameters must be specified if <sec> is not none:
- Authentication type <auth> set to md5 or sha1
- Authentication password <pass1> (8 to 31 chars)

The following parameters must be specified if <sec> is set to auth/priv:
- Privacy algorithm set to des or aes
- Privacy password <pass2> (8 to 31 chars)

For information on configuring SNMP access settings using the applet (GUI), see *Configuring SNMP Access Control on page 4-17.*
AP5131>admin(system.snmp.access)> delete

Description:
Deletes SNMP access entries for specific v1v2 and v3 user definitions.

Syntax:

```
delete acl <idx>       Deletes entry <idx> from the access control list.
delete acl all         Deletes all entries from the access control list.

v1v2c <idx>           Deletes entry <idx> from the v1/v2 configuration list.
v1v2c all              Deletes all entries from the v1/v2 configuration list.

v3 <idx>              Deletes entry <idx> from the v3 user definition list.
v3 all                Deletes all entries from the v3 user definition list.
```

Example:

```
admin(system.snmp.access)>list acl
---------------------------------------------------------------------
index  start ip  end ip
---------------------------------------------------------------------
1  209.236.24.1  209.236.24.46

admin(system.snmp.access)>delete acl all
admin(system.snmp.access)>list acl
---------------------------------------------------------------------
index  start ip  end ip
---------------------------------------------------------------------
```

For information on configuring SNMP access settings using the applet (GUI), see Configuring SNMP Access Control on page 4-17.
AP5131>admin(system.snmp.access)> list

Description:
Lists SNMP access entries.

Syntax:

```
list acl         Lists SNMP access control list entries.
v1v2c           Lists SNMP v1/v2c configuration.
v3 <idx>        Lists SNMP v3 user definition with index <idx>.
all             Lists all SNMP v3 user definitions.
```

Example:

```
admin(system.snmp.access)>list acl
---------------------------------------------
index  start ip     end ip
---------------------------------------------
1  209.236.24.1     209.236.24.46

admin(system.snmp.access)>list v1v2
---------------------------------------------
index  community  access  oid
---------------------------------------------
1   public       read only     1.3.6.1
2   private      read/write   1.3.6.1

admin(system.snmp.access)>list v3 2

index  username  access permission  object identifier  security level  auth algorithm  auth password  privacy algorithm  privacy password
1          judy      read/write           1.3.6.1              auth/priv          md5              ********       des               ********
```

For information on configuring SNMP access settings using the applet (GUI), see Configuring SNMP Access Control on page 4-17.
8.4.4.2 System SNMP Traps Commands

AP5131>admin(system.snmp.traps)

Description:
Displays the SNMP traps submenu. The items available under this command are shown below.

- **show**: Shows SNMP trap parameters.
- **set**: Sets SNMP trap parameters.
- **add**: Adds SNMP trap entries.
- **delete**: Deletes SNMP trap entries.
- **list**: Lists SNMP trap entries.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
AP5131>admin(system.snmp.traps)> show

Description:
Shows SNMP trap parameters.

Syntax:

```
show trap
rate-trap
```

Shows SNMP trap parameter settings.

```
show rate-trap
```

Shows SNMP rate-trap parameter settings.

Example:

```
admin(system.snmp.traps)>show trap
```

**SNMP MU Traps**

- `mu associated`: enable
- `mu unassociated`: disable
- `mu denied association`: disable
- `mu denied authentication`: disable

**SNMP Traps**

- `snmp auth failure`: disable
- `snmp acl violation`: disable

**SNMP Network Traps**

- `physical port status change`: enable
- `denial of service`: enable
- `denial of service trap rate limit`: 10

**SNMP System Traps**

- `system cold start`: disable
- `system config changed`: disable
- `rogue ap detection`: disable
- `ap radar detection`: disable

For information on configuring SNMP traps using the applet (GUI), see *Enabling SNMP Traps on page 4-19.*
AP5131>admin(system.snmp.traps)> set

**Description:**
Sets SNMP trap parameters.

**Syntax:**

```
set mu-assoc enable/disable
mu-unassoc enable/disable
mu-deny-assoc enable/disable
mu-deny-auth enable/disable
snmp-auth enable/disable
snmp-acl enable/disable
port enable/disable
dos-attack enable/disable
interval <rate>
cold enable/disable
cfg enable/disable
rogue-ap enable/disable
ap-radar enable/disable

rate <rate> <scope> <value>

min-pkt <pkt>
```

Sets the particular <rate> to monitor to <value> given the indicated <scope>. See table below for information on the possible values for <rate>, <scope>, and <value>. Sets the minimum number of packets required for rate traps to fire (1-65535).

<table>
<thead>
<tr>
<th>Choices &lt;rate&gt;</th>
<th>Interpretation</th>
<th>Allowed Range for &lt;value&gt;</th>
<th>Allowed &lt;scope&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>pkts</td>
<td>Packets/second &gt; &lt;value&gt;</td>
<td>0-9999.99</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>mbps</td>
<td>Throughput &gt; &lt;value&gt;</td>
<td>0-108.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>avg-bps</td>
<td>Average bit speed in mbps &lt; &lt;value&gt;</td>
<td>0-108.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>pct-ru</td>
<td>% not UNICAST &gt; &lt;value&gt;</td>
<td>0-100.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>avg-signal</td>
<td>Negative average signal &lt; &lt;value&gt;</td>
<td>0-100.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>avg-retries</td>
<td>Average retries &gt; &lt;value&gt;</td>
<td>0-16.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>pct-dropped</td>
<td>% dropped packets &gt; &lt;value&gt;</td>
<td>0-100.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>pct-ndecrypt</td>
<td>% undecryptable &gt; &lt;value&gt;</td>
<td>0-100.00</td>
<td>wlan,ap,du</td>
</tr>
<tr>
<td>assoc-mus</td>
<td>Number of associated MUs &gt; &lt;value&gt;</td>
<td>0-200</td>
<td>wlan,ap,du</td>
</tr>
</tbody>
</table>

**Note:** <value> can be a number with up to two decimal places, except for assoc-mus, which must be an integer.

For information on configuring SNMP traps using the applet (GUI), see Configuring Specific SNMP Traps on page 4-22.
AP5131>admin(system.snmp.traps)> add

Description:
Adds SNMP trap entries.

Syntax:

```plaintext
add v1v2  <ip>  <port>  <comm>  <ver>
Add an entry to the SNMP v1/v2 access list with the destination IP address set to <ip>, the destination UDP port set to <port>, the community string set to <comm> (1 to 31 characters), and the SNMP version set to <ver>.

v3  <ip>  <port>  <user>  <sec>  <auth>  <pass1>  <priv>  <pass2>
Add an entry to the SNMP v3 access list with the destination IP address set to <ip>, the destination UDP port set to <port>, the username set to <user> (1 to 31 characters), and the authentication type set to one of none, auth, or auth/prv.

The following parameters must be specified if <sec> is not none:
  Authentication type <auth> set to md5 or sha1
  Authentication password <pass1> (8 to 31 chars)

The following parameters must be specified if <sec> is set to auth/prv:
  Privacy algorithm set to des or aes
  Privacy password <pass2> (8 to 31 chars)
```

Example:

```plaintext
admin(system.snmp.traps)>add v1v2 203.223.24.2 333 mycomm v1
admin(system.snmp.traps)>list v1v2c

<table>
<thead>
<tr>
<th>index</th>
<th>dest ip</th>
<th>dest port</th>
<th>community</th>
<th>version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>203.223.24.2</td>
<td>333</td>
<td>mycomm</td>
<td>v1</td>
</tr>
</tbody>
</table>

admin(system.snmp.traps)>add v3 201.232.24.33 555 BigBoss none md5
admin(system.snmp.traps)>list v3 all

index : 1
destination ip : 201.232.24.33
destination port : 555
username : BigBoss
security level : none
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ********
```

For information on configuring SNMP traps using the applet (GUI), see Configuring SNMP RF Trap Thresholds on page 4-24.
AP5131>admin(system.snmp.traps)> delete

Description:
Deletes SNMP trap entries.

Syntax:

```
delete v1v2c <idx> Deletes entry <idx> from the v1v2c access control list.
   all Deletes all entries from the v1v2c access control list.
   v3 <idx> Deletes entry <idx> from the v3 access control list.
   all Deletes all entries from the v3 access control list.
```

Example:

```
admin(system.snmp.traps)>delete v1v2 all
```

For information on configuring SNMP traps using the applet (GUI), see Configuring SNMP Settings on page 4-11.
AP5131>admin(system.snmp.traps)> list

Description:
Lists SNMP trap entries.

Syntax:

<table>
<thead>
<tr>
<th>list</th>
<th>v1v2c</th>
<th>Lists SNMP v1/v2c access entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>v3</td>
<td>&lt;idx&gt;</td>
<td>Lists SNMP v3 access entry &lt;idx&gt;.</td>
</tr>
<tr>
<td>all</td>
<td></td>
<td>Lists all SNMP v3 access entries.</td>
</tr>
</tbody>
</table>

Example:

admin(system.snmp.traps)>add v1v2 203.223.24.2 162 mycomm v1
admin(system.snmp.traps)>list v1v2c

<table>
<thead>
<tr>
<th>index</th>
<th>dest ip</th>
<th>dest port</th>
<th>community</th>
<th>version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>203.223.24.2</td>
<td>162</td>
<td>mycomm</td>
<td>v1</td>
</tr>
</tbody>
</table>

admin(system.snmp.traps)>add v3 201.232.24.33 555 BigBoss none md5
admin(system.snmp.traps)>list v3 all

index : 1
destination ip : 201.232.24.33
destination port : 555
username : BigBoss
security level : none
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ********

For information on configuring SNMP traps using the applet (GUI), see Configuring SNMP RF Trap Thresholds on page 4-24.
8.4.5 System Network Time Protocol (NTP) Commands

AP5131>admin(system)> ntp

Description:
Displays the NTP menu. The correct network time is required for numerous functions to be configured accurately on the AP-5131.

Syntax:
- show
  - Shows NTP parameters settings.
- set
  - Sets NTP parameters.
- ..
  - Goes to the parent menu.
- /
  - Goes to the root menu.
- save
  - Saves the configuration to system flash.
- quit
  - Quits the CLI.
P5131>admin(system.ntp)> show

Description:
Displays the NTP server configuration.

Syntax:

show

Shows all NTP server settings.

Example:

admin(system.ntp)> show

current time (UTC) : 2005-08-31 14:35:20
ntp mode : enable
preferred server ip : 203.21.37.18
preferred server port : 123
first alternate server ip : 203.21.37.19
first alternate server port : 123
second alternate server ip : 0.0.0.0
second alternate server port : 123
synchronization interval : 15 minutes

For information on configuring NTP using the applet (GUI), see Configuring Network Time Protocol (NTP) on page 4-26.
**AP5131>admin(system.ntp)> set**

**Description:**
Sets NTP parameters for AP-5131 clock synchronization.

**Syntax:**

```
set mode   <ntp-mode>          Enables or disables NTP.
server    <idx> <ip>           Sets the NTP server IP address.
port       <idx> <port>        Defines the port number.
intrvl    <period>             Defines the clock synchronization interval used between the AP-5131 and the NTP server in minutes (15 - 65535).
```

**Example:**

```
admin(system.ntp)>set mode enable
admin(system.ntp)>set server 203.21.37.18
admin(system.ntp)>set port 1 123
admin(system.ntp)>set intrvl 15
```

For information on configuring NTP using the applet (GUI), see *Configuring Network Time Protocol (NTP) on page 4-26*. 
### 8.4.6 System Log Commands

**AP5131>admin(system)> logs**

**Description:**
Displays the AP-5131 log submenu. Logging options include:

**Syntax:**

- **show**
  - Shows logging options.
- **set**
  - Sets log options and parameters.
- **view**
  - Views system log.
- **delete**
  - Deletes the system log.
- **send**
  - Sends log to the designated FTP Server.
- **..**
  - Goes to the parent menu.
- **/**
  - Goes to the root menu.
- **save**
  - Saves configuration to system flash.
- **quit**
  - Quits the CLI.
AP5131>admin(system.logs)> show

Description:
Displays the current AP-5131 logging settings.

Syntax:

`show` Displays the logging options.

Example:

```
admin(system.logs)> show

log level : L6 Info
syslog server logging : enable
syslog server ip address : 192.168.0.102
ftp/tftp server address : 192.168.0.101
ftp user name : tealtown
ftp password : ********
```

For information on configuring logging settings using the applet (GUI), see Logging Configuration on page 4-28.
**AP5131>admin(system.logs)> set**

**Description:**
Sets log options and parameters.

**Syntax:**

```
set level <level>  
```

Sets the level of the events that will be logged. All events with a level at or above `<level>` (L0-L7) will be saved to the system log.

- L0: Emergency
- L1: Alert
- L2: Critical
- L3: Errors
- L4: Warning
- L5: Notice
- L6: Info (default setting)
- L7: Debug

```
mode <mode>  
ipadr <ip>  
server <a.b.c.d>  
user <username>  
passwd <password>  
```

- Enables or disables syslog server logging.
- Sets the external syslog server IP address to `<ip>` (a.b.c.d).
- Sets the FTP server IP address.
- Sets the FTP user name (1-39 characters).
- Sets the FTP password (1-39 characters).

For information on configuring logging settings using the applet (GUI), see *Logging Configuration on page 4-28.*
**AP5131>admin(system.logs)> view**

**Description:**
Displays the AP-5131 system log file.

**Syntax:**

`view` Displays the entire AP-5131 system log file.

**Example:**

```
Jan  7 16:14:00 (none) syslogd 1.4.1: restart (remote reception).
Jan  7 16:14:10 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:15:43 (none) last message repeated 2 times
Jan  7 16:16:01 (none) CC:  4:16pm  up 6 days, 16:16, load average: 0.00, 0.01, 0.00
Jan  7 16:16:01 (none) CC: Mem:  62384  32520  29864
Jan  7 16:16:01 (none) CC: 0000077e  0012e95b 0000d843 00000000 00000003 0000121e 000034dc 00000000 00000000 00000000
Jan  7 16:16:01 (none) CC:  Mem:  62384  32520  29864
Jan  7 16:16:01 (none) CC: 0000077e  0012e95b 0000d843 00000000 00000003 0000121e 000034dc 00000000 00000000 00000000
Jan  7 16:16:01 (none) CC:  Mem:  62384  32520  29864
Jan  7 16:16:01 (none) CC: 0000077e  0012e95b 0000d843 00000000 00000003 0000121e 000034dc 00000000 00000000 00000000
Jan  7 16:17:15 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:17:15 (none) klogd: :ps log:fc: queue maintenance
```

For information on configuring logging settings using the applet (GUI), see *Logging Configuration on page 4-28*. 
**AP5131>admin(system.logs)> delete**

**Description:**
Deletes the log files.

**Syntax:**
```
delte
```
Deletes the AP-5131 system log file.

**Example:**
```
admin(system.logs)>delete
```

For information on configuring logging settings using the applet (GUI), see *Logging Configuration on page 4-28*. 
**AP5131>admin(system.logs)> send**

**Description:**
Sends log and core file to an FTP Server.

**Syntax:**

```
send
```

Sends the system log file via FTP to a location specified with the set command. Use the set command to set the FTP login and site information.

**Example:**

```
admin(system.logs)> send

File transfer   : [ In progress ]

File transfer   : [ Done ]

admin(system.logs)>
```

For information on configuring logging settings using the applet (GUI), see *Logging Configuration on page 4-28.*
8.4.7 System Configuration-Update Commands

AP5131>admin(system.cfg-update)>

Description:
Displays the AP-5131 configuration update submenu.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Restores the default AP-5131 configuration.</td>
</tr>
<tr>
<td>partial</td>
<td>Restores a partial default AP-5131 configuration.</td>
</tr>
<tr>
<td>show</td>
<td>Shows import/export parameters.</td>
</tr>
<tr>
<td>set</td>
<td>Sets import/export AP-5131 configuration parameters.</td>
</tr>
<tr>
<td>export</td>
<td>Exports AP-5131 configuration to a designated system.</td>
</tr>
<tr>
<td>import</td>
<td>Imports configuration to the AP-5131.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to AP-5131 system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
</tbody>
</table>
AP5131>admin(system.cfg-update)> default

Description:
Restores the full AP-5131 factory default configuration.

Syntax:

default        Restores the AP-5131 to the original (factory) configuration.

Example:

admin(system.cfg-update)> default

Are you sure you want to default the configuration? <yes/no>:

For information on importing/exporting AP-5131 configurations using the applet (GUI), see Importing/Exporting Configurations on page 4-30.
AP5131>admin(system.cfg-update)> partial

Description:
Restores a partial factory default configuration. The AP-5131’s LAN, WAN and SNMP settings are unaffected by the partial restore.

Syntax:

default Restores a partial AP-5131 configuration.

Example:

    admin(system.cfg-update)>partial

    Are you sure you want to partially default the AP5131? <yes/no>:

For information on importing/exporting AP-5131 configurations using the applet (GUI), see Importing/Exporting Configurations on page 4-30.
AP5131>admin(system.cfg-update)> show

Description:
Displays import/export parameters for the AP-5131 configuration file.

Syntax:

show           Shows all import/export parameters.

Example:

    admin(system.cfg-update)> show

    **cfg filename**             :    cfg.txt
    **ftp/tftp server ip address** :    192.168.0.101
    **ftp user name**             :    myadmin
    **ftp password**              :    *******

For information on importing/exporting AP-5131 configurations using the applet (GUI), see Importing/Exporting Configurations on page 4-30.
**AP5131>admin(system.cfg-update)> set**

**Description:**
Sets the import/export parameters.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the configuration file name (1 to 39 characters in length).</td>
</tr>
<tr>
<td>file</td>
<td>Defines the path used for the configuration file upload.</td>
</tr>
<tr>
<td>path</td>
<td>Sets the FTP/TFTP server IP address.</td>
</tr>
<tr>
<td>server</td>
<td>Sets the FTP user name (1 to 39 characters in length).</td>
</tr>
<tr>
<td>user</td>
<td>Sets the FTP password (1 to 39 characters in length).</td>
</tr>
<tr>
<td>passwd</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
admin(system.cfg-update)>set server 192.168.22.12
admin(system.cfg-update)>set user myadmin
admin(system.cfg-update)>set passwd georges
```

```
admin(system.cfg-update)>show

cfg filename : cfg.txt
ftp/tftp server ip address : 192.168.22.12
ftp user name : myadmin
ftp password : ******
```

For information on importing/exporting AP-5131 configurations using the applet (GUI), see *Importing/Exporting Configurations on page 4-30.*
AP5131>admin(system.cfg-update)> export

Description:
Exports the configuration from the system.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export ftp</td>
<td>Exports the AP-5131 configuration to the FTP server. Use the set command to set the server, user, password, and file name before using this command.</td>
</tr>
<tr>
<td>tftp</td>
<td>Exports the AP-5131 configuration to the TFTP server. Use the set command to set the IP address for the TFTP server before using the command.</td>
</tr>
<tr>
<td>terminal</td>
<td>Exports the AP-5131 configuration to a terminal.</td>
</tr>
</tbody>
</table>

Example:

Export FTP Example:
```
admin(system.cfg-update)>set server 192.168.22.12
admin(system.cfg-update)>set user myadmin
admin(system.cfg-update)>set passwd

admin(system.cfg-update)>export ftp

Export operation : [ Started ]
Building configuration file : [ Done ]
File transfer : [ In progress ]
File transfer : [ Done ]
Export operation : [ Done ]
```

Export TFTP Example:
```
admin(system.cfg-update)>set server 192.168.0.101
admin(system.cfg-update)>export tftp

Export operation : [ Started ]
Building configuration file : [ Done ]
File transfer : [ In progress ]
File transfer : [ Done ]
Export operation : [ Done ]
```

For information on importing/exporting AP-5131 configurations using the applet (GUI), see Importing/Exporting Configurations on page 4-30.
**AP5131>admin(system.cfg-update)> import**

**Description:**
Imports the AP-5131 configuration to the AP-5131.

**Syntax:**
- `import ftp` Imports the AP-5131 configuration file from the FTP server. Use the set command to set the server, user, password, and file.
- `tftp` Imports the AP-5131 configuration from the TFTP server. Use the set command to set the server and file.

**Example:**
Import FTP Example

```plaintext
admin(system.cfg-update)>set server 192.168.22.12
admin(system.cfg-update)>set user myadmin
admin(system.cfg-update)>set passwd mysecret
admin(system.cfg-update)>import ftp
Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
```

Import TFTP Example

```plaintext
admin(system.cfg-update)>set server 192.168.0.101
admin(system.cfg-update)>import tftp
Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
```

For information on importing/exporting AP-5131 configurations using the applet (GUI), see *Importing/Exporting Configurations on page 4-30.*
8.4.8 Firmware Update Commands

AP5131>admin(system)>fw-update

Description:
Displays the firmware update submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays the current AP-5131 firmware update settings.</td>
</tr>
<tr>
<td>set</td>
<td>Defines the AP-5131 firmware update parameters.</td>
</tr>
<tr>
<td>update</td>
<td>Executes the firmware update.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the current configuration to the AP-5131 system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI and exits the current session.</td>
</tr>
</tbody>
</table>
AP5131>admin(system.fw-update)>show

Description:
Displays the current AP-5131 firmware update settings.

Syntax:
show

Example:

admin(system.fw-update)>show

    automatic firmware upgrade       : enable
    automatic config upgrade         : LAN

    firmware filename                : APFW.bin
    firmware path                    : /tftpboot/
    ftp/tftp server ip address       : 168.197.2.2
    ftp user name                    : pkeegan
    ftp password                    : *******

For information on updating AP-5131 device firmware using the applet (GUI), see Updating Device Firmware on page 4-34.
**AP5131>admin(system.fw-update)>set**

**Description:**
Defines AP-5131 firmware update settings and user permissions.

**Syntax:**

```
set fw-auto <mode> When enabled, updates device firmware each time the firmware versions are found to be different between the AP-5131 and the specified firmware on the remote system.

cfg-auto <mode> When enabled, updates device configuration file each time the config file versions are found to be different between the AP-5131 and the specified LAN or WAN interface.

iface <wan/lan> Defines the target interface for version updates if the fw-auto and/or cfg-auto options are enabled.

define <name> Defines the firmware file name.

define <path> Specifies a path for the file.

define <ip> The IP address for the FTP/TFTP server used for the firmware and/or config file update.

define <name> Specifies a username for FTP server login.

define <password> Specifies a password for FTP server login. Default is symbol.
```

For information on updating AP-5131 device firmware using the applet (GUI), see *Updating Device Firmware on page 4-34.*
AP5131>admin(system.fw-update)>update

Description:
Executes the AP-5131 firmware update over the WAN or LAN port using either ftp or tftp.

Syntax:

update <mode><iface>  Defines the ftp or tftp mode used to conduct the firmware update. Specifies whether the update is executed over the AP-5131's WAN or LAN interface <iface>.

For information on updating AP-5131 device firmware using the applet (GUI), see Updating Device Firmware on page 4-34.
8.4.9 System Test Commands

AP5131>admin(system.test)>

Description:
Displays the AP-5131 test submenu. The items available under this command include:

- **show**: Displays the AP-5131 test options.
- **set**: Defines the parameters of an AP-5131 system test.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
- **save**: Saves the current configuration to the AP-5131 system flash.
- **quit**: Quits the CLI and exits the current session.
AP5131> admin(system.test)> show

Description:
Displays the AP-5131 test options.

Syntax:

show  Displays the AP-5131 test options.

Example:

admin(system.test)> show

    half fc windows for ap100 val : [ 0x0000 ........ .......0]
    broadcast in psp val       : [ 0x0000 ........ ......1.]
    drop bc pre wep val        : [ 0x0000 ........ .....1..]
    wpa2 tkip disabled val     : [ 0x0000 ........ ....0...]
    wireless disable val       : [ 0x0000 ........ ...0....]
    psp fix more data val      : [ 0x0000 ........ ..0.....]
    wpa2 tkip disabled val     : [ 0x0000 ........ .1......]
    wpa ie before rsn ie val   : [ 0x0000 ........ 0.......
    disable wpa countermeasures val : [ 0x0000 .......0 ........

    int1     : 0x46
    int2     : 0x0
    int3     : 0x0
    int4     : 0x0
    str1
    str2
    str3
    str4
    evtlog   : disabled

    admin(system.test)>
**AP5131>admin(system.test)> set**

**Description:**
Defines the parameters of an AP-5131 system test. These commands are recommended for qualified technicians only.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set flow</td>
<td>&lt;mode&gt;</td>
<td>enable/disable Enables or disables flow control for the AP-5131.</td>
</tr>
<tr>
<td>hbt</td>
<td>&lt;mode&gt;</td>
<td>enable/disable Enables or disables heartbeat mode for the AP-5131.</td>
</tr>
<tr>
<td>wd</td>
<td>&lt;mode&gt;</td>
<td>enable/disable Enables or disables the wireless disable val option for the AP-5131.</td>
</tr>
<tr>
<td>pmd</td>
<td>&lt;mode&gt;</td>
<td>enable/disable Defines a fix psp more data enable val settings as enabled or disabled.</td>
</tr>
<tr>
<td>rs</td>
<td>&lt;mode&gt;</td>
<td>enable/disable Enables or disables the AP-5131 rate scale test setting.</td>
</tr>
<tr>
<td>int1</td>
<td>&lt;value&gt;</td>
<td>Defines integer 1. For example 0x1234.</td>
</tr>
<tr>
<td>int2</td>
<td>&lt;value&gt;</td>
<td>Defines integer 2. For example 0x1234.</td>
</tr>
<tr>
<td>int3</td>
<td>&lt;value&gt;</td>
<td>Defines integer 3. For example 0x1234.</td>
</tr>
<tr>
<td>int</td>
<td>&lt;value&gt;</td>
<td>Defines integer 4. For example 0x1234.</td>
</tr>
<tr>
<td>str1</td>
<td>&lt;value&gt;</td>
<td>String is 1 through 39 characters in length.</td>
</tr>
<tr>
<td>str2</td>
<td>&lt;value&gt;</td>
<td>String is 1 through 39 characters in length.</td>
</tr>
<tr>
<td>str3</td>
<td>&lt;value&gt;</td>
<td>String is 1 through 39 characters in length.</td>
</tr>
<tr>
<td>str4</td>
<td>&lt;value&gt;</td>
<td>String is 1 through 39 characters in length.</td>
</tr>
</tbody>
</table>
8.5 Statistics Commands

AP5131>admin(stats)

Description:
Displays the AP-5131 statistics submenu. The items available under this command are:

- **show**: Displays AP-5131 WLAN, MU, LAN and WAN statistics.
- **send-cfg**: Sends a config file to all AP-5131's within the known AP table.
- **clear**: Clears all statistic counters to zero.
- **flash-all-leds**: Starts and stops the flashing of all AP-5131 LEDs.
- **echo**: Defines the parameters for pinging a designated station.
- **ping**: Initiates a ping test.
- `..`: Moves to the parent menu.
- `/`: Goes to the root menu.
- **save**: Saves the current configuration to system flash.
- **quit**: Quits the CLI.
**AP5131>admin(stats)> show**

**Description:**
Displays AP-5131 system information.

**Syntax:**

```
show  
  wan  Displays stats for the AP-5131 WAN port.  
  lan  Displays stats for the AP-5131 LAN port  
  wlan Displays WLAN status and statistics summary.  
  s-wlan Displays status and statistics for an individual WLAN  
  radio Displays a radio statistics transmit and receive summary.  
  mu Displays all mobile unit (MU) status.  
  s-mu Displays status and statistics for an individual MU.  
  known-ap Displays a Known AP summary.  
```

**Example:**
```
admin(stats)>show wlan

Index  : 1
Name   : Front Lobby
Status : Enabled

Index  : 2
Name   : 1st Floor
Status : Disabled

Index  : 3
Name   : Office
Status : Disabled
```

```
admin(stats)>show known-ap
```

For information on displaying LAN port statistics using the applet (GUI), see Viewing LAN Statistics on page 7-5.

For information on displaying WAN port statistics using the applet (GUI), see Viewing WAN Statistics on page 7-2.

For information on displaying Wireless statistics using the applet (GUI), see Viewing Wireless Statistics on page 7-8.

For information on displaying individual WLAN statistics using the applet (GUI), see Viewing WLAN Statistics on page 7-10.
**AP5131>admin(stats)> send-cfg**

**Description:**
Copies the AP-5131’s configuration to the AP-5131s within the known AP table.

**Syntax:**
```
(send-cfg)
```
Copies the AP-5131’s configuration to the AP-5131s within the known AP table

**Example:**
```
admin(stats)>send-cfg
admin(stats)>
```

For information on copying the AP-5131 config to another AP-5131 with the same ESSID using the applet (GUI), see [Viewing Known Access Point Statistics on page 7-26](#).
**AP5131>admin(stats)> clear**

**Description:**
Clears the specified statistics counters to zero to begin new data calculations.

**Syntax:**

<table>
<thead>
<tr>
<th>clear</th>
<th>wan</th>
<th>Clears WAN statistics counters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>lan</td>
<td>Clears LAN statistics counters.</td>
</tr>
<tr>
<td></td>
<td>rf</td>
<td>Clears all RF data.</td>
</tr>
<tr>
<td>all-wlan</td>
<td></td>
<td>Clears all WLAN summary information.</td>
</tr>
<tr>
<td>wlan</td>
<td></td>
<td>Clears individual WLAN statistic counters.</td>
</tr>
<tr>
<td>all-radio</td>
<td></td>
<td>Clears AP-5131 radio summary information.</td>
</tr>
<tr>
<td>radio1</td>
<td></td>
<td>Clears statistics counters specific to radio1.</td>
</tr>
<tr>
<td>radio2</td>
<td></td>
<td>Clears statistics counters specific to radio2.</td>
</tr>
<tr>
<td>mu</td>
<td></td>
<td>Clears all MU statistic counters</td>
</tr>
<tr>
<td>known-ap</td>
<td></td>
<td>Clears Known AP statistic counters.</td>
</tr>
</tbody>
</table>
AP5131>admin(stats)> flash-all-leds

**Description:**
Starts and stops the illumination of a specified access point’s LEDs.

**Syntax:**

```plaintext
flash-all- leds <index> <stop/start>
```

- `<index>`: Defines the Known AP index number of the target AP to flash.
- `<stop/start>`: Begins or terminates the flash activity.

**Example:**

```
admin(stats)>

admin(stats)> flash-all-leds 1 start
Password ********
admin(stats)> flash-all-leds 1 stop
admin(stats)>
```

For information on flashing AP-5131 LEDs using the applet (GUI), see *Viewing Known Access Point Statistics on page 7-26*. 
**AP5131>admin(stats)> echo**

**Description:**
Defines the echo test values used to conduct a ping test to an associated MU.

**Syntax:**

- **list**: Defines echo test parameters and result.
- **set**: Determines echo test packet data.
- **start**: Begins echoing the defined station.
- **..**: Goes to parent menu.
- **/**: Goes to root menu.
- **quit**: Quits CLI session.

For information on MU Echo and Ping tests using the applet (GUI), see *Pinging Individual MUs on page 7-24.*
AP5131>admin.stats.echo)> list

Description:
Lists echo test parameters and results.

Syntax:
list
Lists echo test parameters and results.

Example:
admin(stats.echo)>list

Station Address : 00A0F8213434
Number of Pings : 10
Packet Length   : 10
Packet Data (in HEX) : 55

Number of MU Responses : 2

admin(stats.echo)>

For information on MU Echo and Ping tests using the applet (GUI), see Pinging Individual MUs on page 7-24.
**AP5131>admin.stats.echo)>set**

**Description:**
Defines the parameters of the echo test.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>station</td>
<td>&lt;mac&gt; Defines MU target MAC address.</td>
</tr>
<tr>
<td></td>
<td>request</td>
<td>&lt;num&gt; Sets number of echo packets to transmit (1-539).</td>
</tr>
<tr>
<td></td>
<td>length</td>
<td>&lt;num&gt; Determines echo packet length in bytes (1-539).</td>
</tr>
<tr>
<td></td>
<td>data</td>
<td>&lt;hex&gt; Defines the particular packet data.</td>
</tr>
</tbody>
</table>

For information on MU Echo and Ping tests using the applet (GUI), see *Pinging Individual MUs on page 7-24.*
AP5131>admin.stats.echo)> start

**Description:**
Initiates the echo test.

**Syntax:**

```
start
```

Initiates the echo test.

**Example:**

```
admin(stats.echo)>start

admin(stats.echo)>list
```

<table>
<thead>
<tr>
<th>Station Address</th>
<th>00A0F843AABB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Pings</td>
<td>10</td>
</tr>
<tr>
<td>Packet Length</td>
<td>100</td>
</tr>
<tr>
<td>Packet Data (in HEX)</td>
<td>1</td>
</tr>
<tr>
<td>Number of MU Responses</td>
<td>2</td>
</tr>
</tbody>
</table>

For information on MU Echo and Ping tests using the applet (GUI), see *Pinging Individual MUs on page 7-24.*
AP5131>admin(stats)> ping

**Description:**

Defines the ping test values used to conduct a ping test to an AP with the same ESSID.

**Syntax:**

- `ping`
- `list`  Defines ping test packet length.
- `set`  Determines ping test packet data.
- `start`  Begins pinging the defined station.
- `..`  Goes to parent menu.
- `/`  Goes to root menu.
- `quit`  Quits CLI session.

For information on Known AP tests using the applet (GUI), see *Pinging Individual MUs on page 7-24.*
AP5131>admin.stats.ping)> list

Description:
Lists ping test parameters and results.

Syntax:
list Lists ping test parameters and results.

Example:

admin(stats.ping)>list

<table>
<thead>
<tr>
<th>Station Address</th>
<th>00A0F8213434</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Pings</td>
<td>10</td>
</tr>
<tr>
<td>Packet Length</td>
<td>10</td>
</tr>
<tr>
<td>Packet Data (in HEX)</td>
<td>55</td>
</tr>
<tr>
<td>Number of AP Responses</td>
<td>2</td>
</tr>
</tbody>
</table>

admin(stats.ping)>

For information on Known AP tests using the applet (GUI), see Pinging Individual MUs on page 7-24.
**AP5131>admin.stats.ping> set**

**Description:**
Defines the parameters of the ping test.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Defines the AP target MAC address.</td>
</tr>
<tr>
<td>request</td>
<td>Sets number of ping packets to transmit (1-539).</td>
</tr>
<tr>
<td>length</td>
<td>Determines ping packet length in bytes (1-539).</td>
</tr>
<tr>
<td>data</td>
<td>Defines the particular packet data.</td>
</tr>
</tbody>
</table>

**Example:**

```
admin(stats.ping)> set station 00A0F843AABB
admin(stats.ping)> set request 10
admin(stats.ping)> set length 100
admin(stats.ping)> set data 1
```

For information on Known AP tests using the applet (GUI), see *Pinging Individual MUs on page 7-24.*
AP5131>admin.stats.echo)> start

Description:
Initiates the ping test.

Syntax:

start 

Initiates the ping test.

Example:

admin(stats.ping)> start

admin(stats.ping)> list

Station Address : 00A0F843AABB
Number of Pings : 10
Packet Length : 100
Packet Data (in HEX) : 1

Number of AP Responses : 2

For information on Known AP tests using the applet (GUI), see Pinging Individual MUs on page 7-24.
Technical Specifications

Technical specifications include specifications in the following areas:

- Physical Characteristics
- Electrical Characteristics
- Radio Characteristics
- Antenna Specifications
- Country Codes

A.1 Physical Characteristics

The AP-5131 has the following physical characteristics:
A.2 Electrical Characteristics

The AP-5131 has the following electrical characteristics:

- **Operating Voltage**: 48Vdc (Nom)
- **Operating Current**: 200mA (Peak) @ 48Vdc
  170mA (Nom) @ 48Vdc
A.3 Radio Characteristics

The AP-5131 has the following radio characteristics:

**Operating Channels**
- 802.11a radio - Channels 1-35 (4920-5825 MHz)
- 802.11b/g radio - Channels 1-13 (2412-2472 MHz)
- 802.11b/g radio - Channel 14 (2484 MHz Japan only)

*Actual operating frequencies depend on regulatory rules and certification agencies.*

**Receiver Sensitivity**

<table>
<thead>
<tr>
<th></th>
<th>802.11a Radio</th>
<th>802.11b/g Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Mbps</td>
<td>-88</td>
<td>11 Mbps -84</td>
</tr>
<tr>
<td>9 Mbps</td>
<td>-87</td>
<td>5.5 Mbps -88</td>
</tr>
<tr>
<td>12 Mbps</td>
<td>-85</td>
<td>2 Mbps -90</td>
</tr>
<tr>
<td>18 Mbps</td>
<td>-81</td>
<td>1 Mbps -94</td>
</tr>
<tr>
<td>24 Mbps</td>
<td>-79</td>
<td></td>
</tr>
<tr>
<td>36 Mbps</td>
<td>-75</td>
<td></td>
</tr>
<tr>
<td>48 Mbps</td>
<td>-70</td>
<td></td>
</tr>
<tr>
<td>54 Mbps</td>
<td>-68</td>
<td></td>
</tr>
</tbody>
</table>

**Radio Data Rates**
- 802.11a radio 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/Sec
- 802.11g radio 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/Sec
- 802.11b radio 1, 2, 5.5, 11 Mbit/Sec

**Wireless Medium**
- Direct Sequence Spread Spectrum (DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

---

A.4 Antenna Specifications

The AP-5131 antenna suite has the following specifications:

---

**CAUTION** Using an antenna other than the Dual-Band Antenna (Part No. ML-2452-APA2-01) could render the AP-5131’s Rogue AP Detector Mode feature inoperable. Contact your Symbol sales associate for specific information.
A.4.1 2.4 GHz Antenna Matrix

The following section describes each 2.4 GHz antenna approved for use with the AP-5131. Below is a table of each of these 2.4 GHz antennas and Symbol’s part number.

<table>
<thead>
<tr>
<th>Symbol Part Number</th>
<th>Antenna Type</th>
<th>Nominal Net Gain (dBi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML-2499-11PNA2-01</td>
<td>Wide Angle Directional</td>
<td>8.5</td>
</tr>
<tr>
<td>ML-2499-HPA3-01</td>
<td>Omni-Directional Antenna</td>
<td>3.3</td>
</tr>
<tr>
<td>ML-2499-BYGA2-01</td>
<td>Yagi Antenna</td>
<td>13.9</td>
</tr>
<tr>
<td>ML-2452-APA2-01</td>
<td>Dual-Band</td>
<td>3.0</td>
</tr>
</tbody>
</table>

A.4.2 5.2 GHz Antenna Matrix

The following section describes each 5.2 GHz antenna approved for use with the AP-5131.

<table>
<thead>
<tr>
<th>Symbol Part Number</th>
<th>Antenna Type</th>
<th>Nominal Net Gain (dBi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML-5299-WPNA1-01</td>
<td>Panel Antenna</td>
<td>13.0</td>
</tr>
<tr>
<td>ML-5299-HPA1-01</td>
<td>Wide-Band Omni-Directional Antenna</td>
<td>5.0</td>
</tr>
<tr>
<td>ML-2452-APA2-01</td>
<td>Dual-Band</td>
<td>4.0</td>
</tr>
</tbody>
</table>

A.4.3 Additional Antenna Components

The following table lists the Symbol part number for various antenna accessories. This table also includes the loss for each accessory at both 2.4 and 5.2 GHz.

<table>
<thead>
<tr>
<th>Item</th>
<th>Symbol Part Number</th>
<th>Description</th>
<th>Loss (db) @ 2.4 GHz</th>
<th>Loss (db) @ 5.2 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>72PJ</td>
<td>ML-1499-72PJ-01</td>
<td>Cable Extension</td>
<td>2.5</td>
<td></td>
</tr>
<tr>
<td>LAK1</td>
<td>ML-1499-LAK1-01</td>
<td>Lightning Arrestor+</td>
<td>0.75</td>
<td></td>
</tr>
<tr>
<td>LAK2</td>
<td>ML-1499-LAK2-01</td>
<td>Lightning Arrestor</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>10JK</td>
<td>ML-1499-10JK-01</td>
<td>Jumper Kit</td>
<td>0.75</td>
<td>1.6</td>
</tr>
<tr>
<td>25JK</td>
<td>ML-1499-25JK-01</td>
<td>Jumper Kit</td>
<td>1.9</td>
<td>3.5</td>
</tr>
</tbody>
</table>
A.4.4 Antenna Accessory Connectors, Cable Type and Length

The following describes each antenna accessory's connector and cable type, plus the length.

<table>
<thead>
<tr>
<th>Item</th>
<th>Symbol Part Number</th>
<th>Description</th>
<th>Loss (db) @ 2.4 GHz</th>
<th>Loss (db) @ 5.2 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>50JK</td>
<td>ML-1499-50JK-01</td>
<td>Jumper Kit</td>
<td>3.75</td>
<td>6.6</td>
</tr>
<tr>
<td>100JK</td>
<td>ML-1499-100JK-01</td>
<td>Jumper Kit</td>
<td>7.5</td>
<td>12.8</td>
</tr>
</tbody>
</table>

A.5 Country Codes

The following list of countries and their country codes is useful when using the AP-5131 configuration file, CLI or the MIB to configure the AP-5131:

<table>
<thead>
<tr>
<th>Country</th>
<th>Code</th>
<th>Country</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>AR</td>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Australia</td>
<td>AU</td>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Austria</td>
<td>AT</td>
<td>Oman</td>
<td>OM</td>
</tr>
<tr>
<td>Bahrain</td>
<td>BH</td>
<td>Peru</td>
<td>PE</td>
</tr>
<tr>
<td>Belarus</td>
<td>BY</td>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Belgium</td>
<td>BE</td>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Country</td>
<td>Code</td>
<td>Country</td>
<td>Code</td>
</tr>
<tr>
<td>-----------------</td>
<td>------</td>
<td>------------------</td>
<td>------</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>BG</td>
<td>Qatar</td>
<td>QA</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
<td>Russian Federation</td>
<td>RU</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Colombia</td>
<td>CO</td>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
<td>Slovak Republic</td>
<td>SK</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
<td>Slovenia</td>
<td>SI</td>
</tr>
<tr>
<td>Cyprus</td>
<td>CY</td>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>Czech Rep.</td>
<td>CZ</td>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Denmark</td>
<td>DK</td>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Ecuador</td>
<td>EC</td>
<td>Sri Lanka</td>
<td>LK</td>
</tr>
<tr>
<td>Estonia</td>
<td>EE</td>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Egypt</td>
<td>EG</td>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Finland</td>
<td>FI</td>
<td>Taiwan</td>
<td>TW</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
<td>Thailand</td>
<td>TH</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
<td>Turkey</td>
<td>TR</td>
</tr>
<tr>
<td>Greece</td>
<td>GR</td>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>HK</td>
<td>UAE</td>
<td>AE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
<td>United Kingdom</td>
<td>UK</td>
</tr>
<tr>
<td>Iceland</td>
<td>IS</td>
<td>USA</td>
<td>US</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
<td>Uruguay</td>
<td>UY</td>
</tr>
<tr>
<td>Indonesia</td>
<td>ID</td>
<td>Vietnam</td>
<td>VN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
<td>Venezuela</td>
<td>VE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td>IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jordan</td>
<td>JO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>KZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kuwait</td>
<td>KW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td>LV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>LI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luxembourg</td>
<td>LU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td>MY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malta</td>
<td>MT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Morocco</td>
<td>MA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nambia</td>
<td>NA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number.
**North American Contacts**

Inside North America:

- Symbol Technologies, Inc.
  One Symbol Plaza Holtsville, New York 11742-1300
  Telephone: 1-631-738-2400/1-800-SCAN 234
  Fax: 1-631-738-5990

Symbol Support Center (for warranty and service information):

- telephone: 1-800-653-5350
- fax: (631) 738-5410
- Email: support@symbol.com

**International Contacts**

Outside North America:

- Symbol Technologies
  Symbol Place
  Winnersh Triangle, Berkshire, RG41 5TP
  United Kingdom
  0800-328-2424 (Inside UK)
  +44 118 945 7529 (Outside UK)
**Web Support Sites**

**MySymbolCare**

http://www.symbol.com/services/msc

**Symbol Services Homepage**

http://symbol.com/services

**Symbol Software Updates**

http://symbol.com/services/downloads

**Symbol Developer Program**

http://software.symbol.com/devzone

**Additional Information**

Obtain additional information by contacting Symbol at:

1-800-722-6234, inside North America
+1-516-738-5200, in/outside North America

http://www.symbol.com/
Index

A
access options ........................................... 1-23
access point
   CAM ............................................................ 1-12
   encryption .................................................. 1-7
   PSP ............................................................ 1-12
   RSSI ............................................................ 1-22
accessories bag .............................................. 4-3
addresses, Symbol ........................................ viii
administrator access ....................................... 4-7
antenna options ............................................. 2-5
antenna support ............................................ 1-3
antenna, 2.4 GHz ............................................ A-4
AP-5131 access .............................................. 4-5
AP-5131-13040-WW........................................ 1-1, 2-2
AP-5131-13041-WW........................................ 1-1, 2-2
AP-5131-13042-WW........................................ 2-2
AP-5131-13043-WW........................................ 2-2
AP-5131-40020-WW.......................................... 2-3
AP-5131-40021-WW.......................................... 1-1, 2-3
AP-5131-40022-WW.......................................... 2-3
AP-5131-40023-WW.......................................... 2-3
AP-PSBIAS-T-1P2-AF................................. 2-3, 2-4
association process
   beacon ....................................................... 1-12
   RSSI ............................................................ 1-22
automatic firmware update ................................... 4-22
available AP-5131 product configurations ........... 2-2
available protocols ........................................ 6-30

B
bandwidth management ................................... 5-45

AP-5131 statistical displays .......................... 1-12
AP-5131 version ......................................... 4-3
AP-5131-13040-WW........................................ 2-2
AP-5131-13041-WW........................................ 1-1, 2-2
AP-5131-13042-WW........................................ 2-2
AP-5131-13043-WW........................................ 2-2
AP-5131-40020-WW.......................................... 2-3
AP-5131-40021-WW.......................................... 1-1, 2-3
AP-5131-40022-WW.......................................... 2-3
AP-5131-40023-WW.......................................... 2-3
AP-PSBIAS-T-1P2-AF................................. 2-3, 2-4
association process
   beacon ....................................................... 1-12
   RSSI ............................................................ 1-22
automatic firmware update ................................... 4-22
available AP-5131 product configurations ........... 2-2
available protocols ........................................ 6-30

B
bandwidth management ................................... 5-45
basic device configuration ......................... 3-3
beacon ........................................ 1-12
CAM stations .................................. 1-12
PSP stations .................................. 1-12
BSSID ........................................... 1-4
bullets, use of ................................ viii
C
CA certificate ..................................... 4-8
CAM ............................................. 1-12
cellular coverage .................. 1-15
certificate authority ................ 4-8
certificate management ........ 4-8
CLI, ACL commands ...................... 8-71
CLI, bandwith management .......... 8-98
CLI, common commands .......... 8-3
CLI, connection ......................... 8-1
CLI, firewall commands ........ 8-111
CLI, firmware update ........ 8-168
CLI, log commands ................. 8-155
CLI, network commands .......... 8-12
CLI, network LAN commands .... 8-13
CLI, network LAN, DHCP commands .... 8-23
CLI, network LAN, VLAN commands .... 8-16
CLI, network wireless commands .. 8-56
CLI, NTP ...................................... 8-152
CLI, QoS ...................................... 8-93
CLI, radio configuration ........ 8-76
CLI, rogue-AP commands ........ 8-101
CLI, router commands ........ 8-116
CLI, security commands ........ 8-62
CLI, serial port ................. 8-1
CLI, SNMP access ................. 8-141
CLI, SNMP commands .......... 8-140
CLI, SNMP traps .................. 8-146
CLI, statistics ...................... 8-175
CLI, system access commands .... 8-126
CLI, system commands ........ 8-121
CLI, system test .................. 8-172
CLI, telnet ................. 8-2
CLI, type filter commands .... 8-29
CLI, WAN App Commands ........ 8-52
CLI, WAN commands ........ 8-34
CLI, WAN NAT commands .......... 8-37
CLI, WAN VLAN Commands ........ 8-43
command line interface (CLI) ........ 3-2
config file ........................................ 3-2
config import/export ........ 4-31
configuration
CLI ........................................ 1-15
configuration file import/export .... 1-13
configuration options ........ 3-2
configuration restoration ........ 1-13
content filtering ................ 6-48
conventions, notational .......... viii
country codes ................. 4-3, A-15
customer support ........ viii, B-1
data access, configuring .......... 4-5
data decryption ............. 1-7
data encryption ............. 1-5
data security ............. 1-5
Desk Mounting ............ 2-11
device firmware ............ 4-34
device settings ............. 3-4
DHCP support ........ 1-13
DHCP, advanced settings .... 5-10
direct-sequence spread spectrum .... 1-20
document conventions .... 1-vii
dual-radio sku ........... 1-3
E
EAP authentication .............. 1-6
electrical characteristics .... A-2
event logging ................ 1-12
firewall ....................... 1-8
firewall security ........ 1-8
firewall, configuring ........ 6-25
firmware .................. 1-10
firmware update ........ 4-34
firmware, updates ........ 4-34
H
hardware installation .......... 2-1
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio, statistics</td>
<td>7-14</td>
</tr>
<tr>
<td>restore default configuration</td>
<td>4-4</td>
</tr>
<tr>
<td>rogue AP detection</td>
<td>6-51</td>
</tr>
<tr>
<td>rogue AP detection, allowed APs</td>
<td>6-54</td>
</tr>
<tr>
<td>rogue AP, details</td>
<td>6-57</td>
</tr>
<tr>
<td>security, WPA</td>
<td>6-19</td>
</tr>
<tr>
<td>security decryption</td>
<td>1-7</td>
</tr>
<tr>
<td>security, content filtering</td>
<td>6-48</td>
</tr>
<tr>
<td>security, firewall</td>
<td>6-25</td>
</tr>
<tr>
<td>security, KeyGuard</td>
<td>6-17</td>
</tr>
<tr>
<td>security, rogue AP detection</td>
<td>6-51</td>
</tr>
<tr>
<td>security, VPN</td>
<td>6-33</td>
</tr>
<tr>
<td>security, WLAN</td>
<td>3-9</td>
</tr>
<tr>
<td>security, WPA2-CCMP</td>
<td>6-22</td>
</tr>
<tr>
<td>self certificates</td>
<td>4-9</td>
</tr>
<tr>
<td>serial number</td>
<td>4-4</td>
</tr>
<tr>
<td>service information</td>
<td>viii</td>
</tr>
<tr>
<td>setting up MUs</td>
<td>2-22</td>
</tr>
<tr>
<td>single sku</td>
<td>1-2</td>
</tr>
<tr>
<td>site surveys</td>
<td>2-5</td>
</tr>
<tr>
<td>SNMP</td>
<td>1-10</td>
</tr>
<tr>
<td>SNMP Access</td>
<td>4-14</td>
</tr>
<tr>
<td>SNMP access control</td>
<td>4-17</td>
</tr>
<tr>
<td>SNMP settings</td>
<td>4-11</td>
</tr>
<tr>
<td>SNMP v1/v2</td>
<td>4-15</td>
</tr>
<tr>
<td>SNMP v1/v2/v3 trap support</td>
<td>1-10</td>
</tr>
<tr>
<td>SNMP v3</td>
<td>4-15</td>
</tr>
<tr>
<td>SNMP, access control</td>
<td>4-17</td>
</tr>
<tr>
<td>SNMP, RF trap thresholds</td>
<td>4-24</td>
</tr>
<tr>
<td>SNMP, specific traps</td>
<td>4-22</td>
</tr>
<tr>
<td>SNMP, traps</td>
<td>4-19</td>
</tr>
<tr>
<td>SNMP, v1/v2c</td>
<td>4-20</td>
</tr>
<tr>
<td>SNMP, v3 user definitions</td>
<td>4-15</td>
</tr>
<tr>
<td>statistics, AP-5131</td>
<td>7-26</td>
</tr>
<tr>
<td>statistics, LAN</td>
<td>7-5</td>
</tr>
<tr>
<td>statistics, mu</td>
<td>7-20</td>
</tr>
<tr>
<td>statistics, radio</td>
<td>7-14</td>
</tr>
<tr>
<td>statistics, WLAN</td>
<td>7-2</td>
</tr>
<tr>
<td>statistics, WLAN</td>
<td>7-8</td>
</tr>
<tr>
<td>suspended T-Bar installations</td>
<td>2-15</td>
</tr>
<tr>
<td>Symbol support center</td>
<td>viii</td>
</tr>
<tr>
<td>system configuration</td>
<td>4-1</td>
</tr>
<tr>
<td>system location</td>
<td>4-3</td>
</tr>
<tr>
<td>system name</td>
<td>4-3</td>
</tr>
<tr>
<td>system settings</td>
<td>4-2</td>
</tr>
<tr>
<td>system settings, configuration</td>
<td>4-2</td>
</tr>
<tr>
<td>system uptime</td>
<td>4-3</td>
</tr>
<tr>
<td>technical support</td>
<td>viii</td>
</tr>
<tr>
<td>testing AP-5131 connectivity</td>
<td>3-11</td>
</tr>
<tr>
<td>testing connectivity</td>
<td>3-11</td>
</tr>
<tr>
<td>theory of operations</td>
<td>1-14</td>
</tr>
<tr>
<td>TKIP</td>
<td>1-7</td>
</tr>
<tr>
<td>transmit power control</td>
<td>1-12</td>
</tr>
<tr>
<td>type filter, configuration</td>
<td>5-11</td>
</tr>
<tr>
<td>VLAN</td>
<td>1-9</td>
</tr>
<tr>
<td>VLAN, config</td>
<td>5-3</td>
</tr>
<tr>
<td>VLAN, configuring</td>
<td>5-5</td>
</tr>
<tr>
<td>VLAN, management tag</td>
<td>5-8</td>
</tr>
<tr>
<td>VLAN, name</td>
<td>5-3</td>
</tr>
<tr>
<td>VLAN, native tag</td>
<td>5-9</td>
</tr>
<tr>
<td>Voice prioritization</td>
<td>1-11</td>
</tr>
<tr>
<td>VPN</td>
<td>1-8</td>
</tr>
<tr>
<td>VPN, tunnels</td>
<td>1-8</td>
</tr>
<tr>
<td>VPN, auto key settings</td>
<td>6-40, 6-41</td>
</tr>
<tr>
<td>VPN, configuring</td>
<td>6-33</td>
</tr>
<tr>
<td>VPN, IKE key settings</td>
<td>6-42</td>
</tr>
<tr>
<td>VPN, manual key settings</td>
<td>6-36</td>
</tr>
<tr>
<td>VPN, status</td>
<td>6-46</td>
</tr>
<tr>
<td>wall mounting</td>
<td>2-13</td>
</tr>
<tr>
<td>WAN port</td>
<td>1-3</td>
</tr>
<tr>
<td>WAN, configuring</td>
<td>5-13</td>
</tr>
<tr>
<td>WAN, port forwarding</td>
<td>5-20</td>
</tr>
<tr>
<td>WAN, statistics</td>
<td>7-2</td>
</tr>
<tr>
<td>WEP</td>
<td>1-6</td>
</tr>
<tr>
<td>WEP, encryption</td>
<td>1-5, 1-6</td>
</tr>
<tr>
<td>Wi-Fi Protected Access (WPA)</td>
<td>1-7</td>
</tr>
<tr>
<td>WLAN, ACL</td>
<td>5-29</td>
</tr>
<tr>
<td>WLAN, creating</td>
<td>5-24</td>
</tr>
<tr>
<td>WLAN, editing</td>
<td>5-24</td>
</tr>
</tbody>
</table>
WLAN, enabling ........................................ 5-22
WLAN, security ....................................... 5-27
WLAN, statistics ...................................... 7-8
WPA ...................................................... 6-19
WPA2-CCMP ........................................... 1-8, 6-22

WPA2-CCMP (802.11i) .................................. 1-8
WPA-CCMP (802.11i) ...................................... 1-5
WPA-TKIP .................................................. 1-5
WPA, 256-bit keys ........................................ 6-21