53-1001932-01
Sept 2010

Brocade Mobility 7131 Series Access Point

Product Reference Guide

Supporting software release 4.1.0.0 and later

BROCADE

Copyright © 2010 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, StorageX, and TurboIron are registered trademarks, and DCFM, Extraordinary Networks, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade Mobility 7131 Series Access Point Product Reference Guide	*53-1001932-01*	New document	Sept 2010

About This Document xi
In this chapter xi
Audience xi
Supported hardware and software xi
Document conventions xi
Notice to the reader xiii
Web support sites xiii
Product downloads xiii
Manuals xiii
Additional information xiii
Customer support xiii

1 Introduction 1
Access point menu navigation 2
New features 2
Power management antenna configuration file 3
Hotspot customization 3
WAN failover 4
Proxy ARP support 4
Multi cipher support 5
Dynamic chain selection 5
Broadcast/multicast transmit rate control 5
Dedicated sensor support 6
LED disable 6
Feature overview 6
802.11n support 7
Sensor support 7
Mesh roaming client 9
Single or dual mode radio options 9
Separate LAN and WAN ports 10
Multiple mounting options 10
Antenna support for 2.4 GHz and 5 GHz radios 10
Sixteen configurable WLANs 11
Support for 4 BSSIDs per radio 11
Quality of Service (QoS) support 11
Industry leading data security 12
VLAN support 15
Multiple management accessibility options 15
Updatable firmware 16
Programmable SNMP v1/v2/v3 trap support 16
Client-Client transmission disallow 16
Voice prioritization 16
Support for CAM and PSP clients 17
Statistical displays 17
Transmit power control 17
Advanced event logging capability 18
Configuration file import/export functionality 18
Default configuration restoration 18

DHCP support . . . 18
Mesh networking . . . 19
Additional LAN subnet . . . 19
On-board Radius Server authentication . . . 20
Hotspot support . . . 20
Routing Information Protocol (RIP) . . . 20
Manual date and time settings . . . 21
Dynamic DNS . . . 21
Auto negotiation . . . 21
Adaptive AP . . . 21
Rogue AP enhancements . . . 21
Bandwidth management enhancements . . . 22
Radius time-based authentication . . . 22
QBSS support . . . 22
Triple radio support . . . 22
IP filtering . . . 23
Client rate limiting . . . 23
Per radio client limit . . . 23
Power setting configuration . . . 24
AMSDU transmission support . . . 24
IPSec VPN support . . . 24
Theory of operations . . . 25
Wireless coverage . . . 25
MAC layer bridging . . . 26
Media types . . . 26
Direct-Sequence Spread Spectrum . . . 27
Client association process . . . 27
Operating modes . . . 28
Management access options . . . 29
Brocade Mobility 7131 Series Access Point MAC address assignment . . . 29

2 Hardware Installation 31

Precautions . . . 31
Requirements . . . 31
Package contents . . . 31
Access point placement . . . 32
Site surveys . . . 33
Antenna options . . . 33
Mounting a Brocade Mobility 7131 Series Access Point . . . 35
Wall mounted installations . . . 35
Suspended ceiling T-Bar installations . . . 38
Above the ceiling (plenum) installations . . . 39
Brocade Mobility 7131 Series Access Point LED indicators . . . 42
Three Radio Mobility 7131N LEDs . . . 43
Dual radio (2.4/5 GHz) Brocade Mobility 7131 Series Access Point . . . 44
Single radio 2.4 GHz Brocade Mobility 7131 Series Access Point LEDs . . . 44
Single radio 5 GHz Brocade Mobility 7131 Series Access Point LEDs . . . 45

Rear Brocade Mobility 7131 Series Access Point LED 45
Setting up clients 45
802.11n clients 45

3 Getting Started 49
Installing the access point 49
Configuration options 49
Initially connecting to the access point 50
Connecting to the Brocade Mobility 7131 Series Access Point using the WAN port 50
Connecting to the Brocade Mobility 7131 Series Access Point using the LAN port 50
Basic device configuration 51
Configuring device settings 53
Testing connectivity 61
Where to go from here? 61

4 System Configuration 63
Configuring system settings 63
Configuring power settings 67
Radios at full power 68
Radios at low power 69
Adaptive AP setup 72
Configuring data access 74
Managing certificate authority (CA) certificates 78
Importing a CA certificate 79
Creating self certificates for accessing the VPN 80
Creating a certificate for Onboard Radius Authentication 83
Configuring SNMP settings 86
Configuring SNMP access control 90
Enabling SNMP traps 92
Configuring specific SNMP traps 94
Configuring SNMP RF trap thresholds 96
Configuring LLDP settings 98
Configuring network time protocol (NTP) 99
Logging configuration 102
Importing/exporting configurations 103
Updating device firmware 108

5 Network Management 113
Configuring the LAN interface 113
Configuring VLAN support 116
Configuring LAN1 and LAN2 settings 120
Configuring WAN settings 125
Configuring Network Address Translation (NAT) settings 131
Configuring Dynamic DNS 135
Enabling wireless LANs (WLANs) 137

Creating/editing individual WLANs . . . 139
Setting the WLAN's radio configuration . . . 161
Configuring client rate limiting . . . 177
Configuring router settings . . . 178
Setting the RIP configuration . . . 180
Configuring IP filtering . . . 182
Applying a filter to LAN1, LAN2 or a WLAN (1-16) . . . 184
IP filter configuration - example . . . 185

6 Configuring Access Point Security 191

Configuring security options . . . 192
Setting passwords . . . 192
Resetting the access point password . . . 194
Enabling authentication and encryption schemes . . . 194
Configuring Kerberos authentication . . . 196
Configuring 802.1x EAP authentication . . . 198
Configuring WEP encryption . . . 202
Configuring KeyGuard encryption . . . 204
Configuring WPA/WPA2 using TKIP . . . 206
Configuring WPA2-CCMP (802.11i) . . . 208
Configuring multi cipher support . . . 211
Configuring firewall settings . . . 213
Configuring LAN to WAN access . . . 215
Configuring Advanced Subnet Access . . . 218
Configuring VPN tunnels . . . 220
Creating a VPN tunnel between two access points . . . 223
Configuring manual key settings . . . 225
Configuring auto key settings . . . 228
Configuring IKE key settings . . . 230
Viewing VPN status . . . 233
Configuring content filtering settings . . . 235
Configuring rogue AP detection . . . 238
Moving rogue APs to the allowed AP list . . . 241
Using clients to detect rogue devices . . . 244
Configuring user authentication . . . 245
Configuring the Radius Server . . . 245
Configuring LDAP authentication . . . 248
Configuring a proxy Radius server . . . 250
Managing the local User database . . . 252
Defining user access permissions by group . . . 254
Defining the user access policy . . . 254

7 Monitoring Statistics 259

Viewing WAN statistics . . . 259
Viewing LAN statistics . . . 263

Viewing a LAN's STP statistics . . . 265
Viewing a LAN's IP filter statistics . . . 267
Viewing wireless statistics . . . 269
Viewing WLAN statistics . . . 270
Viewing a WLAN's IP filter statistics . . . 273
Viewing radio statistics summary . . . 275
Viewing radio statistics . . . 276
Viewing client statistics summary . . . 280
Viewing Client details . . . 282
Client authentication statistics . . . 284
Viewing the mesh statistics summary . . . 284
Viewing known access point statistics . . . 286

8 CLI Reference 291
Connecting to the CLI . . . 291
Accessing the CLI through the serial port . . . 291
Accessing the CLI via Telnet . . . 291
Admin and common commands . . . 292
Network commands . . . 300
Network LAN commands . . . 301
Network WAN commands . . . 328
Network wireless commands . . . 356
Network firewall commands . . . 445
Network router commands . . . 450
Network IP Filter Commands . . . 456
Network DHCP Client Hostname Option Commands . . . 461
System commands . . . 464
Power setup commands . . . 470
Adaptive AP setup commands . . . 473
LLDP Commands . . . 477
System access commands . . . 480
System certificate management commands . . . 483
System SNMP commands . . . 496
System user database commands . . . 509
System Radius commands . . . 522
System Network Time Protocol (NTP) commands . . . 545
System log commands . . . 550
System configuration-update commands . . . 556
Firmware update commands . . . 563
Statistics commands . . . 567

9 Configuring Mesh Networking 583
Mesh networking overview . . . 583
The Brocade Mobility 7131 Series Access Point client bridge association process . . . 584
Spanning tree protocol (STP) . . . 585
Defining the mesh topology . . . 585

Mesh networking and the Brocade Mobility 7131 Series Access Point's two subnets . . . 586
Normal operation . . . 586
Impact of importing/exporting configurations to a mesh network . . . 586
Configuring mesh networking support . . . 587
Setting the LAN configuration for mesh networking support . . . 587
Configuring a WLAN for mesh networking support . . . 588
Configuring the access point radio for mesh support . . . 591
Mesh network deployment - quick setup . . . 597
Scenario 1 - two base bridges and one client bridge . . . 597
Scenario 2 - two hop mesh network with a base bridge repeater and a client bridge . . . 605
Mesh networking frequently asked questions . . . 610

10 Adaptive AP 613

Adaptive AP overview . . . 613
Where to go from here . . . 614
Adaptive AP management . . . 614
Licensing . . . 614
Controller discovery . . . 614
Securing a configuration channel between controller and AP . . . 616
Adaptive AP WLAN topology . . . 616
Configuration updates . . . 616
Securing data tunnels between the controller and AAP . . . 616
Adaptive AP controller failure . . . 617
Remote site survivability (RSS) . . . 617
Adaptive mesh support . . . 617
Supported adaptive AP topologies . . . 618
Topology deployment considerations . . . 618
Extended WLANs only . . . 618
Independent WLANs Only . . . 619
Extended WLANs with independent WLANs . . . 619
Extended WLAN with mesh networking . . . 619
How the AP receives its adaptive configuration . . . 619
Establishing basic adaptive AP connectivity . . . 620
Adaptive AP configuration . . . 621
Controller configuration . . . 623
Adaptive AP deployment considerations . . . 625
Sample controller configuration file for IPSec and independent WLAN . . . 625

A Technical Specifications . . . 631

Mobility 7131 physical characteristics . . . 631
Mobility 7131N physical characteristics . . . 631
Electrical characteristics . . . 632
Radio characteristics . . . 632
Antenna specifications . . . 633
2.4 GHz antenna matrix . . . 633
Country codes . . . 634

B Usage Scenarios . . . 637

Configuring automatic updates using a DHCP or Linux BootP Server 637
Windows - DHCP server configuration 637
Linux - BootP server configuration 641
Configuring an IPSEC tunnel and VPN FAQs 643
Configuring a VPN tunnel between two access points 643
Configuring a Cisco VPN device 647
Frequently asked VPN questions 648

About This Document

In this chapter

- Audience. xi
- Supported hardware and software. xi
- Document conventions xi
- Notice to the reader xiii
- Web support sites xiii
- Customer support xiii

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade Layer 3 Controller, you should be familiar with the following protocols if applicable to your network – IP, RIP, OSPF, BGP, ISIS, IGMP, PIM, DVMRP, and VRRP.

Supported hardware and software

The following hardware platforms are supported by this release of this guide:

- Brocade Mobility 7131 Series Access Points

The following software version is supported by this release of this guide:

- Software version 4.1.0.0

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, controllerShow. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Command syntax conventions

Command syntax in this manual follows these conventions:

command and parameters	Commands and parameters are printed in bold.
[ ]	Optional parameter.
variable	Variables are printed in italics enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
|	Choose from one of the parameters.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced trademarks and products
Phillips Screw Company, Inc.	Phillips

Web support sites

Product downloads

http://www.brocade.com

Manuals

http://www.brocade.com

Additional information

http://www.brocade.com

Customer support

If you have a problem with your equipment, contact customer support for your region. Contact information is available at: *http://www.brocade.com/support/.*

When contacting customer support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Brocade responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Brocade business partner, contact that business partner for support.

Customer Support Web Sites

Brocade's Support Central Web site, located at *http://www.brocade.com/support/* provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Chapter

1 Introduction

In this chapter

- Feature overview 6
- Theory of operations 25

As a standalone access point, the Brocade Mobility 7131 Series Access Point provides small and medium-sized businesses with a consolidated wired and wireless networking infrastructure, all in a single device. The integrated router, gateway, firewall, DHCP and AAA Radius servers, VPN, hot-spot gateway and *Power-over-Ethernet* (PoE) simplify and reduce the costs associated with networking by eliminating the need to purchase and manage multiple pieces of equipment.

The Brocade Mobility 7131 Series Access Point is also designed to meet the needs of large, distributed enterprises by converging the functionality of a thick access point and thin access point into a single device. This mode enables the deployment of a fully featured intelligent access point that can be centrally configured and managed via a Brocade wireless controller in either corporate headquarters or a *network operations center* (NOC). In the event the connection between the Brocade Mobility 7131 Series Access Point and the wireless controller is lost, a *Remote Site Survivability* (RSS) feature ensures the delivery of uninterrupted wireless services at the local or remote site. All traffic between the adaptive access points and the wireless controller is secured though an IPSec tunnel. Additionally, compatibility with Brocade's RF Management Suite allows you to centrally plan, deploy, monitor, and secure large Brocade Mobility 7131 Series Access Point deployments.

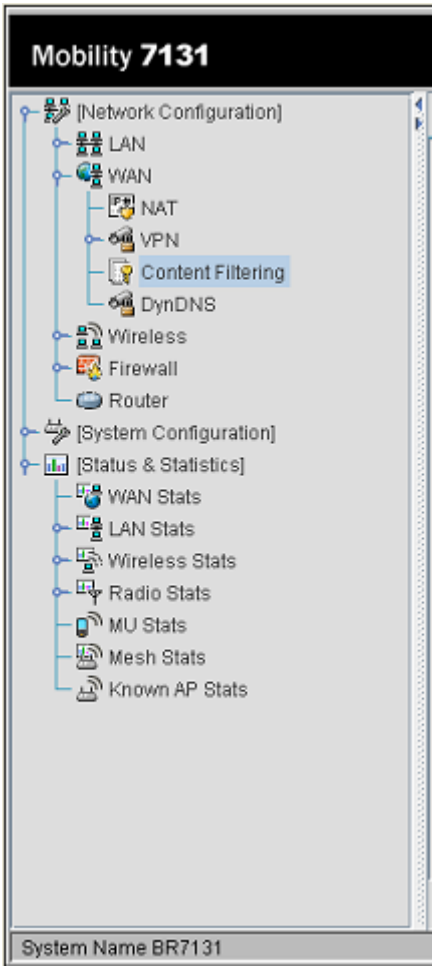
With the introduction of the Brocade Mobility 7131 4.x firmware baseline, Brocade is also introducing a new series of Brocade Mobility 7131N Access Points as a compliment to the existing Brocade Mobility 7131 Access Point family. The new Brocade Mobility 7131N Access Points support the same feature set and firmware as existing Brocade Mobility 7131 Access Points, however Brocade Mobility 7131N Access Points support a three radio model (with the third radio dedicated exclusively for sensor support). For more information on the three radio Brocade Mobility 7131N, see "Triple radio support" on page 22.

NOTE
Both the Brocade Mobility 7131 and Brocade Mobility 7131N Access Points share the same Web applet (user interface) and installation methods. Therefore, the UI and installation descriptions within this guide apply to both models. There are instances where this common interface is used differently to configure various features (radio configuration, power management etc.), however those differences are carefully noted.

If you are new to using an access point for managing your network, refer to "Theory of operations" on page 25 for an overview on wireless networking fundamentals.

Access point menu navigation

The access point supports an expandable menu tree located on the left-hand side of the *Graphical User Interface* (GUI) shown in the following figure. Additional menu items can be accessed by expanding the Network Configuration, System Configuration and Status & Statistics main menu items. The data presented in this guide is arranged based on the access point's GUI organizational structure, with the exception of access point security features, which can be displayed and configured from various locations within the access point's GUI.



New features

The following features are now available with the introduction of the new Brocade Mobility 7131N Access Point hardware and firmware baseline:

- *Power management antenna configuration file*
- *Hotspot customization*
- *WAN failover*
- *Proxy ARP support*

- *Multi cipher support*
- *Dynamic chain selection*
- *Broadcast/multicast transmit rate control*
- *Dedicated sensor support*
- *LED disable*

Power management antenna configuration file

With this most recent release of the access point firmware, a *Power Management Antenna Configuration File* (PMACF) has been added to the access point firmware that automatically configures the access point's radio transmit power based on the antenna type deployed, its supported gain and the deployed country's regulatory domain restrictions. The anntenna type is defined using the access point's CLI by assigning a numerical code representing a particular type (or category) of antenna. The following are the numerical codes representing available anatenna types: 0-Default antenna, 1-Dual band antenna, 2-Omni antenna, 3-Yagi antenna, 4-Embedded antenna, 5-Panel antenna, 6-Patch antenna and 7-Sector antenna. The antenna gain can be defined using either the access point's CLI, applet or SNMP interfaces.

Once the antenna type and gain are provided, the access point calculates the power range. The PMACF contains transmit power data for each Brocade approved antenna type. Professional installers enter the antenna type (using the access point's CLI interface), and the access point firmware calculates the transmit power automatically. Therefore, professional installers no longer need to second guess whether the power is over the maximum allowed level.

NOTE
The antenna type and antenna gain values are maintained by the access point after a power cycle, and are available in imported or exported configurations.

For information on defining the antenna gain using the access point's GUI applet, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

Hotspot customization

To date, the default hotspot supported on the access point does not allow users to change the text on the hotspot portal or the logo for the enterprise where the hotspot is deployed. With this most recent release of the access point firmware, users now have the ability to customize the appearance of an access point's WLAN hotspot pages. The access point's hotspot feature is supported by three customer accessible pages (login page, welcome page and failure page) displayed on the client attempting to access the AP's supported hotspot. These three pages can be unique to each hotspot supported by one of the access point's 16 WLANs. The content of the three hotspot pages can be customized by:

- Altering the text that displays on the screen
- Altering the properties of various screen elements (such as background colors, banner and logos)

NOTE
The access point allows two logos to be displayed per page. The user has the ability to alter logo placement and screen banner color schemes.

- Configuring a *cascading style sheet* (css) to define how hotspot pages display font usage, text size etc.

For information on customizing a WLAN's hotspot display, see "Customizing a hotspot display" on page 156.

For information on the access point's existing (default) hotspot functionality, see "Hotspot support" on page 20.

WAN failover

With this most recent release of the Brocade Mobility 7131N Access Point firmware, a WAN failover feature has been introduced, since a cellular network infrastructure is completely separate from the access point's wired transmission infrastructure.

A WWAN card is a specialized network interface card, allowing a network device to connect, transmit and receive data over a cellular WAN. The WWAN card uses *point to point protocol* (PPP) to connect to an *Internet Service Provider* (ISP) and access the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point links.

The wired WAN is the primary WAN link for a Brocade Mobility 7131N Access Point, as long as it is enabled and connected, and the wireless WAN interface is the secondary link. For a WWAN to be a WAN or LAN recovery solution, the Brocade Mobility 7131N Access Point needs to monitor the link status of the wired WAN and actively check the health of the WAN connection. If a wired WAN or LAN connection failure is detected, a Brocade Mobility 7131N Access Point immediately establishes the WWAN connection and updates the default gateway to the WWAN interface.

The WWAN card is detected automatically when inserted into the Brocade Mobility 7131N Access Point express card slot. The card is detected as a USB/Serial device once its modules are loaded. If the card is inserted before or during module installation, the user has to wait until all the modules are loaded before the card is operational. These modules are loaded when the Brocade Mobility 7131N Access Point boots up (at runtime). Activate and configure the WWAN card from the access point's applet and CLI.

NOTE
The WAN failover feature is only supported on Brocade Mobility 7131N Access Points, as the Brocade Mobility 7131 Access Point does not support the required PCI express card slot.

For more information on configuring a Brocade Mobility 7131N Access Point for WAN failover support, see "Configuring WAN settings" on page 125.

Proxy ARP support

With this most recent release of the access point firmware, the access point can respond to ARP requests on behalf of an associated client and protect the client's network credentials from being broadcasted on a publicly accessible network.

When Proxy ARP is enabled on the access point, the access point can make an client physically located on one network appear part of a different network connected to the same access point. Proxy AP allows the access point to "hide" an client's IP address behind the access point's firewall, while still having the client appear to be on the public network. Proxy ARP is enabled by default.

For example, when Proxy ARP is enabled on the access point and the access point receives an ARP request (either a wired or wireless request) for the IP address of an associated client, the access point responds directly to the request (on behalf of the client) instead of broadcasting the ARP request over the publicly accessible wireless network.

When enabled on the access point, any system on the wireless network that ARPs for the IP address of an associated client will receive an ARP reply from the access point stating the requesting system should be sending packets destined for the client to access point instead. In turn, the access point forwards the requesting packets to the target client. Through this process, the access point can pass ARP requests in both directions, making an client appear to be connected to a public network even though it's on a private network hidden behind the access point. Proxy ARP supports both strict and dynamic modes on the access point.

For detailed information on configuring Proxy AP support of the access point, see "Enabling wireless LANs (WLANs)" on page 137.

Multi cipher support

Beginning with this release, professional installers have the option of deploying both new and legacy clients within the same WLAN. Multi cipher support extends the access point's existing WLAN security options by allowing dynamic WEP and 802.11i configurations to co-exist, and allowing multiple security policies to be associated with the same ESSID on different WLANs. Within such an environment, legacy clients are capable of WEP, while new clients are capable of WPA/2-TKIP and WPA2-CCMP encryption. This particular form of multi cipher (security) support helps maintain the co-existence of dynamic WEP and 802.11i based environments.

For information on configuring Multi Cipher support, see "Configuring multi cipher support" on page 211.

Dynamic chain selection

When enabled, dynamic chain selection forces an access point radio to transmit packets using legacy transmit rates (11b, 11g and/or 11a rates) using a single transmit chain. Transmissions utilizing 11n rates (MCS0 - MCS15) continue to use a normal number of transmit chains, which may be 1, 2, or 3 depending on the configuration and power source. If dynamic chain selection is disabled, all transmissions utilize the same number of transmit chains. This feature is disabled by default.

Dynamic chain selection is configured using the access point's CLI, as no applet support is available.

Broadcast/multicast transmit rate control

Beginning with this release, professional installers now have the ability to define the access point's broadcast/multicast transmission configuration. Traditionally, the access point used the lowest basic rate for broadcast/multicast transmissions, which was ideal from a range perspective (and remains the default configuration).

The new enhancement provides an option to increase performance by transmitting broadcast/multicast group packets at a higher rate (based on the radio's defined basic data rates). This option is optimal in environments where the access point's broadcast/multicast (group packet) transmission range is secondary to performance. Broadcast/multicast rate control is configurable from the access point's GUI applet, CLI and SNMP interfaces.

For information on configuring broadcast/multicast transmit rate control, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

Dedicated sensor support

Beginning with this release, the access point supports a CLI command enabling an access point radio to convert to sensor only support. When enabled, only sensor mode radio configurations are permitted. Radio configurations supporting data (WLAN) support are not configurable using the access point's GUI, CLI or SNMP interfaces.

LED disable

Through extensive field research, Brocade has learned that not all customers wish to deploy an access point with blinking LEDs. Health care deployments in particular have requested an option to disable blinking LEDs. With this most recent release of the Brocade Mobility 7131N Access Point firmware, an option has been added to the access point's GUI applet and CLI to disable blinking LEDs. The LEDs display and blink default until the disable option is invoked.

For information on disabling the access points LEDs, refer to "Configuring system settings" on page 63.

Feature overview

The following legacy features have been carried forward into the 4.x firmware baseline:

- *802.11n support*
- *Sensor support*
- *Mesh roaming client*
- *Single or dual mode radio options*
- *Separate LAN and WAN ports*
- *Multiple mounting options*
- *Antenna support for 2.4 GHz and 5 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*
- *Client-Client transmission disallow*
- *Voice prioritization*
- *Support for CAM and PSP clients*
- *Statistical displays*

- *Transmit power control*
- *Advanced event logging capability*
- *Configuration file import/export functionality*
- *Default configuration restoration*
- *DHCP support*
- *Mesh networking*
- *Additional LAN subnet*
- *On-board Radius Server authentication*
- *Hotspot support*
- *Routing Information Protocol (RIP)*
- *Manual date and time settings*
- *Dynamic DNS*
- *Auto negotiation*
- *Adaptive AP*
- *Rogue AP enhancements*
- *Bandwidth management enhancements*
- *Radius time-based authentication*
- *QBSS support*
- *Triple radio support*
- *IP filtering*
- *Client rate limiting*
- *Per radio client limit*
- *Power setting configuration*
- *AMSDU transmission support*
- *IPSec VPN support*

802.11n support

Brocade provides full life-cycle support for either a new or existing 802.11n mobility deployment, from network design to day-to-day support. For information on deploying your 802.11n radio, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

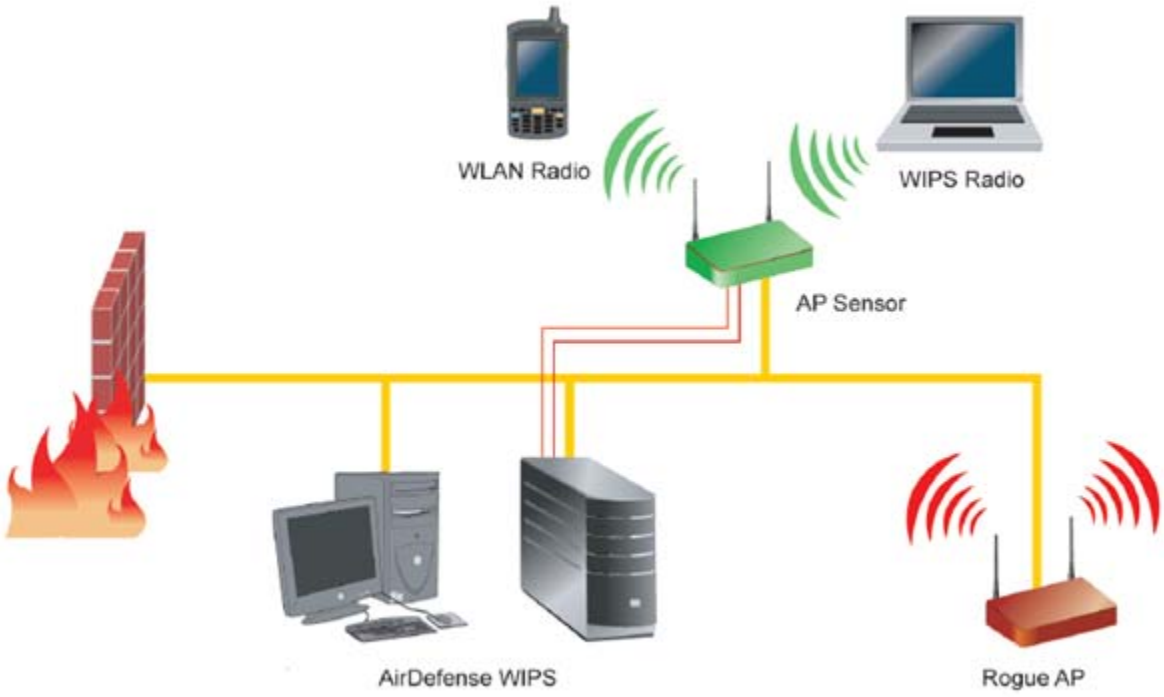
Sensor support

An access point radio can function as a Wireless Intrusion Protection System (WIPS) sensor and upload sensor mode operation information to a dedicated WIPS server. Either one or both of the Brocade Mobility 7131 Series Access Point's radios can be configured as WIPS supported radio. WIPS is not supported on a WLAN basis, rather WIPS is supported on the access point radio(s) available to each WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all channels within the 2.4 and 5.0 GHz bands.

WIPS protects your wireless network, mobile devices and traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock 802.11a/b/g wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

NOTE
WIPS support requires a AirDefense WIPS Server on the network. WIPS functionality is not provided by the Brocade Mobility 7131 Series Access Point alone. The Brocade Mobility 7131 Series Access Point works in conjunction with a dedicated WIPS server.

The following is a network topology illustrating how a sensor functions within an access point supported wireless network:



A radio in sensor mode supports the following basic features:

NOTE
The functions described below are conducted on the WIPS server side, not on the access point.

- *Wireless Termination* - The access point attempts to force an unwanted (or unauthorized) connection to disconnect.
- *Wireless Sniffing* - All received frames are reported to the WIPS server. This feature provides the WIPS server with visibility into the activity on the wireless network. The WIPS server processes the received traffic and provides the IT administrator with useful information about the 802.11 RF activities in the enterprise.

- *Spectrum Analysis* - The data needed to provide the current RF Spectrum is provided to the WIPS server. The access point does not display the data, but it is available to the WIPS server. Spectrum analysis can operate only when there are no WLAN radios configured. The WIPS daemon and server are responsible for limiting operation only when there is no radio in WLAN mode. When a configuration change is made at the AP, the Spectrum Analysis operation stops.
- *Live View*- The WIPS application provides a live view of the sensors, APs and clients operating in a WLAN. Live view support exists throughout the WIPS application, wherever a device icon appears in an information panel or navigation tree. Access Live View by right-clicking on the device, which automatically limits the data to the specific device your choose.

Sensor radios can be tuned to channels in both the 2.4GHz and 5.0 GHz band. The channels in use by a given radio are defined by the WIPS application. There is no need to explicitly set a band for a sensor radio. Instead, select either default values or specific channels. Specific channels can be in either band.

NOTE
Brocade Mobility 7131N Access Points with three radios never dedicate the third radio to traditional WLAN support. The third radio is either disabled or set exclusively to WIPS support (referred to in the access point interface as sensor mode).

CAUTION

Users cannot define a radio as a WIPS sensor when one of the access point radios is functioning as a rogue AP detector. To use one of the radios as a WIPS sensor, you must disable its current detector method(s) first, then set the radio for WIPS sensor support. For information on disabling rogue AP detection, see "Configuring rogue AP detection" on page 238.

WIPS functionality is defined as part of the access point's quick setup procedure. For information on using the access point's Quick Setup screen to define how WIPS can be supported on an access point radio, see "Configuring device settings" on page 53.

Mesh roaming client

Enable the Mesh Roaming Client feature (using the access point's CLI) to allow a client bridge to associate in the same manner as a regular mesh client bridge. After an initial (single) association, the client bridge will not attempt additional associations. Since STP will be disabled, the association forwards data as soon as the association attempt is successful. When Mesh Roaming Client is enabled, base bridge mode is not supported to avoid a loop within the mesh topology. Thus, the Mesh Roaming Client is always an end point (by design) within the mesh wireless topology. The base bridge will need STP disabled to immediately begin forwarding data when a roaming client bridge associates.

Single or dual mode radio options

One or two possible configurations are available on the access point depending on which model is purchased. If the access point is manufactured as a single radio access point, the access point enables you to configure the single radio for either 802.11a/n or 802.11b/g/n support.

If the access point is manufactured as a dual-radio access point, the access point enables you to configure one radio for 802.11a/n support, and the other for 802.11b/g/n support.

For detailed information, see “Setting the WLAN’s radio configuration” on page 161.

Separate LAN and WAN ports

The Brocade Mobility 7131 Series Access Point has one LAN (GE1/POE) port and one WAN (GE2) port, each with their own MAC address. The access point 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 access point can only use a Power-over-Ethernet device when connected to the LAN port.

For detailed information on configuring the Brocade Mobility 7131 Series Access Point LAN port, see “Configuring the LAN interface” on page 113.

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 Brocade Mobility 7131 Series Access Point’s intended mode of operation.

For detailed information on configuring the Brocade Mobility 7131 Series Access Point’s WAN port, see “Configuring WAN settings” on page 125.

The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens.

For detailed information on locating the access point’s MAC addresses, see “Viewing WAN statistics” on page 259 and “Viewing LAN statistics” on page 263. For information on access point MAC address assignments, see “Brocade Mobility 7131 Series Access Point MAC address assignment” on page 29.

Multiple mounting options

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point in a location that has not been approved in an Brocade Mobility 7131 Series Access Point radio coverage site survey.

For detailed information on the mounting options available, see “Mounting a Brocade Mobility 7131 Series Access Point” on page 35.

Antenna support for 2.4 GHz and 5 GHz radios

The Brocade Mobility 7131 Series Access Point supports several 802.11a/n and 802.11b/g/n 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 GHz) antennas supported on the Brocade Mobility 7131 Series Access Point’s *Reverse SMA (RSMA)* connectors, see “Antenna specifications” on page 633.

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 Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point.

To enable and configure WLANs on a Brocade Mobility 7131 Series Access Point radio, see "Enabling wireless LANs (WLANs)" on page 137.

Support for 4 BSSIDs per radio

The access point 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 00:24:38:28:9B:DC, then the BSSIDs for that radio will have the following MAC addresses:

BSSID	MAC address	Hexadecimal addition
BSSID #1	00:24:38:28:9B:DC	Same as Radio MAC address
BSSID #2	00:24:38:28:9B:DD	Radio MAC address +1
BSSID #3	00:24:38:28:9B:DE	Radio MAC address +2
BSSID #4	00:24:38:28:9B:DF	Radio MAC address +3

For detailed information on strategically mapping BSSIDs to WLANs, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167. For information on access point MAC address assignments, see "Brocade Mobility 7131 Series Access Point MAC address assignment" on page 29.

Quality of Service (QoS) support

The Brocade Mobility 7131 Series Access Point QoS implementation provides applications running on different wireless devices a variety of priority levels to transmit data to and from the Brocade Mobility 7131 Series Access Point. 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 Brocade Mobility 7131 Series Access Point QoS implementation.The *WiFi Multimedia QOS Extensions (WMM)* implementation used by the Brocade Mobility 7131 Series Access Point shortens the time between transmitting higher priority data traffic and is thus desirable for multimedia applications. In addition, U-APSD (WMM Power Save) is also supported.

WMM defines four access categories—*voice, video*, *best effort* and *background*—to prioritize traffic for enhanced multimedia support.

For detailed information on configuring QoS support, see "Setting the WLAN Quality of Service (QoS) policy" on page 147.

Industry leading data security

The Brocade Mobility 7131 Series Access Point supports numerous encryption and authentication techniques to protect the data transmitting on the WLAN.

The following authentication techniques are supported:

- *Kerberos authentication*
- *EAP authentication*

The following encryption techniques are supported:

- *WEP encryption*
- *KeyGuard encryption*
- *Wi-Fi protected access (WPA) using TKIP encryption*
- *WPA2-CCMP (802.11i) encryption*

In addition, the Brocade Mobility 7131 Series Access Point supports the following additional security features:

- *Firewall security*
- *VPN tunnels*
- *Content filtering*

For an overview on the encryption and authentication schemes available, refer to *"Configuring Access Point Security" on page 191*.

Kerberos authentication

Authentication is a means of verifying information transmitted from a secure source. If information is *authentic*, you know who created it and you know 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. The access point 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 works. 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 detailed information on Kerbeors configurations, see "Configuring Kerberos authentication" on page 196.

EAP authentication

The *Extensible Authentication Protocol (EAP)* feature provides access points and their associated Clients 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 is a mutual authentication method whereby both the Client 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 Brocade Mobility 7131 Series Access Point. The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point by the user) and then transmits the user data back to the server to complete the authentication process.

A Client is not able to access the network if not authenticated. When configured for EAP support, the access point displays the Client 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 detailed information on EAP configurations, see "Configuring 802.1x EAP authentication" on page 198.

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 *key* is the specific code used by the algorithm to encrypt or decrypt the data. *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 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.

Wired Equivalent Privacy (WEP) is an encryption security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b and supported by the Brocade Mobility 7131 Series Access Point 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 Client and the access point. A Brocade Mobility 7131 Series Access Point and its associated wireless clients must use the same encryption key (typically 1 through 4) to interoperate.

For detailed information on WEP, see "Configuring WEP encryption" on page 202.

KeyGuard encryption

Use KeyGuard to shield the master encryption keys from being discovered through hacking. KeyGuard negotiation takes place between the access point and Client upon association. The access point can use KeyGuard with Motorola Clients.

For detailed information on KeyGuard configurations, see "Configuring KeyGuard encryption" on page 204.

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
- a re-keying mechanism

WPA uses an encryption method called *Temporal Key Integrity Protocol* (TKIP). WPA employs 802.1X and *Extensible Authentication Protocol* (EAP).

For detailed information on WPA using TKIP configurations, see "Configuring WPA/WPA2 using TKIP" on page 206.

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 Brocade Mobility 7131 Series Access Point provides.

For detailed information on WPA2-CCMP, see "Configuring WPA2-CCMP (802.11i)" on page 208.

Firewall security

A firewall keeps personal data in and hackers out. The Brocade Mobility 7131 Series Access Point's firewall prevents suspicious Internet traffic from proliferating the Brocade Mobility 7131 Series Access Point managed network. The Brocade Mobility 7131 Series Access Point 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 detailed information on configuring the Brocade Mobility 7131 Series Access Point's firewall, see "Configuring firewall settings" on page 213.

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 Brocade Mobility 7131 Series Access Point can function as a robust VPN gateway.

For detailed information on configuring VPN security support, see "Configuring VPN tunnels" on page 220.

Content filtering

Content filtering allows system administrators to block specific commands and URL extensions from going out through the Brocade Mobility 7131 Series Access Point's WAN port. 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 detailed information on configuring content filtering support, see "Configuring content filtering settings" on page 235.

VLAN support

A *Virtual Local Area Network (VLAN)* can electronically separate data on the same AP 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 Brocade Mobility 7131 Series Access Point. 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 access point 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 detailed information on configuring VLAN support, see "Configuring VLAN support" on page 116.

Multiple management accessibility options

The Brocade Mobility 7131 Series Access Point can be accessed and configured using one of the following:

- 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 Brocade Mobility 7131 Series Access Point's DB-9 serial port for direct access to the command-line interface from a PC. Use a Null-Modem cable for the best fitting connection.

Updatable firmware

Brocade periodically releases updated versions of device firmware to the Brocade Web site. If the Brocade Mobility 7131 Series Access Point firmware version displayed on the System Settings screen (see "Configuring system settings" on page 63) is older than the version on the Web site, Brocade recommends updating the Brocade Mobility 7131 Series Access Point to the latest firmware version for full feature functionality.

For detailed information on updating the Brocade Mobility 7131 Series Access Point firmware using FTP or TFTP, see "Updating device firmware" on page 108.

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 OID is used to uniquely identify each object variable of a MIB.

SNMP allows a network administrator to configure the access point, manage network performance, find and solve network problems, and plan network growth. The Brocade Mobility 7131 Series Access Point supports SNMP management functions for gathering information from its network components. The access point's download site contains MIB files supporting the Brocade Mobility 7131 Series Access Point:

The Brocade Mobility 7131 Series Access Point's 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 community names, thus providing backward compatibility.

For detailed information on configuring SNMP traps, see "Configuring SNMP settings" on page 86.

Client-Client transmission disallow

The access point's Client-Client Disallow feature prohibits Clients from communicating with each other even if on the same WLAN, assuming one of the WLAN's is configured to disallow Client-Client communication. Therefore, if an Client's WLAN is configured for Client-Client disallow, it will not be able to communicate with any other Clients connected to this access point.

For detailed information on configuring an Brocade Mobility 7131 Series Access Point WLAN to disallow Client to Client communications, see "Creating/editing individual WLANs" on page 139.

Voice prioritization

Each Brocade Mobility 7131 Series Access Point WLAN has the capability of having its QoS policy configured to prioritize the network traffic requirements for associated Clients. A WLAN QoS page is available for each enabled WLAN on either the 802.11a/n or 802.11b/g/n 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 Brocade Mobility 7131 Series Access Point 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 detailed information on configuring voice prioritization over other voice enabled devices, see "Setting the WLAN Quality of Service (QoS) policy" on page 147.

Support for CAM and PSP clients

The Brocade Mobility 7131 Series Access Point supports both CAM and PSP powered Clients. *CAM (Continuously Aware Mode)* Clients leave their radios on continuously to hear every beacon and message transmitted. These systems operate without any adjustments by the Brocade Mobility 7131 Series Access Point.

A beacon is a uniframe system packet broadcast by the AP to keep the network synchronized. A beacon includes the ESSID, MAC address, Broadcast destination addresses, a time stamp, a *DTIM (Delivery Traffic Indication Message)* and the *TIM (Traffic Indication Map)*.

PSP (Power Save Polling) Clients power off their radios for short periods. When a Client in PSP mode associates with a Brocade Mobility 7131 Series Access Point, it notifies the Brocade Mobility 7131 Series Access Point of its activity status. The Brocade Mobility 7131 Series Access Point responds by buffering packets received for the Client. PSP mode is used to extend an Client's battery life by enabling the Client to "sleep" during periods of inactivity.

Statistical displays

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point's 802.11a/n and 802.11b/g/n radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated Client stats can be displayed collectively and individually for specific Clients. An echo (ping) test is also available to ping specific Clients to assess association strength. Finally, the Brocade Mobility 7131 Series Access Point can detect and display the properties of other APs detected within its radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs.

For detailed information on available Brocade Mobility 7131 Series Access Point statistical displays and the values they represent, see "Monitoring Statistics" on page 259.

Transmit power control

The Brocade Mobility 7131 Series Access Point 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 access point's placement or network requirements as defined in the Brocade Mobility 7131 Series Access Point site survey.

For detailed information on setting the radio transmit power level, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

Advanced event logging capability

The Brocade Mobility 7131 Series Access Point periodically logs system events. Logging events is useful in assessing the throughput and performance of the Brocade Mobility 7131 Series Access Point or troubleshooting problems on the Brocade Mobility 7131 Series Access Point managed *Local Area Network* (LAN).

For detailed information on Brocade Mobility 7131 Series Access Point events, see "Logging configuration" on page 102.

Configuration file import/export functionality

Configuration settings for a Brocade Mobility 7131 Series Access Point can be downloaded from the current configuration of another Brocade Mobility 7131 Series Access Point. This affords the administrator the ability to save the current configuration before making significant changes or restoring a default configuration.

For detailed information on importing or exporting configuration files, see "Importing/exporting configurations" on page 103.

Default configuration restoration

The Brocade Mobility 7131 Series Access Point can 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 Clients the Brocade Mobility 7131 Series Access Point supports have been moved to different radio coverage areas.

For detailed information on restoring a default or partial default configuration, see "Configuring system settings" on page 63.

DHCP support

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point to send out a *DHCP request* searching for a *DHCP/BOOTP* server to acquire HTML, firmware or network configuration files when the Brocade Mobility 7131 Series Access Point boots. Because BOOTP and DHCP interoperate, whichever responds first becomes the server that allocates information.

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point is running (this parameter is programmed at the DHCP server). For example: Windows 2000 servers typically are set for 3 days.

Mesh networking

Utilize the new mesh networking functionality to allow the access point to function as a bridge to connect two Ethernet networks or as a repeater to extend your network's coverage area without additional cabling. Mesh networking is configurable in two modes. It can be set in a wireless client bridge mode and/or a wireless base bridge mode (which accepts connections from client bridges). These two modes are not mutually exclusive.

In client bridge mode, the access point scans to find other access points using the selected WLAN's ESSID. The access point must go through the association and authentication process to establish a wireless connection. The mesh networking association process is identical to the access point's Client association process. Once the association/authentication process is complete, the wireless client adds the connection as a port on its bridge module. This causes the access point (in client bridge mode) to begin forwarding configuration packets to the base bridge. An access point in base bridge mode allows the access point radio to accept client bridge connections.

The two bridges communicate using the *Spanning Tree Protocol* (STP). The spanning tree determines the path to the root and detects if the current connection is part of a network loop with another connection. Once the spanning tree converges, both access points begin learning which destinations reside on which side of the network. This allows them to forward traffic intelligently.

After the access point (in client bridge mode) establishes at least one wireless connection, it will begin beaconing and accepting wireless connections (if configured to support mobile users). If the access point is configured as both a client bridge and a base bridge, it begins accepting client bridge connections. In this way, the mesh network builds itself over time and distance.

Once the access point (in client bridge mode) establishes at least one wireless connection, it establishes other wireless connections in the background as they become available. In this way, the access point can establish simultaneous redundant links. An access point (in client bridge mode) can establish up to 3 simultaneous wireless connections with other access points. A client bridge always initiates the connections and the base bridge is always the acceptor of the mesh network data proliferating the network.

Since each access point can establish up to 3 simultaneous wireless connections, some of these connections may be redundant. In that case, the STP algorithm determines which links are the redundant links and disables the links from forwarding.

For an overview on mesh networking as well as details on configuring the access point's mesh networking functionality, see "Configuring Mesh Networking" on page 583.

Additional LAN subnet

In a typical retail or small office environment (wherein a wireless network is available along with a production WLAN) it is often necessary to segment a LAN into two subnets. Consequently, a second LAN is required to "segregate" wireless traffic.

The access point has a second LAN subnet enabling administrators to segment the access point's LAN connection into two separate networks. The main access point LAN screen now allows the user to select either LAN1 or LAN2 as the active LAN over the access point's Ethernet port. Both LANs can still be active at any given time, but only one can transmit over the access point's physical LAN connection. Each LAN has a separate configuration screen (called LAN 1 and LAN 2 by default) accessible under the main LAN screen. The user can rename each LAN as necessary. Additionally, each LAN can have its own Ethernet Type Filter configuration, and subnet access (HTTP, SSH, SNMP and telnet) configuration.

For detailed information on configuring the access point for additional LAN subnet support, see “Configuring the LAN interface” on page 113.

On-board Radius Server authentication

The access point can function as a Radius Server to provide user database information and user authentication. Several new screens have been added to the access point’s menu tree to configure Radius server authentication and configure the local user database and access policies. The new Radius Server functionality allows an administrator to define the data source, authentication type and associate digital certificates with the authentication scheme. The LDAP screen allows the administrator to configure an external LDAP Server for use with the access point. A new Access Policy screen enables the administrator to set WLAN access based on user groups defined within the User Database screen. Each user is authorized based on the access policies applicable to that user. Access policies allow an administrator to control access to a user groups based on the WLAN configurations.

For detailed information on configuring the access point for AAA Radius Server support, see “Configuring user authentication” on page 245.

Hotspot support

The access point allows hotspot operators to provide user authentication and accounting without a special client application. The access point uses a traditional Internet browser as a secure authentication device. Rather than rely on built-in 802.11security features to control access point association privileges, you can configure a WLAN with no WEP (an open network). The access point issues an IP address to the user using a DHCP server, authenticates the user and grants the user to access the Internet.

If a tourist visits a public hotspot and wants to browse a Web page, they boot their laptop and associate with a local Wi-Fi network by entering a valid SSID. They start a browser, and the hotspot’s access controller forces the un-authenticated user to a Welcome page (from the hotspot operator) that allows the user to login with a username and password. In order to send a redirected page (a login page), a TCP termination exists locally on the access point. Once the login page displays, the user enters their credentials. The access point connects to the Radius server and determines the identity of the connected wireless user. Thus, allowing the user to access the Internet once successfully authenticated.

For detailed information on configuring the access point for Hotspot support, see “Configuring WLAN hotspot support” on page 152.

Routing Information Protocol (RIP)

RIP is an interior gateway protocol that specifies how routers exchange routing-table information. The parent Router screen also allows the administrator to select the type of RIP and the type of RIP authentication used.

For detailed information on configuring RIP functionality as part of the access point’s Router functionality, see “Setting the RIP configuration” on page 180.

Manual date and time settings

As an alternative to defining a NTP server to provide access point system time, the access point can now have its date and time set manually. A new Manual Date/Time Setting screen can be used to set the time using a Year-Month-Day HH:MM:SS format.

For detailed information on manually setting the access point's system time, see "Configuring network time protocol (NTP)" on page 99.

Dynamic DNS

The access point supports the Dynamic DNS service. *Dynamic DNS* (or DynDNS) is a feature offered by *www.dyndns.com* allowing the mapping of domain names to dynamically assigned IP addresses. When the dynamically assigned IP address of a client changes, the new IP address is sent to the DynDNS service and traffic for the specified domain(s) is routed to the new IP address. For information on configuring Dynamic DNS, see "Configuring Dynamic DNS" on page 135.

Auto negotiation

Auto negotiation enables the access point to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when using the access point in an environment where different devices are connected and disconnected on a regular basis. For information on configuring the auto negotiation feature, see "Configuring the LAN interface" on page 113 or "Configuring WAN settings" on page 125.

Adaptive AP

An *adaptive AP* (AAP) is an Brocade Mobility 7131 Series Access Point that can adopt like a Brocade Mobility 300 Access Point . The management of an AAP is conducted by a controller, once the access point connects to a Brocade Mobility RFS4000 Controller, Brocade Mobility RFS6000 Controller or Brocade Mobility RFS7000 Controller and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- the tunneling of centralized traffic to the wireless controller

For a information overview of the adaptive AP feature as well as how to configure it, refer to "Adaptive AP" on page 613.

Rogue AP enhancements

The access point can scan for rogues over all channels on both of the access point's radio bands. The switching of radio bands is based on a timer with no user intervention required.

For information on configuring the access point for Rogue AP support, see "Configuring rogue AP detection" on page 238.

Bandwidth management enhancements

Use the Bandwidth Management screen to control the network bandwidth allotted to individual WLANs. Define a weighted scheme as needed when WLAN traffic supporting a specific network segment becomes critical. Bandwidth management is configured on a per-WLAN basis. With this segregated radio approach, bandwidth management can be configured uniquely for individual WLANs on different access point radios.

For information on configuring bandwidth management, see "Configuring client rate limiting" on page 177.

Radius time-based authentication

An external server maintains a users and groups database used by the access point for access permissions. Various kinds of access policies can be applied to each group. Individual groups can be configured with their own time-based access policy. Each group's policy has a user defined interval defining the days and hours access is permitted. Authentication requests for users belonging to the group are honored only during these defined hourly intervals.

For more information on defining access point access policies by group, see "Defining user access permissions by group" on page 254.

QBSS support

Each access point radio can be configured to optionally allow the access point to communicate channel usage data to associated devices and define the beacon interval used for channel utilization transmissions. The QBSS load represents the percentage of time the channel is in use by the access point and the access point's station count. This information is very helpful in assessing the access point's overall load on a channel, its availability for additional device associations and multi media traffic support.

For information on enabling QBSS and defining the channel utilization transmission interval, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

Triple radio support

The new Brocade Mobility 7131N Access Points are available in single, dual and three radio configurations. The third Mobility 7131N radio is never a WLAN radio. The third radio is either disabled or set to sensor mode. A radio's mode is called its RF function. By default, a radio's RF function is WLAN. A WLAN radio is a traditional access point radio that does not provide WIPS support. When a radio's RF function becomes WIPS, the radio takes on the role of what is typically referred to as a sensor.

NOTE
Since the only radio function allowed for the third radio is WIPS, there is no radio 3 submenu in the access point CLI.

For information on setting the configuration of a three radio model Mobility 7131N, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

IP filtering

IP filtering determines which IP packets are processed normally and which are discarded. If discarded, the packet is deleted and completely ignored (as if never received). Optionally apply different criteria to better refine which packets to filter.

IP filtering supports the creation of up to 20 filter rules enforced at layer 3. Once defined (using the access point's SNMP, GUI or CLI), filtering rules can be enforced on the access point's LAN1, LAN2 and WLAN interfaces. An additional default action is also available denying traffic when the filter rules fail. Lastly, imported and exported configurations retain their defined IP filtering configurations.

For information on configuring the access point's IP filtering functionality, see "Configuring IP filtering" on page 182.

Client rate limiting

client rate limiting enables an administrator to determine how much radio bandwidth is allocated to each client within any one of the 16 supported WLANs.

Before the 4.x firmware baseline, Mobility 7131 series access points supported bandwidth management on a per-WLAN basis. Each WLAN could be configured to receive (at most) a certain percentage of the total available downstream bandwidth. The new rate limiting feature is a replacement of the bandwidth management feature allowing for better client radio bandwidth allotments on a per WLAN basis.

To globally enable or disable the client rate limit and assess the WLANs in which it's currently invoked, see "Configuring client rate limiting" on page 177.

To define the actual client rate limit (maximum downstream bandwidth allocation in kbps), see "Creating/editing individual WLANs" on page 139.

Per radio client limit

Prior to the 4.x AP firmware baseline, a Brocade Mobility 7131 Series Access Point allowed a total of 127 client associations, regardless of the number of radios on the AP. With a dual-radio AP, if there were already 127 clients associated to one radio, that were no slots available for a client to associate with another radio.

An access point can now reserve slots on each radio so clients of one radio type (11a/n or 11bg/n) have better chances for AP association. Therefore, the total number of clients allowed to associate remains at 127, but you can now strategically distribute the 127 client associations between the data radios.

For information on setting the number of client associations on a specific radio, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

Power setting configuration

The access point's power management functionality automatically configures the AP's operational mode so it safely operates within available power. The power setting feature enables the user to select one of three power operating modes, 3af, 3at and full power. When an access point is operating in either 3af or 3at mode, the transmit power is always lower than the full power setting. With the introduction of the Brocade Mobility 7131N Access Point and its optional three radio SKU, the power options available amongst single, dual and three radio model access points has never been more diverse, and careful consideration must be made before deploying the access point.

The AP's hardware design uses a *complex programmable logic device* (CPLD). When an AP is powered on (or performing a cold reset), the CPLD determines the maximum power available to the AP by a POE device. Once an operational power configuration is defined, the AP firmware can read the power setting and configure operating characteristics based on the AP's SKU and power configuration. If the POE cannot provide sufficient power (with all interfaces enabled), the following interfaces could be disabled or modified:

- Radio transmit power could be reduced due to lack of sufficient power or the radio can be disabled
- The WAN port configuration could be changed (enabled or disabled)

For information on configuring the access point's power configuration, see "Configuring power settings" on page 67.

AMSDU transmission support

Aggregate MAC Service Data Unit (AMSDU) is an 802.11n specific MAC feature which enhances the transmission of multiple MSDU contents wrapped within a single preamble/packet infrastructure. The AMSDU transmission limit is set to 3839 bites by default.

For information on configuring AMSDU support for an access point radio, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167. AMSDU support can be defined by selecting the Set Aggregation button within the *Network Configuration -> Wireless -> Radio Configuration -> Radio1* screen.

IPSec VPN support

A VPN ensures data privacy between two end points, even while using a communication medium which is itself insecure (like the Internet). VPNs create a secure tunnel between two end points as if they are directly connected over a secure connection. Traffic is secured using a robust IPSec encryption technique.

You can get the safety of a VPN in a WLAN by hosting the VPN server at the access point, and the VPN client software on the client. For that reason, a VPN provides secure WLAN access to clients. A VPN solution was more common before 802.11i was introduced, but is not as common now, since 802.11i/WPA2 is considered more secure.

For information on configuring VPN support, see "Configuring VPN tunnels" on page 220. For instructions on configuring a IPSec VPN tunnel using two access points, see "Creating a VPN tunnel between two access points" on page 223.

Theory of operations

To understand Brocade Mobility 7131 Series Access Point management and performance alternatives, users need familiarity with Brocade Mobility 7131 Series Access Point functionality and configuration options. The Brocade Mobility 7131 Series Access Point includes features for different interface connections and network management.

The Brocade Mobility 7131 Series Access Point uses electromagnetic waves to transmit and receive electric signals without wires. Users communicate with the network by establishing radio links between *wireless clients* and access points.

The Brocade Mobility 7131 Series Access Point 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 carriers using a DSSS *chipping algorithm*. The Brocade Mobility 7131 Series Access Point radio signal propagates into the air as electromagnetic waves. A receiving antenna (on the Client) in the path of the waves absorbs the waves as electrical signals. The receiving Client interprets (demodulates) the signal by reapplying the direct sequence chipping code. This demodulation results in the original digital data.

The Brocade Mobility 7131 Series Access Point uses its environment (the air and certain objects) as the transmission medium.The Brocade Mobility 7131 Series Access Point can either transmit in the 2.4 to 2.5-GHz frequency range (802.11b/g/n radio) or the 5 GHz frequency range (802.11a/n radio), the actual range is country-dependent. Brocade 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:

- *Wireless coverage*
- *MAC layer bridging*
- *Media types*
- *Direct-Sequence Spread Spectrum*
- *Client association process*
- *Operating modes*
- *Management access options*
- *Brocade Mobility 7131 Series Access Point MAC address assignment*

Wireless coverage

A Brocade Mobility 7131 Series Access Point establishes an average communication range with Clients called a *Basic Service Set (BSS)* or cell. When in a particular cell, the Client associates and communicates with the Brocade Mobility 7131 Series Access Point supporting the radio coverage area of that cell. Adding Brocade Mobility 7131 Series Access Points to a single LAN establishes more cells to extend the range of the network. Configuring the same *ESSID (Extended Service Set Identifier)* on all Brocade Mobility 7131 Series Access Points makes them part of the same Wireless LAN.

Brocade Mobility 7131 Series Access Points with the same ESSID define a coverage area. A valid ESSID is an alphanumeric, case-sensitive identifier up to 32 characters. A Client searches for an Brocade Mobility 7131 Series Access Point with a matching ESSID and synchronizes (associates) to establish communications. This device association allows Clients within the coverage area to move

about or *roam.* As the Client roams from cell to cell, it associates with a different Brocade Mobility 7131 Series Access Point. The roam occurs when the Client analyzes the reception quality at a location and determines a different Brocade Mobility 7131 Series Access Point provides better signal strength and lower Client load distribution.

If the Client does not find a Brocade Mobility 7131 Series Access Point with a workable signal, it can perform a scan to find any AP. As Clients 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/n or 802.11b/g/n 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 Brocade Mobility 7131 Series Access Point to another like a phone system. WLANs can therefore be configured around the needs of specific groups of users, even when they are not in physical proximity.

MAC layer bridging

The Brocade Mobility 7131 Series Access Point provides *MAC layer bridging* between its interfaces. The Brocade Mobility 7131 Series Access Point monitors traffic from its interfaces and, based on frame address, forwards the frames to the proper destination. The access point tracks source and destination addresses to provide intelligent bridging as Clients roam or network topologies change. The Brocade Mobility 7131 Series Access Point also handles broadcast and multicast messages and responds to Client association requests.

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point. The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point internal stack interface handles all messages directed to the Brocade Mobility 7131 Series Access Point. Each Brocade Mobility 7131 Series Access Point stores information on destinations and their interfaces to facilitate *forwarding*. When a user sends an *ARP (Address Resolution Protocol)* request packet, the Brocade Mobility 7131 Series Access Point forwards it over all enabled interfaces except over the interface the ARP request packet was received.

On receiving the ARP response packet, the Brocade Mobility 7131 Series Access Point database keeps a record of the destination address along with the receiving interface. With this information, the Brocade Mobility 7131 Series Access Point forwards any directed packet to the correct destination. Transmitted ARP request packets echo back to other Clients. The access point removes from its database the destination or interface information not used for a specified time. The AP refreshes its database when it transmits or receives data from these destinations and interfaces.

Media types

The Brocade Mobility 7131 Series Access Point radio interface conforms to IEEE 802.11 specifications. The Brocade Mobility 7131 Series Access Point supports multiple-cell operations with fast roaming between cells. Within a direct-sequence system, each cell can operates independently. Adding cells to the network provides an increased coverage area and total system capacity.

The serial port provides a *Command Line Interface (CLI)* connection. The serial link supports a direct serial connection. The Brocade Mobility 7131 Series Access Point is a *Data Terminal Equipment (DTE)* device with male pin connectors for the RS-232 port. Connecting the Brocade Mobility 7131 Series Access Point to a PC requires a null modem serial cable.

Direct-Sequence 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 access point 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 Brocade Mobility 7131 Series Access Point 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 output signal.

Clients 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 Brocade Mobility 7131 Series Access Point. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting Brocade Mobility 7131 Series Access Point to the receiving Client. This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving Client 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 Brocade Mobility 7131 Series Access Point uses different modulation schemes to encode more bits per chip at higher data rates.

Client association process

A Brocade Mobility 7131 Series Access Point recognizes Clients as they begin the association process. A Brocade Mobility 7131 Series Access Point keeps a list of the Clients it services. Clients associate with a Brocade Mobility 7131 Series Access Point based on the following conditions:

- Signal strength between the Brocade Mobility 7131 Series Access Point and Client
- Number of Clients currently associated with the Brocade Mobility 7131 Series Access Point
- Clients encryption and authentication capabilities
- Clients supported data rate

Clients perform pre-emptive roaming by intermittently scanning for Brocade Mobility 7131 Series Access Point's and associating with the best available Brocade Mobility 7131 Series Access Point. Before roaming and associating, Clients perform full or partial scans to collect Brocade Mobility 7131 Series Access Point statistics and determine the direct-sequence channel used by the Brocade Mobility 7131 Series Access Point.

Scanning is a periodic process where the Client sends out probe messages on all channels defined by the country code. The statistics enable a Client to reassociate by synchronizing its channel to the Brocade Mobility 7131 Series Access Point. The Client continues communicating with that Brocade Mobility 7131 Series Access Point until it needs to switch cells or roam.

Clients perform partial scans at programmed intervals, when missing expected beacons or after excessive transmission retries. In a partial scan, the Client scans access points classified as proximate on the Brocade Mobility 7131 Series Access Point table. For each channel, the Client tests for *Clear Channel Assessment* (CCA). The Client 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 Brocade Mobility 7131 Series Access Point and updates the table.

An Client can roam within a coverage area by switching Brocade Mobility 7131 Series Access Points. Roaming occurs when:

- Unassociated Client attempts to associate or reassociate with an available Brocade Mobility 7131 Series Access Point
- Supported rate changes or the Client finds a better transmit rate with another Brocade Mobility 7131 Series Access Point
- *RSSI (received signal strength indicator)* of a potential Brocade Mobility 7131 Series Access Point exceeds the current Brocade Mobility 7131 Series Access Point
- Ratio of good-transmitted packets to attempted-transmitted packets that fall below a threshold.

A Client selects the best available Brocade Mobility 7131 Series Access Point and adjusts itself to the Brocade Mobility 7131 Series Access Point direct-sequence channel to begin association. Once associated, the Brocade Mobility 7131 Series Access Point begins forwarding frames addressed to the target Client. Each frame contains fields for the current direct-sequence channel. The Client uses these fields to resynchronize to the Brocade Mobility 7131 Series Access Point.

The scanning and association process continues for active Clients. This process allows Clients to find new Brocade Mobility 7131 Series Access Points and discard out-of-range or deactivated Brocade Mobility 7131 Series Access Points. By testing the airwaves, Clients can choose the best network connection available.

Operating modes

The Brocade Mobility 7131 Series Access Point can operate in a couple of configurations.

- *Access Point* - As an *Access Point*, the Brocade Mobility 7131 Series Access Point functions as a layer 2 bridge. The wired uplink can operate as a trunk and support multiple VLANs. Up to 16 WLANs can be defined and mapped to Brocade Mobility 7131 Series Access Point WLANs. Each WLAN can be configured to be broadcast by one or both Brocade Mobility 7131 Series Access Point radios. An Brocade Mobility 7131 Series Access Point can operate in both an Access Point mode and Wireless Gateway/Router mode simultaneously. The network architecture and access point configuration define how the Access Point and Wireless Gateway/Router mode are negotiated.
- *Wireless Gateway/Router* - If operating as a *Wireless Gateway/Router*, the access point functions as a router between two layer 2 networks: the WAN uplink (the ethernet port) and the Wireless side. The following options are available providing a solution for single-cell deployment:
  - *PPPoE* - The WAN interface can terminate a PPPoE connection, thus enabling the Brocade Mobility 7131 Series Access Point to operate in conjunction with a DSL or Cable modem to provide WAN connectivity.
  - *NAT - (Network Address Translation)* on the Wireless interface. Using NAT, the Brocade Mobility 7131 Series Access Pointrouter is able to manage a private IP scheme. NAT allows translation of private addresses to the WAN IP address.

- *DHCP* - The Brocade Mobility 7131 Series Access Point can assign private IP addresses.
- *Firewall* - A Firewall protects against a number of known attacks.

Management access options

Managing the Brocade Mobility 7131 Series Access Point includes viewing network statistics and setting configuration options. Statistics track the network activity of associated Clients and data transfers on the AP interfaces.

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point SNMP function using a MIB Browser. The access point's download site contains the following MIB files supporting the Brocade Mobility 7131 Series Access Point:

- BROCADE-CC-BR7131-MIB-2.0.mib (standard MIB file)
- BROCADE-BR7131-MIB.mib (relevant for use on an Brocade Mobility 7131 Series Access Point model access point)

Make configuration changes to Brocade Mobility 7131 Series Access Point's individually. Optionally, use the Brocade Mobility 7131 Series Access Point import/export configuration function to download settings to other access points.

For detailed information, see "Importing/exporting configurations" on page 103.

Brocade Mobility 7131 Series Access Point MAC address assignment

For an Brocade Mobility 7131 Series Access Point model access point, MAC address assignments are as follows:

- *WAN (GE2)* - The access point MAC address can be found underneath the access point chassis.
- *LAN1 (GE1)* - WAN MAC address + 1.
- *LAN2* - A virtual LAN not mapped to the LAN Ethernet port. This address is the lowest of the two radio MAC addresses.
- *Radio1 (802.11b/g/n)* - Random address located on the Web UI, CLI and SNMP interfaces.
- *Radio2 (802.11a/n)* - Random address located on the Web UI, CLI and SNMP interfaces.

The access point's BSS (virtual AP) MAC addresses are calculated as follows:

- *BSS1* - The same as the corresponding base radio's MAC address.
- *BSS2* - Base radio MAC address +1
- *BSS3* - Base radio MAC address +2
- *BSS4* - Base radio MAC address +3

1 Theory of operations

Chapter

Hardware Installation 2

In this chapter

- Precautions 31
- Requirements 31
- Package contents 31
- Access point placement 32
- Mounting a Brocade Mobility 7131 Series Access Point 35
- Brocade Mobility 7131 Series Access Point LED indicators 42
- Setting up clients 45

A Brocade Mobility 7131 Series Access Point access point installation includes mounting the access point, connecting the access point to the network, connecting antennae and applying power. Installation procedures vary for different environments.Brocade recommends conducting a radio site survey prior to installing an access point. A site survey is an excellent method of documenting areas of radio interference and providing a tool for device placement.

Precautions

Before installing a Brocade Mobility 7131 Series Access Point model access point verify the following:

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

Requirements

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

- A Brocade Mobility 7131 Series Access Point (either a dual or single radio model)
- 48 Volt Power Supply (Part No. 50-14000-247R)
- A power outlet
- Dual-band antennae or an antenna specifically supporting the AP's 2.4 or 5 GHz band

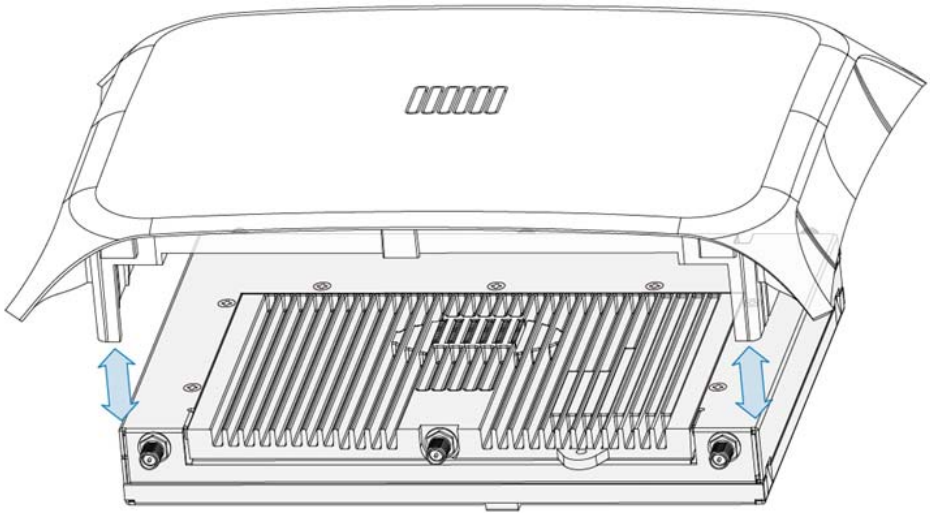
Package contents

Check package contents for the correct model and applicable Brocade Mobility 7131 Series Access Point accessories. Each available configuration (at a minimum), contains:

- Brocade Mobility 7131 Series Access Point model access point (accessories dependent on SKU ordered)
- Brocade Mobility 7131 Series Access Point Installation Guide
- China ROHS compliance addendum
- Wall mount screw and anchor kit
- Accessories Bag (4 rubber feet and a LED light pipe and badge with label for above the ceiling installations)

Contact the Brocade Support Center to report missing or improperly functioning items.

NOTE
The access point façade with 6 Element Antenna (Part No. ML-2452-PTA2M3X3-2) is separately orderable and provides an integrated antenna option. The facade connects to the access point as illustrated. Once attached, the Brocade Mobility 7131 Series Access Point's LEDs continue to illuminate through the facade. Contact your Brocade sales associate for information on ordering a facade with your Brocade Mobility 7131 Series Access Point.



Access point placement

For optimal performance, install the access point 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 access point in an open area 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 access point using the following guidelines:

- Install the access point at an ideal height of 10 feet from the ground.
- Orient the access point antennas vertically for best reception.
- Point the access point antennas downward if attaching to the ceiling.

To maximize the access point's radio coverage area, Brocade recommends conducting a site survey to define and document radio interference obstacles before installing the access point.

Site surveys

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

Brocade recommends conducting a new site survey and developing a new coverage area floor plan when switching from a Brocade Mobility 5181 Access Point to a Brocade Mobility 7131 Series Access Point model, as the device placement requirements *could be* significantly different.

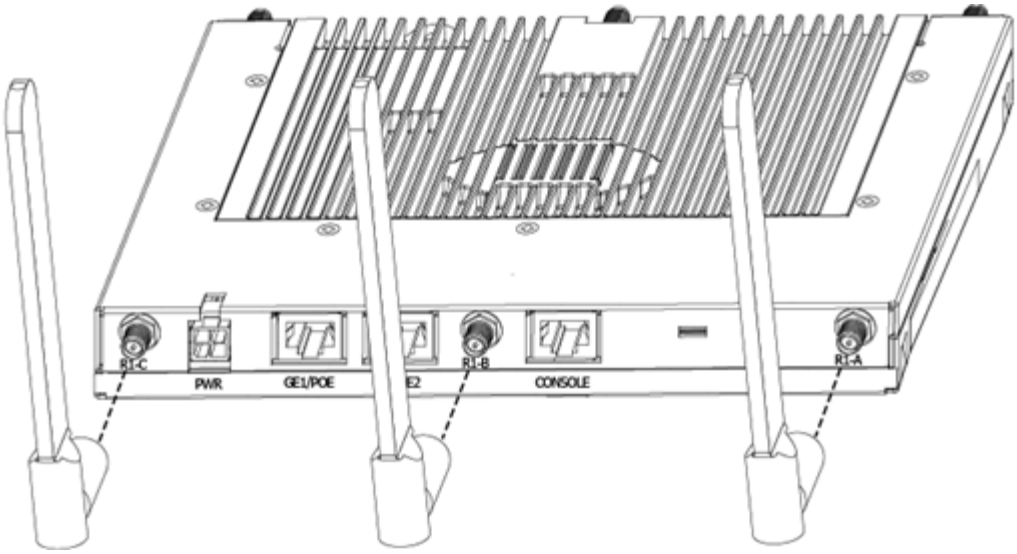
Antenna options

Brocade supports two antenna suites for the Brocade Mobility 7131 Series Access Point. One antenna suite supporting the 2.4 GHz band and another antenna suite supporting the 5 GHz band. Select an antenna model best suited to the intended operational environment of your Brocade Mobility 7131 Series Access Point. The Moblity 7131N model access point can be purchased in a three radio configuration. If a three radio SKU is purchased, the access point ships with a single antenna, factory connected, to the access point chassis (next to the existing R1-A connector). This antenna is in addition to the other six antennas available to the access point's other two radios. The single antenna supporting the Moblity 7131N's third radio supports sensor mode only and can not function as a WLAN radio.

NOTE

On a single-radio Brocade Mobility 7131 Series Access Point, Radio 1 can be configured to be either a 2.4 GHz or 5 GHz radio. On a dual-radio model, Radio 1 refers to the Brocade Mobility 7131 Series Access Point's 2.4 GHz radio and Radio 2 refers to the Brocade Mobility 7131 Series Access Point 5 GHz radio. However, there could be some cases where a dual-radio Brocade Mobility 7131 Series Access Point is performing a Rogue AP detector function. In this scenario, the Brocade Mobility 7131 Series Access Point is receiving in either 2.4 GHz or 5 GHz over the Radio 1 or Radio 2 antennae depending on which radio is selected for the scan.

Antenna connectors for single radio model Brocade Mobility 7131 Series Access Points are located on the same side of the access point as the LAN and WAN port connections (GE1/POE and GE2). 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.



R1 defines the Brocade Mobility 7131 Series Access Point's radio 1 antenna connectors and R2 defines the Brocade Mobility 7131 Series Access Point's radio 2 antenna connectors.

The Brocade Mobility 7131 Series Access Point 2.4 GHz antenna suite includes the following models:

Part No.	Antenna type	Nominal net gain (dBi)
ML-2499-11PNA2-01R	Wide Angle Directional	8.5
ML-2499-HPA3-01R	Omni-Directional Antenna	3.3
ML-2499-BYGA2-01R	Yagi Antenna	13.9
ML-2452-APA2-01	Dual-Band	3.0
ML-2452-PTA2M3X3-2	Facade with 6 Element Antenna Module	2.0
ML-2452-PTA3M3-036	3 Port MIMO Antenna	3.0

NOTE
An additional adapter is required to use ML-2499-11PNA2-01 and ML-2499-BYGA2-01 model antennae. Please contact Brocade for more information.

The Brocade Mobility 7131 Series Access Point 5 GHz antenna suite includes the following models:

Part No.	Antenna type	Nominal net gain (dBi)
ML-5299-WPNA1-01R	Panel Antenna	13.0
ML-5299-HPA1-01R	Wide-Band Omni-Directional Antenna	5.0
ML-2452-APA2-0	Dual-Band	4.0
ML-2452-PTA2M3X3-2	Facade with 6 Element Antenna Module	2.0
ML-2452-PTA3M3-036	3 Port MIMO Antenna	3.0

For detailed specifications on the 2.4 GHz and 5 GHz antennae mentioned in this section, see section "2.4 GHz antenna matrix" on page 633 and section "5 GHz antenna matrix" on page 633. For a more exhaustive overview of the antennas and associated components supported by the Brocade access point family, refer to the *Enterprise Wireless LAN Antenna Specification Guide* available at *http://www.brocade.com.*

Mounting a Brocade Mobility 7131 Series Access Point

The Brocade Mobility 7131 Series Access Point can 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 Brocade Mobility 7131 Series Access Point in a location that has not been approved in a site survey.

Refer to the following, depending on how you intend to mount the Brocade Mobility 7131 Series Access Point:

- *Wall mounted installations*
- *Suspended ceiling T-Bar installations*
- *Above the ceiling (plenum) installations*

Wall mounted installations

Wall mounting requires hanging the Brocade Mobility 7131 Series Access Point along its width (or length) using the pair of slots on the bottom of the unit and using the Brocade Mobility 7131 Series Access Point mounting template for the screws.

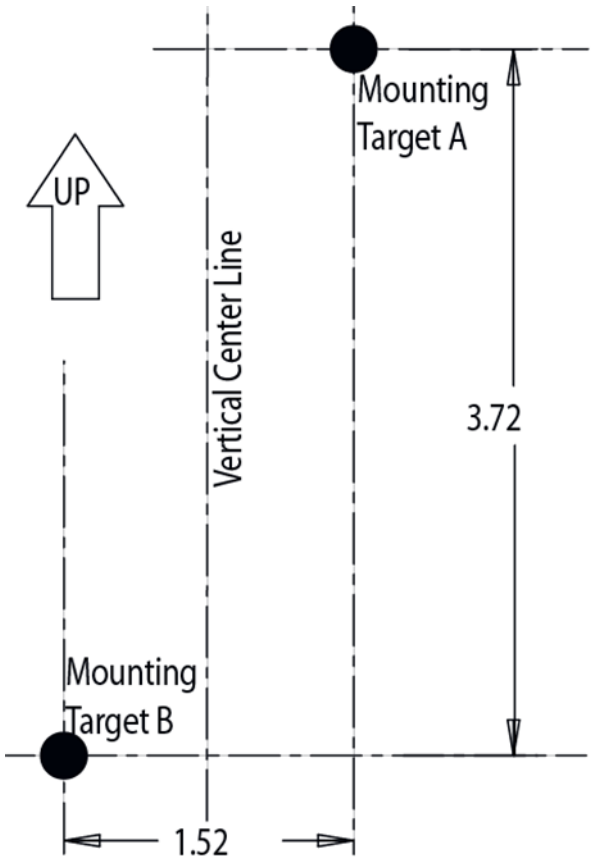
CAUTION

A Brocade Mobility 7131 Series Access Point should be wall mounted to concrete or plaster-wall-board (dry wall) only. Do not wall mount a Brocade Mobility 7131 Series Access Point to combustible surfaces.

The hardware and tools (customer provided) required to install the Brocade Mobility 7131 Series Access Point 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
- Wall mount template (included on next page)
- Security cable (optional)

To mount the Brocade Mobility 7131 Series Access Point on a wall using the provided template:


Mounting
Target A
UP
Vertical Center Line
3.72
Mounting
Target B
1.52

1. Photocopy the template (on the previous page) to a blank piece of paper. Do not reduce or enlarge the scale of the template.

CAUTION

If printing the mounting template (on the previous page) from an electronic PDF, dimensionally confirm the template by measuring each value for accuracy.

2. Tape the template to the wall mounting surface.
   - If the installation requires the antenna be positioned vertically, the centerline reference (of the template) needs to be positioned vertically. The cabling shall exit the access point in a vertical direction.
   - If the installation requires the antenna be positioned horizontally, the vertical centerline (of the template) needs to be positioned horizontally. The cabling shall exit the access point in a horizontal direction.
3. At mounting targets A and B, mark the mounting surface through the template at the target center.
4. Discard the mounting template.
5. 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.
6. If required, install and attach a security cable to the Brocade Mobility 7131 Series Access Point lock port.
7. Attach the antennas to their correct connectors.

   For more information on the antennas available to the Brocade Mobility 7131 Series Access Point, see “Antenna options” on page 33.
8. Place the large center opening of each of the mount slots over the screw heads.
9. Slide the Brocade Mobility 7131 Series Access Point down along the mounting surface to hang the mount slots on the screw heads.

CAUTION

Ensure you are placing the antennas on the correct connectors (depending on your single or dual-radio model and frequency used) to ensure the successful operation of the Brocade Mobility 7131 Series Access Point.

NOTE

It is recommended the Brocade Mobility 7131 Series Access Point be mounted with the RJ45 cable connector oriented upwards or downwards to ensure proper operation.

10. Cable the Brocade Mobility 7131 Series Access Point using an approved line cord and power supply.
11. Verify the behavior of the Brocade Mobility 7131 Series Access Point LEDs. For more information, see “Brocade Mobility 7131 Series Access Point LED indicators” on page 42.

The Brocade Mobility 7131 Series Access Point is ready to configure. For information on a Brocade Mobility 7131 Series Access Point default configuration, see "Getting Started" on page 49. For specific details on Brocade Mobility 7131 Series Access Point system configurations, see "System Configuration" on page 63.

Suspended ceiling T-Bar installations

A suspended ceiling mount requires holding the Brocade Mobility 7131 Series Access Point up against the T-bar of a suspended ceiling grid, and twisting the Brocade Mobility 7131 Series Access Point chassis onto the T-bar.

The mounting tools (customer provided) and hardware required to install the Brocade Mobility 7131 Series Access Point on a ceiling
T-bar consists of:

- Safety wire (recommended and customer supplied)
- Security cable (and customer supplied)

To install the Brocade Mobility 7131 Series Access Point on a ceiling T-bar:

1. Brocade recommends you 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 Brocade Mobility 7131 Series Access Point's console connector) and secure the loop.
2. If desired, install and attach a security cable to the Brocade Mobility 7131 Series Access Point lock port.
3. Attach the radio antennas to their correct connectors.

   For more information on the antennas available to the Brocade Mobility 7131 Series Access Point, see "Antenna options" on page 33.
4. Cable the Brocade Mobility 7131 Series Access Point using the Brocade Mobility 7131 Series Access Point approved power supply.

CAUTION

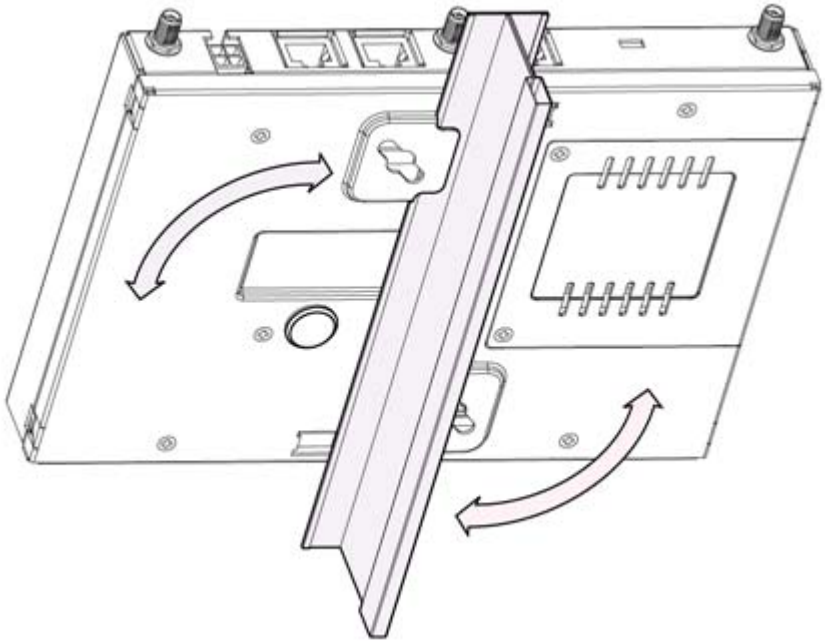
Do not supply power to the Brocade Mobility 7131 Series Access Point until the cabling of the unit is complete.

5. Verify the behavior of the Brocade Mobility 7131 Series Access Point LEDs. For more information, see "Brocade Mobility 7131 Series Access Point LED indicators" on page 42.
6. Align the bottom of the ceiling T-bar with the back of the Brocade Mobility 7131 Series Access Point.
7. Orient the Brocade Mobility 7131 Series Access Point chassis by its length and the length of the ceiling T-bar.
8. Rotate the Brocade Mobility 7131 Series Access Point chassis 45 degrees clockwise.
9. Push the back of the Brocade Mobility 7131 Series Access Point chassis on to the bottom of the ceiling T-bar.

CAUTION

Ensure the safety wire and cabling used in the T-Bar Brocade Mobility 7131 Series Access Point installation is securely fastened to the building structure in order to provide a safe operating environment.

10. Rotate the Brocade Mobility 7131 Series Access Point chassis 45 degrees counter-clockwise. The clips click as they fasten to the T-bar.



11. The Brocade Mobility 7131 Series Access Point is ready to configure. For information on a Brocade Mobility 7131 Series Access Point default configuration, see "Getting Started" on page 49. For specific details on Brocade Mobility 7131 Series Access Point system configurations, see "System Configuration" on page 63.

Above the ceiling (plenum) installations

A Brocade Mobility 7131 Series Access Point above the ceiling installation requires placing the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point installation enables installations compliant with drop ceilings, suspended ceilings and industry standard tiles from .625 to .75 inches thick.

NOTE

The Brocade Mobility 7131 Series Access Point is Plenum rated to UL2043 and NEC1999 to support above the ceiling installations.

CAUTION

Brocade does not recommend mounting the Brocade Mobility 7131 Series Access Point 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.). Brocade strongly recommends fitting the Brocade Mobility 7131 Series Access Point 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.

The mounting hardware required to install the Brocade Mobility 7131 Series Access Point above a ceiling consists of:

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

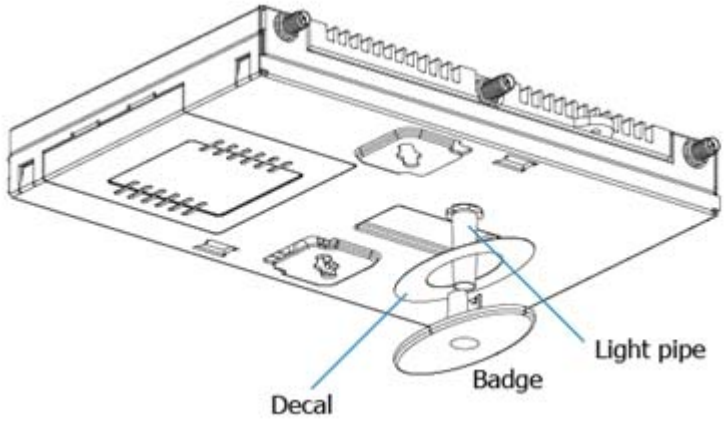
To install the Brocade Mobility 7131 Series Access Point above a ceiling:

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 Brocade Mobility 7131 Series Access Point'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 Brocade Mobility 7131 Series Access Point LED light pipe.

CAUTION

Brocade 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 Brocade Mobility 7131 Series Access Point. Align the tabs and rotate approximately 90 degrees. Do not over tighten



9. Fit the light pipe into hole in the tile from its unfinished side.
10. Place the decal on the back of the badge and slide the badge onto the light pipe from the finished side of the tile.
11. Attach the radio antennas to their correct connectors.

    For more information on the antennas available to the Brocade Mobility 7131 Series Access Point, see "Antenna options" on page 33.
12. Brocade recommends attaching safety wire to the Brocade Mobility 7131 Series Access Point safety wire tie point or security cable (if used) to the Brocade Mobility 7131 Series Access Point's lock port.
13. Align the ceiling tile into its former ceiling space.
14. Cable the Brocade Mobility 7131 Series Access Point using an approved line cord and power supply.

CAUTION

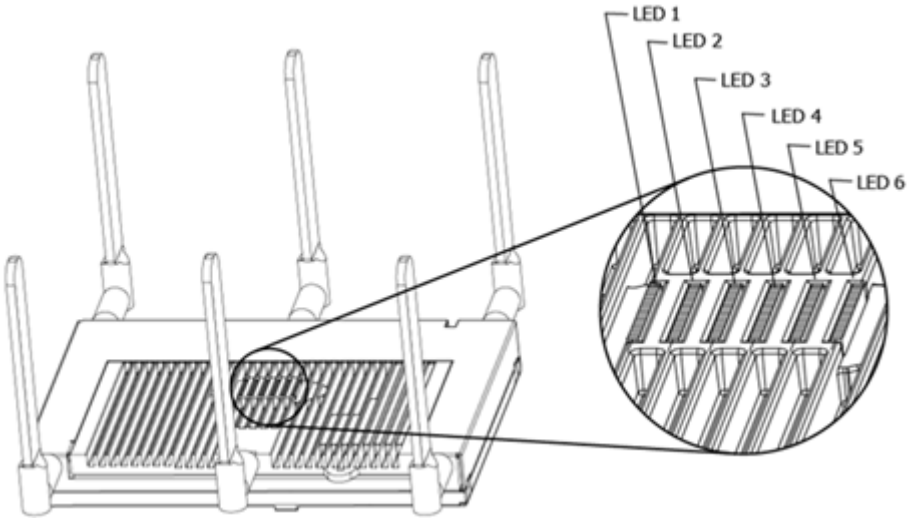
Do not supply power to the Brocade Mobility 7131 Series Access Point until the cabling of the unit is complete.

15. Verify the behavior of the Brocade Mobility 7131 Series Access Point LED lightpipe. For more information, see "Brocade Mobility 7131 Series Access Point LED indicators" on page 42.
16. Place the ceiling tile back in its frame and verify it is secure.

    The Brocade Mobility 7131 Series Access Point is ready to configure. For information on a Brocade Mobility 7131 Series Access Point default configuration, see "Getting Started" on page 49. For specific details on Brocade Mobility 7131 Series Access Point system configurations, see "System Configuration" on page 63.

Brocade Mobility 7131 Series Access Point LED indicators

Five LEDs illuminate on the front of the Brocade Mobility 7131 Series Access Point (on top of the Brocade Mobility 7131 Series Access Point housing) for dual radios models and four illuminate for single radio models. One LED (for above the ceiling installations) is located on the back of the device.



NOTE
The LED blink rate is proportional to activity. The busiest traffic corresponds to the fastest blink, while the slowest traffic corresponds to slowest blink.

NOTE
Depending on how the 5 GHz and 2.4 GHz radios are configured, the LEDs will blink at different intervals between amber and yellow (5 GHz radio) and emerald and yellow (2.4 GHz radio).

The LEDs on the top housing of the Brocade Mobility 7131 Series Access Point are clearly visible in wall and below ceiling installations. The top housing LEDs have the following display and functionality:

Three Radio Mobility 7131N LEDs

A three radio model Mobility 7131N has the following unique LED behavior:

LED 1	LED 2 (LAN)	LED 3 (WAN)	LED 4 - 5 GHz	LED 5 - 2.4 GHz	LED 6
Blinking **Red** indicates booting. Solid **Red** defines the diagnostic mode. **White** defines normal operation.	**Green** defines normal GE1 operation.	**Green** defines normal GE2 operation.	Blinking **Amber** indicates 802.11a activity. A 5 second **Amber** and **Yellow** blink rate defines 802.11an activity. A 2 second **Amber** and **Yellow** blink rate defines 802.11an (40 MHz) activity. When functioning as a sensor, LED alternates between **Amber** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Blinking **Emerald** indicates 802.11bg activity. A 5 second **Emerald** and **Yellow** blink rate defines 802.11bgn activity. A 2 second **Emerald** and **Yellow** blink rate defines 802.11bgn (40 MHz) activity. When functioning as a sensor, LED alternates between **Emerald** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Blinking **Emerald** indicates the radio is defined as a sensor, but is disabled. Alternates between **Emerald** and **Amber** when the radio is defined as a sensor with no Server connected. The blink interval is 1 second. Alternates between **Emerald** and **Amber** when the radio is defined as a sensor and a Server is connected. The blink interval is 0.5 seconds.

Dual radio (2.4/5 GHz) Brocade Mobility 7131 Series Access Point

A dual radio (2.4/5 Ghz) model Brocade Mobility 7131 Series Access Point has the following unique LED behavior:

LED 1	LED 2	LED 3	LED 4 - 5 GHz	LED 5 - 2.4 GHz	LED 6
Blinking **Red** indicates booting. Solid Red defines a failure condition. **White** defines normal operation	**Green** defines normal GE1 operation. **Yellow** defines a collision	**Green** defines normal GE2 operation. **Yellow** defines a collision	**Amber** defines 5 GHz radio as configured. When functioning as a sensor, LED alternates between **Amber** and **Yellow**. The blink interval is 0.5 seconds.	**Emerald** defines 2.4 GHz radio as configured. When functioning as a sensor, LED alternates between **Emerald** and **Yellow**. The blink interval is 0.5 seconds.	Not used

Single radio 2.4 GHz Brocade Mobility 7131 Series Access Point LEDs

The single 2.4 Ghz radio model Brocade Mobility 7131 Series Access Point has the following unique LED behavior:

LED 1	LED 2	LED 3	LED 4 - 5 GHz	LED 5 - 2.4 GHz	LED 6
Blinking **Red** indicates booting. Solid **Red** defines a failure condition. **White** defines normal operation	**Green** defines normal GE1 operation. **Yellow** defines a collision	**Green** defines normal GE2 operation. **Yellow** defines a collision	Off	**Emerald** defines 2.4 GHz radio as configured. When functioning as a sensor, LED alternates between **Emerald** and **Yellow**. The blink interval is 0.5 seconds.	Not used

Single radio 5 GHz Brocade Mobility 7131 Series Access Point LEDs

The single 5 Ghz radio model Brocade Mobility 7131 Series Access Point has the following unique LED behavior:

LED 1	LED 2	LED 3	LED 4 - 5 GHz	LED 5 - 2.4 GHz	LED 6
Blinking **Red** indicates booting. Solid **Red** defines a failure condition. **White** defines normal operation	**Green** defines normal GE1 operation. **Yellow** defines a collision	**Green** defines normal GE2 operation. **Yellow** defines a collision	**Amber** defines 5 GHz radio as configured. When functioning as a sensor, LED alternates between **Amber** and **Yellow**. The blink interval is 0.5 seconds.	Off	Not used

Rear Brocade Mobility 7131 Series Access Point LED

The LED on the rear (bottom) of the Brocade Mobility 7131 Series Access Point is viewed using a single (customer installed) extended light pipe, adjusted as required to suit above the ceiling installations. The LED displayed using the light pipe has the following color display and functionality:

LED 7
Blinking **Red** indicates booting. Solid **Red** defines a failure condition. **White** defines normal operation.

Setting up clients

802.11n clients

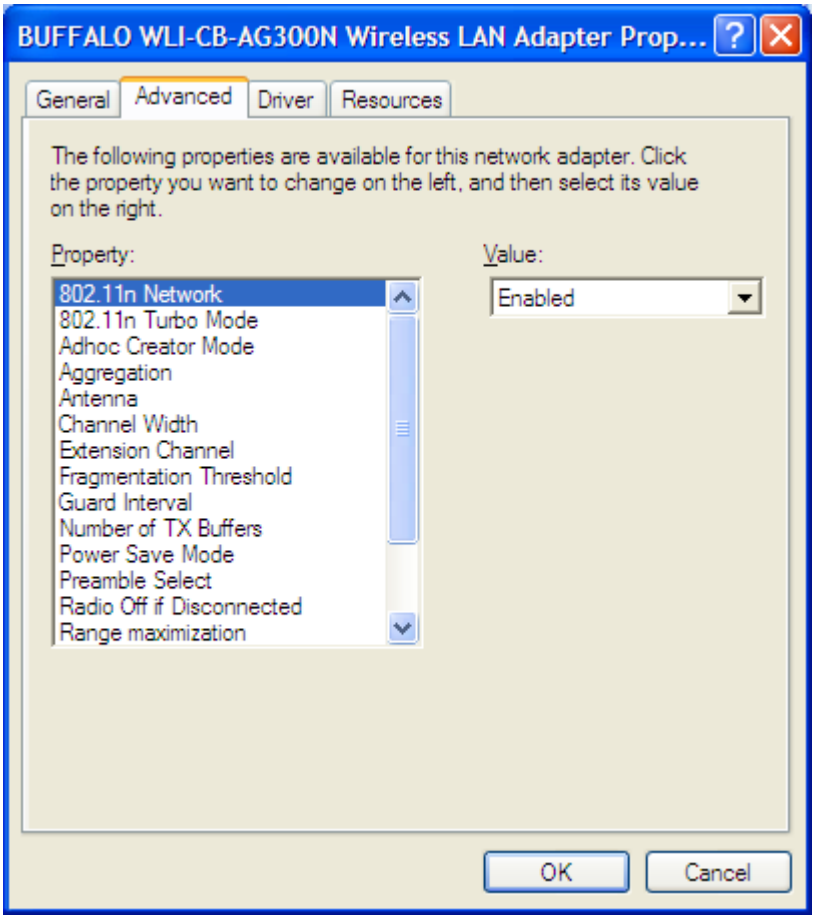
Third-party 802.11n clients can connect to a Brocade Mobility 7131 Series Access Point using default settings with no additional user intervention. However, there could be instances where the specific (high-performance) 802.11n settings cannot be sustained due to adverse radio traffic conditions within the network. When this occurs, Brocade recommends changing the Windows XP settings so the adapter can use settings defined for legacy (802.11a/bg) adapter operation. Once network conditions improve, use Windows XP to re-enable the adapter for 802.11n support.

To change the Brocade Mobility 7131 Series Access Point's settings to support legacy 802.11a/bg operation (using Windows XP):

1. Select *My Network Places.*
2. Right-click and select *Properties.* The *Network Connections* screen displays.
3. Select (right-click on) the adapter supporting 802.11n operation with the Brocade Mobility 7131 Series Access Point and select *Properties*.
4. Click on the *Configure* button.

   The Network Connection screen displays supporting the 802.11n adapter.
5. Select the *Advanced* tab.
6. Select *802.11n Network* from the Property field and select either *Enable* or *Disable* from the Value drop-down menu.

   Select *Disable* when the 802.11n rate settings and performance values defined on the Brocade Mobility 7131 Series Access Point cannot be sustained (due to network congestion or interference). Once network conditions improve to the point where 802.11n traffic can be sustained, enable the *802.11n Network* parameter once again.



NOTE
If re-enabling the adapter for 802.11 support, ensure additional 802.11n settings (*Aggregation*, *Channel Width*, *Guard Interval* etc.) are also enabled to ensure optimal operation.

7. Click *OK* to save the updates to the adapter's configuration.

Chapter

Getting Started 3

In this chapter

- Installing the access point 49
- Configuration options 49
- Initially connecting to the access point 50
- Basic device configuration 51

The access point should be installed in an area tested for radio coverage using one of the site survey tools available to the 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*.

Installing the access point

Make the required cable and power connections before mounting the access point in its final operating position. Test the access point with an associated Client before mounting and securing the access point. Carefully follow the mounting instructions in one of the following sections to ensure the Brocade Mobility 7131 Series Access Point access point is installed correctly:

- For instructions on mounting a Brocade Mobility 7131 Series Access Point to a wall, see "Wall mounted installations" on page 35.
- For instructions on mounting a Brocade Mobility 7131 Series Access Point to a ceiling T-bar, see "Suspended ceiling T-Bar installations" on page 38.
- For instructions on installing the Brocade Mobility 7131 Series Access Point in an above the ceiling attic space, see "Above the ceiling (plenum) installations" on page 39.

For information on the antenna suite available to the Brocade Mobility 7131 Series Access Point, see "Antenna options" on page 33. To verify Brocade Mobility 7131 Series Access Point LED behavior once installed, see "Brocade Mobility 7131 Series Access Point LED indicators" on page 42.

Configuration options

Once installed and powered, a Brocade Mobility 7131 Series Access Point can be configured using one of several connection techniques. Managing the Brocade Mobility 7131 Series Access Point includes viewing network statistics and setting configuration options. The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point default configuration, see "Basic device configuration" on page 51 or chapters 4 through 7 of this guide.

- *Command Line Interface (CLI)* via Serial, Telnet and SSH. The access point CLI is accessed through the 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 access point, see "CLI Reference" on page 291.
- *Config file* - Readable text file; Importable/Exportable via FTP, TFTP and HTTP. Configuration settings for an access point can be downloaded from the current configuration of another access point meeting the import/export requirements. For information on importing or exporting configuration files, see "Importing/exporting configurations" on page 103.
- *MIB (Management Information Base)* accessing the Brocade Mobility 7131 Series Access Point SNMP functions using a MIB Browser

Initially connecting to the access point

NOTE
The procedures described below assume this is the first time you are connecting to a Brocade Mobility 7131 Access Point or a Brocade Mobility 7131N Access Point.

NOTE
The computer being used should be configured to use the same IP address and subnet mask as the Brocade Mobility 7131 Series Access Point.

Connecting to the Brocade Mobility 7131 Series Access Point using the WAN port

To initially connect to the access point using the access point's WAN port:

1. Connect AC power to the access point, as Power-Over-Ether support is not available on the access point's WAN (or GE2) port.
2. Start a browser and enter the access point's static IP address (10.1.1.1). The default password is "*admin123*."
3. Refer to "Basic device configuration" on page 51 for instructions on the initial (basic) configuration of the access point.

Connecting to the Brocade Mobility 7131 Series Access Point using the LAN port

To initially connect to the access point using the access point's LAN port:

1. The LAN (or GE1/POE) port default is set to DHCP. Connect the access point's GE1/POE port to a DHCP server.

   The access point will receive its IP address automatically.
2. To view the IP address, connect one end of a null modem serial cable to the access point and the other end to the serial port of a computer running HyperTerminal or similar emulation program.
3. Configure the following settings:

- Baud Rate - 19200
- Data Bits - 8
- Stop Bits - 1
- No Parity
- No Flow Control

4. Press <ESC> or <Enter> to access the access point CLI.
5. Enter the default username of "*admin*" and the default password of "*admin123*"

   As this is the first time you are logging into the access point, you are prompted to enter a new password and set the county code. Refer to "Country codes" on page 634 for a list of each available countries two digit country code.
6. At the CLI prompt (admin>), type "*summary*."

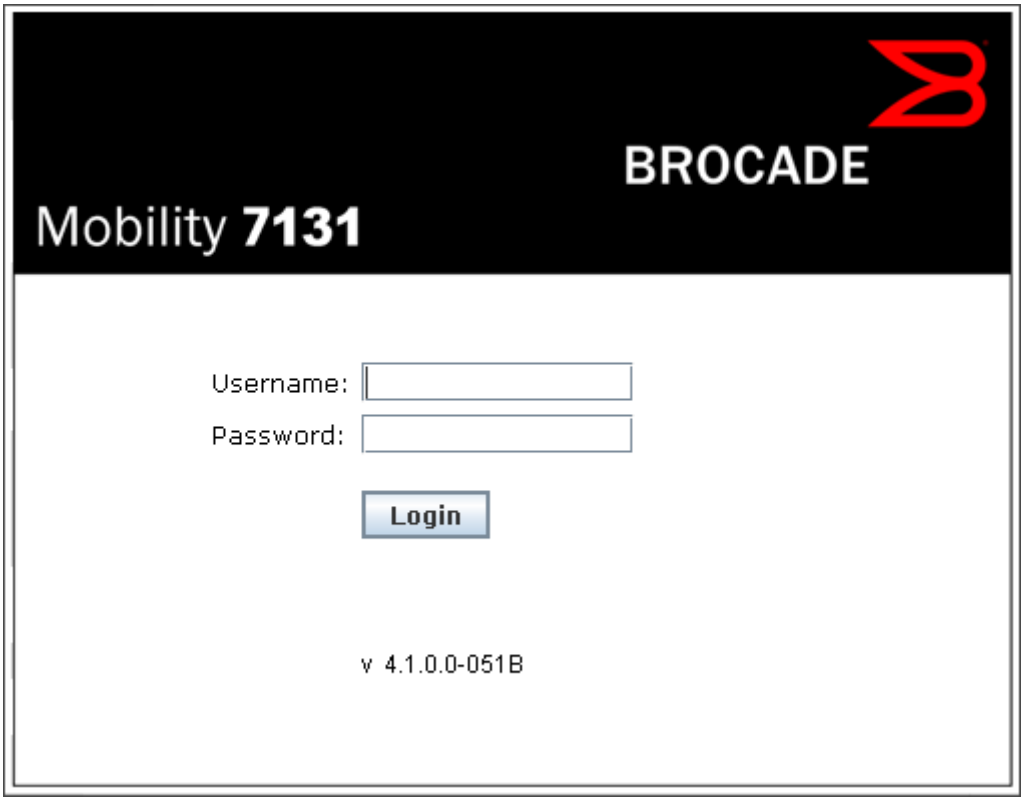
   The access point's LAN IP address will display.
7. Using a Web browser, use the access point's IP address to access the access point.
8. Refer to "Basic device configuration" on page 51 for instructions on the initial (basic) configuration of the access point.

Basic device configuration

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

1. Log in using *admin* as the default Username and *admin123* as the default Password. Use your new password if it has been updated from default.

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.



2. If the default login is successful, the *Change Admin Password* window displays. Change the password.

Enter the current password and a new admin password in fields provided. Click *Apply*. Once the admin password has been updated, a warning message displays stating the access point must be set to a country.

The export function will always export the encrypted Admin User password. The import function will import the Admin Password only if the access point is set to factory default. If the access point is not configured to factory default settings, the Admin User password WILL NOT get imported.

NOTE
.Though the Brocade Mobility 7131 Series Access Point can have its basic settings defined using a number of different screens, Brocade recommends using the Brocade Mobility 7131 Series Access Point *Quick Setup* screen to set the correct country of operation and define its minimum required configuration from one convenient location.

Configuring device settings

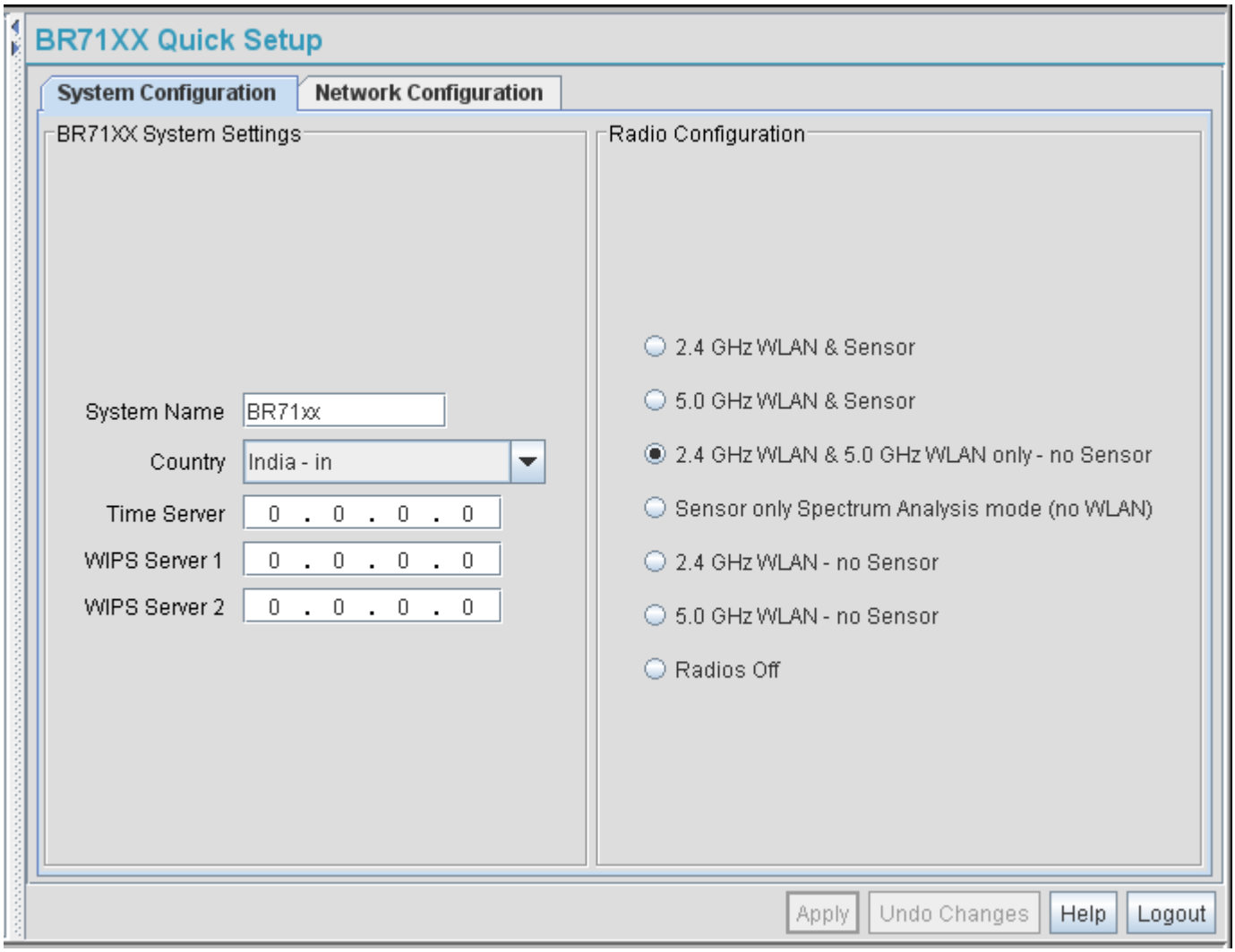
Configure a set of minimum required device settings within the *Quick Setup* screen. The values defined within the Quick Setup screen are also configurable in numerous other locations within the menu tree. When you change the settings in the Quick Setup screen, the values also change within the screen 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.

NOTE
A scheme for radio configuration and WIPS server management has been added within the Quick Setup GUI applet. Up to eight radio buttons are now available (depending on the number radios supported by the SKU). These radio buttons define how WLAN and sensor functionality are supported amongst the radios available to the access point. The options available depend on the SKU supported (and are described within this section).

To define a basic access point configuration:

1. Select *System Configuration -> Quick Setup* from the menu tree, if the Quick Setup screen is not already displayed.
2. Select the *System Configuration* tab to define the access point's system, WIPS server and radio configuration.

NOTE
The WIPS Server designation and radio configuration is defined as part of the access point's quick setup. For a description of sensor functionality and how it relates to access point operation, see "Sensor support" on page 7.



3. Refer to the *System Settings* field to define the following parameters:

System Name	Assign a System Name to define a title for this access point. The System Name is useful if multiple devices are being administered.
Country	Select the *Country* for the access point's country of operation. The access point prompts for the correct country code on the first login. A warning message also displays stating an incorrect country setting may result in illegal radio operation. Selecting the correct country is central to legally operating the access point. 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, set the country accurately. CLI and MIB users cannot configure their access point until a two character country code (for example, United States - us) is set. Refer to "Country codes" on page 634 for the two character country codes.

Time Server	Optionally enter the IP address of the server used to provide system time to the access point within the *Time Server* field. Once the IP address is entered, the access point's *Network Time Protocol (NTP)* functionality is engaged automatically. Refer to "Configuring network time protocol (NTP)" on page 99 (if necessary) for information on setting alternate time servers and setting a synchronization interval for the access point to adjust its displayed time.
WIPS Servers	Define a primary and alternate WIPS server IP Address for WIPS Server 1 and 2. These are the addresses of the primary and secondary WIPS console server. WIPS support requires a Brocade AirDefense WIPS Server on the network. WIPS functionality is not provided by the access point alone. The access point works in conjunction with the dedicated WIPS server(s).

NOTE
The System Name and Country are also configurable within the *System Setting*s screen. Refer to "Configuring system settings" on page 63 (if necessary) to set a system location and admin email address for the access point or to view other default settings.

4. Refer to the new *Radio Configuration* field to define how WLAN and WIPS are supported by the access point's radio(s). Remember, the options available depend on the single, dual or three radio model SKU deployed.

NOTE
If using a three radio model Mobility 7131N access point, the radio three configuration option could be rendered unavailable if Rogue AP detection is enabled, or if the power source cannot provide adequate power for the third radio.

The Quick Setup screen on the previous page displays the Radio Configuration field with all 8 radio button options available. This is only the case with three radio access point SKUs. A dual radio model access point would display 7 of the eight possible configuration options and a single radio model would display 4. Refer to the following table for the options available to single, dual and three radio models.

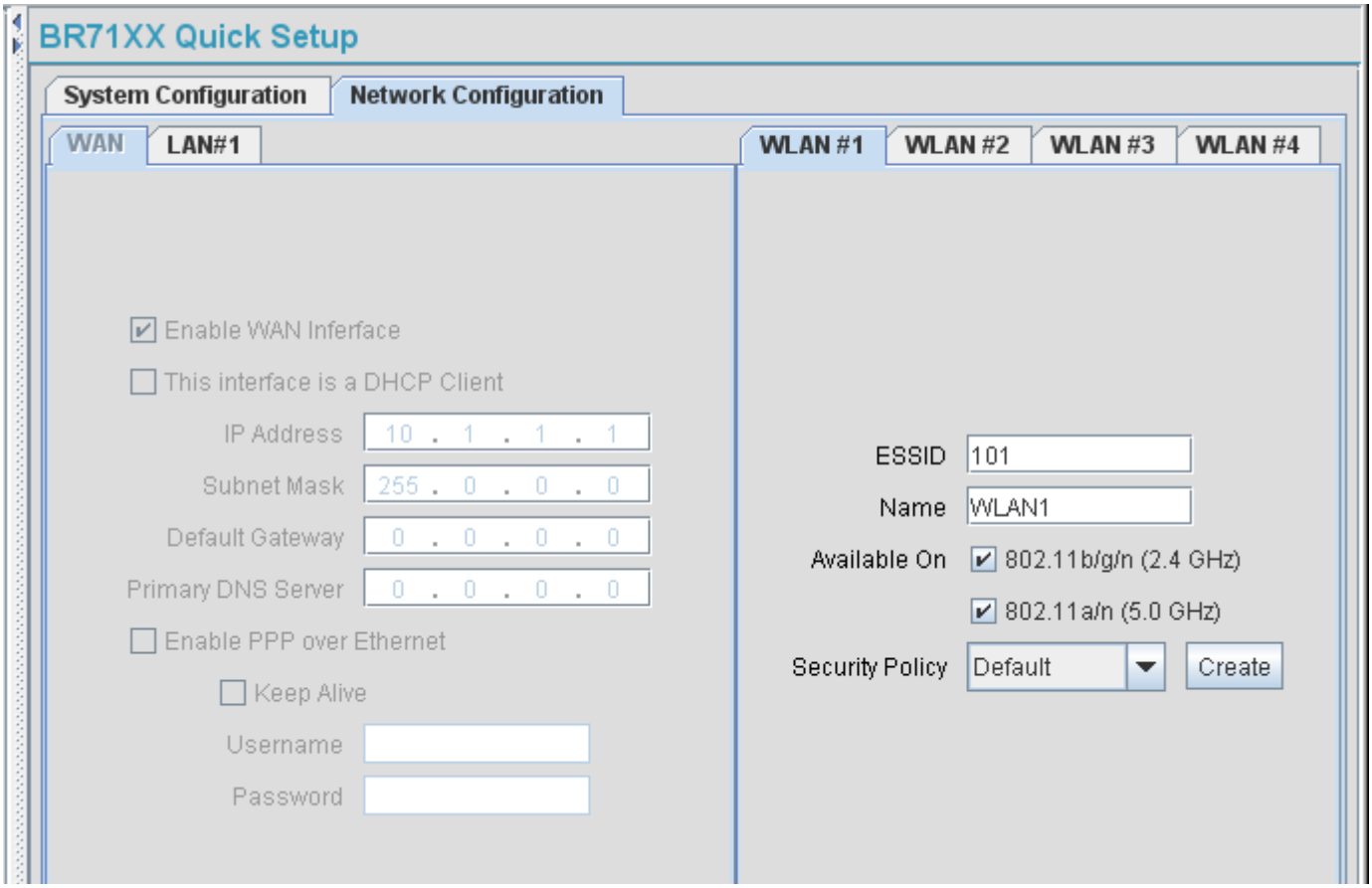
Radio Button	Single Radio SKU	Dual Radio SKU	Three Radio SKU
2.4 GHz WLAN, 5.0 GHz WLAN & Sensor	Not Available	Not Available	Radio 1 WLAN, Radio 2 WLAN, Radio 3 WIPS
2.4 GHz WLAN, & Sensor	Not Available	Radio1 WLAN, Radio 2 WIPS	Radio 1 WLAN, Radio 2 WIPS, Radio 3 WIPS
5.0 GHz WLAN & Sensor	Not Available	Radio 1 WIPS, Radio 2 WLAN	Radio 1 WIPS, Radio 2 WLAN, Radio 3 WIPS
2.4 GHz WLAN & 5.0 GHz WLAN only - no Sensor	Not Available	Radio 1 WLAN, Radio 2 WLAN	Radio 1 WLAN, Radio 2 WLAN, Radio 3 Disabled
Sensor only Spectrum Analysis mode (no WLAN)	Radio 1 WIPS	Radio 1 WIPS, Radio 2 WIPS	Radio 1 WIPS, Radio 2 WIPS, Radio 3 Disabled

2.4 GHz WLAN - no Sensor	Radio 1 WLAN (B/G/N)	Radio1 WLAN, Radio 2 Disabled	Radio 1 WLAN, Radio 2 Disabled, Radio 3 Disabled
5.0 GHz WLAN - no Sensor	Radio 1 WLAN (A/N)	Radio1 Disabled, Radio 2 WLAN	Radio 1 Disabled, Radio 2 WLAN, Radio 3 Disabled
Radios Off	Radio 1 Disabled	Radios 1 and 2 Disabled	Radios 1, 2 and 3 Disabled

NOTE
If an access point transitions from a one-wlan-radio configuration to a two-wlan-radio config, the radio's previous user set values (like maximum clients on radio) are not remembered and need to be defined again.

CAUTION
Only a qualified wireless network administrator should set the access point radio configuration. Refer to "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167 for an understanding of additional radio values and their implications.

5. Select the Quick Setup screen's *Network Configuration* tab to define a minimum set of WAN or LAN configuration values. The WAN tab displays by default.



Set a minimum set of parameters for using the WAN interface.

a. Select the *Enable WAN Interface* checkbox to enable a connection between the access point and a larger network or outside world through the WAN port. Disable this option to effectively isolate the access point's WAN connection. No connections to a larger network or the Internet will be possible. clients cannot communicate beyond the configured subnets.

b. Select the *This Interface is a DHCP Client* checkbox to enable DHCP for the access point's 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
Brocade recommends that the WAN and LAN ports should not be configured as DHCP clients at the same time.

c. Specify an *IP address* for the access point'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 access point's WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the access point 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 access point'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.

g. Optionally, use the *Enable PPP over Ethernet* checkbox to enable *Point-to-Point Protocol 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 access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data networks.

h. 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 access point automatically reestablishes the connection to the ISP.

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

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

For additional access point WAN port configuration options, see "Configuring WAN settings" on page 125.

6. Select the *LAN#1* tab to set a minimum set of parameters to use the LAN#1 interface.

a. Select the *Enable LAN Interface* checkbox to forward data traffic over the access point's 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 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 access point 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
.Brocade recommends that the WAN and LAN ports should not both be configured as DHCP clients.

c. Enter the network-assigned *IP Address* of the access point.

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

d. 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.

e. If using the static or DHCP Server option, enter a *Default Gateway* to define the numerical IP address of a router the access point uses on the Ethernet as its default gateway.

f. 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 access point LAN port configuration options, see "Configuring the LAN interface" on page 113.

7. 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 Wireless Configuration screen. The limitation of 16 WLANs exists regardless of whether the access point 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 access point, see "Creating/editing individual WLANs" on page 139.

b. Use the *Available On* checkboxes to define whether the target WLAN is operating in the 2.4 or 5 GHz radio band. Ensure the radio selected has been enabled (see step 8).

8. Once the WLAN's radio designations have been made, the radio must be configured in respect to intended 2.4 or 5 GHz radio traffic and the antennas used. Refer to *Network Configuration -> Wireless -> Radio Configuration -> Radio1* (or *Radio2*), and configure the Radio Settings field (at a minimum). If you know the radio's Properties, Performance and Beacon Settings, those fields can also be defined at this time.

   Define the Channel Settings, Power Level and 802.11 mode in respect to the 2.4 or 5 GHz 802.11b/g/n or 802.11a/n radio traffic and anticipated gain of the antennas.

CAUTION

Only a qualified wireless network administrator should set the access point radio configuration. Refer to "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167 for an understanding of additional radio values and their implications.

NOTE
Even an access point 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 security requirements change. Brocade recommends you familiarize yourself with the security options available on the access point before defining a security policy. Refer to "Configuring WLAN security settings" on page 59.

9. Click *Apply* to save any changes to the access point Quick Setup screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
10. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the access point Quick Setup screen to the last saved configuration.

Configuring WLAN security settings

To configure a basic security policy for a WLAN:

1. From the Brocade Mobility 7131 Series Access Point 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.

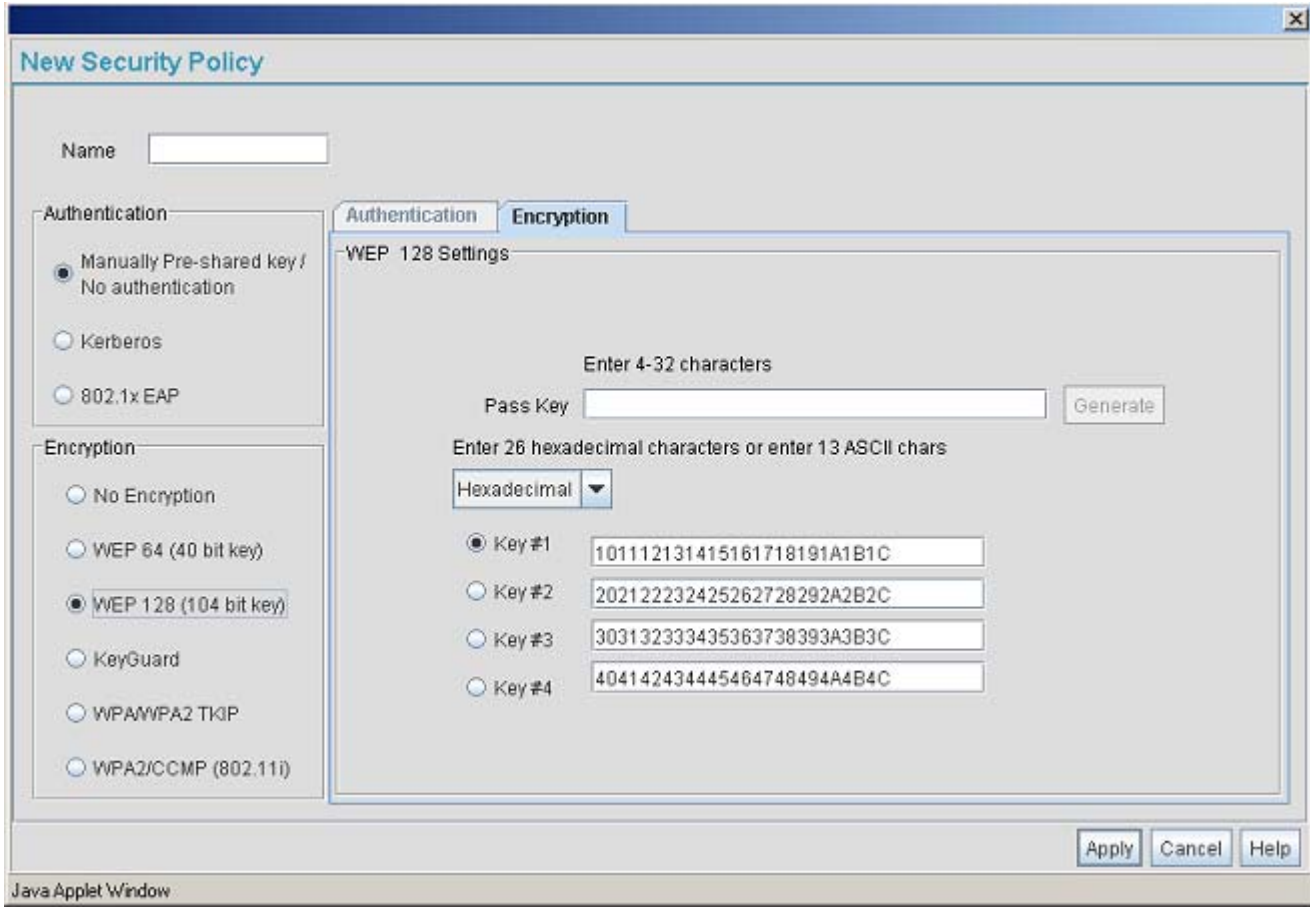
NOTE
For information on configuring the other encryption and authentication options available to the Brocade Mobility 7131 Series Access Point, see "Configuring security options" on page 192.

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. Brocade 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 access point, other proprietary routers and Clients use the same algorithm to convert a string to the same hexadecimal number. Non-Motorola clients and devices need to enter WEP keys manually as hexadecimal numbers. The access point and its target client(s) must use the same pass key to interoperate.
Keys #1-4	Use the *Key #1-4* fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for activation by clicking its radio button. The access point and its target client(s) must use the same key to interoperate.

5. Click the *Apply* button to save the security policy and return to the Brocade Mobility 7131 Series Access Point *Quick Setup* screen.

At this point, you can test the Brocade Mobility 7131 Series Access Point for Client interoperability.

Testing connectivity

Verify the access point's link with a Client by sending *Wireless Network Management Protocol* (WNMP) ping packets to the associated Client. Use the Echo Test screen to specify a target Client and configure the parameters of the test. The WNMP ping test only works with Motorola Clients. Only use a Motorola Client to test access point connectivity using WNMP.

NOTE
Before testing for connectivity, the target Client needs to be set to the same ESSID as the access point. Since WEP 128 has been configured for the access point, the Client also needs to be configured for WEP 128 and use the same WEP keys. Ensure the Client is associated with the access point before testing for connectivity.

To ping a specific Client to assess its connection with an access point:

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

Station Address	The station address is the IP address of the target Client. Refer to the Client Stats Summary screen for associated Client IP address information.
Number of Pings	Defines the number of packets to be transmitted to the Client. The default is 100.
Packet Length	Specifies the length of each packet transmitted to the Client during the test. The default length is 100 bytes.

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

   Refer to the Number of Responses value to assess the number of responses from the Client versus the number of ping packets transmitted by the access point. Use the ratio of packets sent versus the number of packets received the link quality between the Client and the access point.

   Click the *OK* button to exit the Echo Test screen and return to the Client Stats Summary screen.

Where to go from here?

Once basic connectivity has been verified, the Brocade Mobility 7131 Series Access Point can be fully configured to meet the needs of the network and the users it supports. Refer to the following:

- For detailed information on Brocade Mobility 7131 Series Access Point device access, SNMP settings, network time, importing/exporting device configurations and device firmware updates, see "System Configuration" on page 63.
- For detailed information on configuring Brocade Mobility 7131 Series Access Point LAN interface (subnet) and WAN interface see, "Network Management" on page 113.

- For detailed information on configuring specific encryption and authentication security schemes for individual Brocade Mobility 7131 Series Access Point WLANs, see “Configuring Access Point Security” on page 191.
- To view detailed statistics on the Brocade Mobility 7131 Series Access Point and its associated Clients, see “Monitoring Statistics” on page 259.

Chapter

System Configuration

4

In this chapter

- Configuring system settings 63
- Configuring power settings 67
- Adaptive AP setup 72
- Configuring data access 74
- Managing certificate authority (CA) certificates 78
- Configuring SNMP settings 86
- Configuring LLDP settings 98
- Configuring network time protocol (NTP) 99
- Logging configuration 102
- Importing/exporting configurations 103
- Updating device firmware 108

The access point 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 (version 0.8 or higher is recommended). The browser interface also allows for system monitoring of the access point.

Web management of the Brocade Mobility 7131 Series Access Point requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

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.

To connect to the access point, an IP address is required. If connected to the access point using the WAN port, the default static IP address is 10.1.1.1. The default password is "*admin123*." If connected to the access point using the LAN port, the default setting is DHCP client. The user is required to know the IP address to connect to the access point using a Web browser.

Configuring system settings

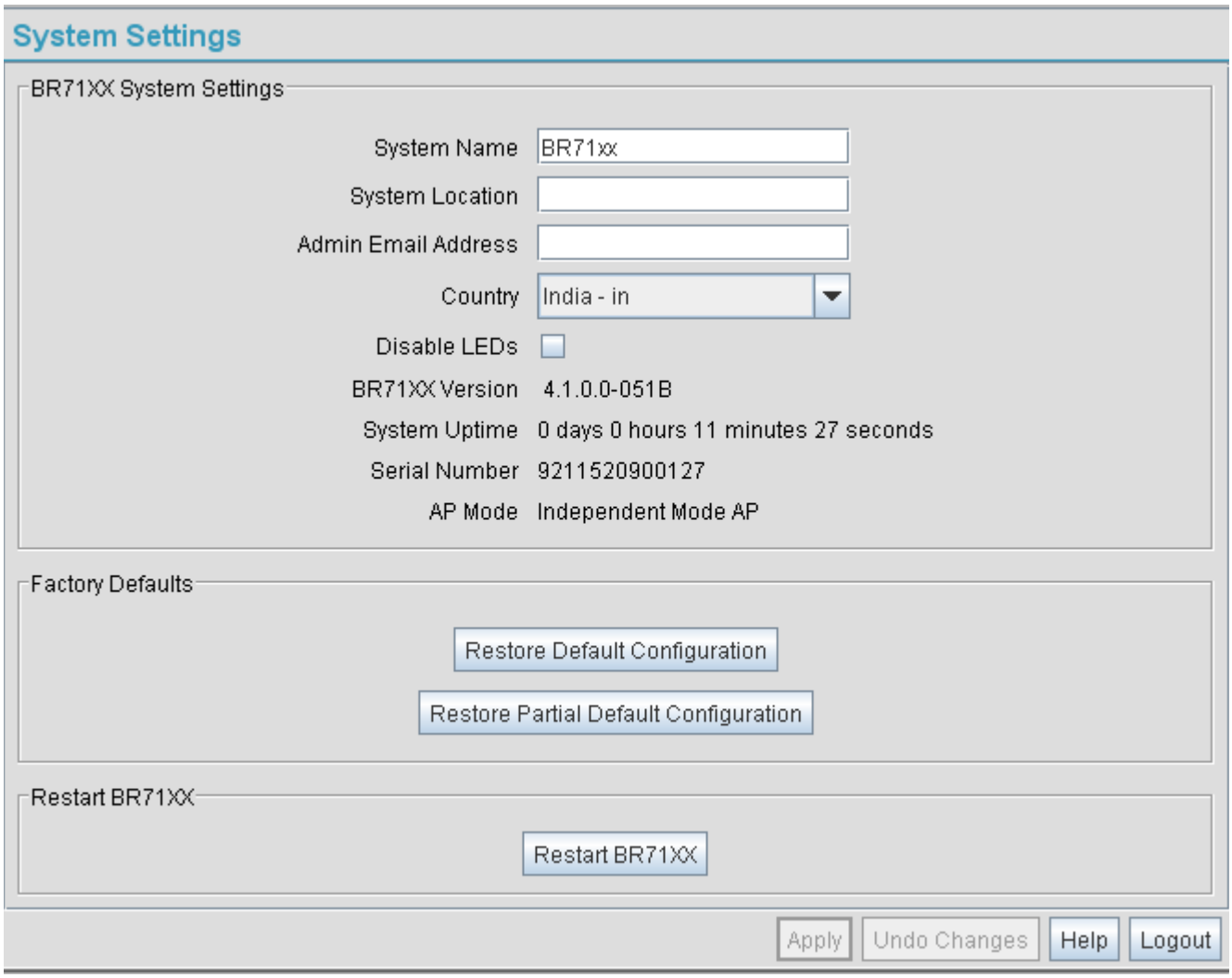
Use the *System Settings* screen to specify the name and location of the Brocade Mobility 7131 Series Access Point, assign an email address for the network administrator, restore the access point's default configuration or restart the access point.

To configure System Settings for the Brocade Mobility 7131 Series Access Point:

CAUTION

The access point's country of operation is set from within the System Settings screen. If the country code is changed, the access point's power level, primary channel and secondary channel return to their default values. If changing the country code, be aware these values will require modification to their previous settings.

1. Select *System Configuration -> System Settings* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the Brocade Mobility 7131 Series Access Point *System Settings* field to assign a system name and location, set the country of operation and view device version information.

System Name	Specify a device name for the Brocade Mobility 7131 Series Access Point. Brocade recommends selecting a name serving as a reminder of the user base the Brocade Mobility 7131 Series Access Point supports (engineering, retail, etc.). This name will appear in the WIPS server when one of the radios is configured as a sensor and the WIPS functionality connects to the WIPS server. The WIPS module only accepts names with up to 20 characters, keep that if intending to use this AP as a sensor.
System Location	Enter the location of the Brocade Mobility 7131 Series Access Point. The *System Location* 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, “second floor engineering”
Admin Email Address	Specify the access point administrator's email address.
Country	The Brocade Mobility 7131 Series Access Point 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 access point. 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 *Country* field correctly.
Disable LEDs	Select the *Disable LEDs* radio button to stop the access points LEDs from blinking during startup and normal operation. Selecting this option turns off all of the access point’s light pipes and none of the access point’s states are displayed by the LEDs. This option is disabled by default.
BR71XX Version	The dIsplayed number is the current version of the device firmware. Use this information to determine if the access point is running the most recent firmware available from Brocade. Use the *Firmware Update* screen to keep the AP’s firmware up to date.
System Uptime	Displays the current uptime of the Brocade Mobility 7131 Series Access Point defined in the System Name field. *System Uptime* is the cumulative time since the Brocade Mobility 7131 Series Access Point was last rebooted or lost power.
Serial Number	Displays the Brocade Mobility 7131 Series Access Point *Media Access Control (MAC)* address. The Brocade Mobility 7131 Series Access Point 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.
AP Mode	Displays the access point’s mode of operation to convey whether the access point is functioning as a standalone access point (Independent mode) or in Adaptive (thin AP) mode. If in Adaptive mode, the access point attempts to discover a controller through one or more of several mechanisms: DNS, DHCP, ICMP, CAPWAP or a statically programmed IP address.

3. Refer to the *Factory Defaults* field to restore either a full or partial default configuration.

CAUTION

Restoring the access point's configuration back to default settings changes the administrative password back to "admin123." If restoring the configuration back to default settings, be sure you change the administrative password accordingly.

Restore Default Configuration	Select the *Restore Default Configuration* button to reset the AP's configuration to factory default settings. If selected, a message displays warning the user the current configuration will be lost if the default configuration is restored.
Restore Partial Default Configuration	Select the *Restore Partial Default Configuration* button to restore a default configuration with the exception of the current LAN, WAN, SNMP settings and IP address used to launch the browser. If selected, a message displays warning the user all current configuration settings will be lost with the exception of WAN and SNMP settings.

4. Use the *Restart* Brocade Mobility 7131 Series Access Point field to restart the AP (if necessary).

Restart Brocade Mobility 7131 Series Access Point	Click the *Restart* Brocade Mobility 7131 Series Access Point button to reboot the AP. Restarting the Brocade Mobility 7131 Series Access Point resets all data collection values to zero. Brocade does not recommend restarting the AP during significant system uptime or data collection activities.

CAUTION

After a reboot, static route entries disappear from the AP Route Table if a LAN Interface is set to DHCP Client. The entries can be retrieved (once the reboot is done) by performing an Apply operation from the WEB UI or a save operation from the CLI.

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 Brocade Mobility 7131 Series Access Point default configuration or restarting the Brocade Mobility 7131 Series Access Point.

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 Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring power settings

Use the *Power Setting* screen to select one of two power modes, *3af* or *Auto.* When automatic is selected, the access point safely operates within available power. Once the power configuration is determined, the access point configures its operating power characteristics based on its SKU and power configuration.

The access point uses a *complex programmable logic device* (CPLD). The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the access point's maximum power budget. When the AP is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the access point. The CPLD also determines the access point hardware SKU and the number of radios. If the access point's POE resource cannot provide sufficient power to run the access point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- The access point's transmit and receive algorithms could be negatively impacted
- The access point's transmit power could be reduced due to insufficient power
- The access point's WAN port configuration could be changed (either enabled or disabled)

Automatic is the default mode. When Auto is selected, the CPLD determines how much power is available at startup, either 3af, Mid Power or Full Power for a Brocade Mobility 7131 Access Point or 3af, 3at or Full Power for a Brocade Mobility 7131N Access Point. Based on the power level, the access point configures its power consumption based on the table below:

NOTE
Single radio models always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models.

Mobility 7131 Available Power	Mobility 7131 Operational Configuration (for Dual Radio)
13 watts (3af) *Power Status: 3af*	Two radios, processor running at 500 MHz, GE1 port (1000BASE-T) and GE2 port disabled.
18 watts *Power Status: Mid Power*	Two radios, processor running at 500 MHz, GE1 port (1000BASE-T) and GE2 port (100 BASE-T).
24 watts or external power supply *Power Status: Full Power*	Two radios, processor running at 500 MHz, GE1 port (1000BASE-T) and GE2 port (1000 BASE-T).

NOTE
A Brocade Mobility 7131N Access Point has different available power from a Brocade Mobility 7131 Access Point. A Brocade Mobility 7131N Access Point uses 22 watts when its power status is 3af, 23 - 26 watts when its power status is 3at and 27 watts when its power status is Full Power.

CAUTION
The power modes described in the section are only obtainable using the 48-Volt Power Supply (Part No. 50-14000-247R) designed specifically for a Brocade Mobility 7131 Access Point and Mobility 7131N.

NOTE
Radio transmit power is not used as one of the factors to determine the available power budget. If an external power supply is used, it is assumed it will provide full power. When operating using full power, each radio has 3x3 antenna mode support and its intended transmit power budget.

Radios at full power

The table below describes the maximum transmit power available to each radio (at varying data rates) when the access point is receiving full DC power and is not compromised in its power budget. These values should be viewed as the safe limit for the access point's radio at full power and should not be exceeded.

Rates (Mbps)	MCS Indices	EVM	Bandwidth	Maximum Transmit Power 2.4 GHz	Maximum Transmit Power 5 GHz
1		-9	20MHz	23	NA
2		-9	20MHz	23	NA
5.5		-9	20MHz	23	NA
11		-9	20MHz	23	NA
6		-5	20MHz	23	20
9		-8	20MHz	23	20
12		-10	20MHz	23	20
18		-13	20MHz	23	20
24		-16	20MHz	22	20
36		-19	20MHz	22	19
48		-22	20MHz	21	18
54		-25	20MHz	20	17
	MCS0/MCS8	-5	HT20/40	23	20
	MCS1/MCS9	-10	HT20/40	23	20
	MCS2/MCS10	-13	HT20/40	23	20
	MCS3/MCS11	-16	HT20/40	23	19
	MCS4/MCS12	-19	HT20/40	22	19
	MCS5/MCS13	-22	HT20/40	22	18
	MCS6/MCS14	-25	HT20/40	21	17
	MCS7/MCS15	-28	HT20/40	20	17

Radios at low power

The table below describes the maximum transmit power available to each radio (at varying data rates) when the access point is receiving low DC power in either af or at mode.

CAUTION

Exceeding the limits listed below can cause damage to the access point or cause the radio to operate unpredictably. Thus, these values should be viewed as the safe limit for the access point's radio and should not be exceeded in either af or at mode.

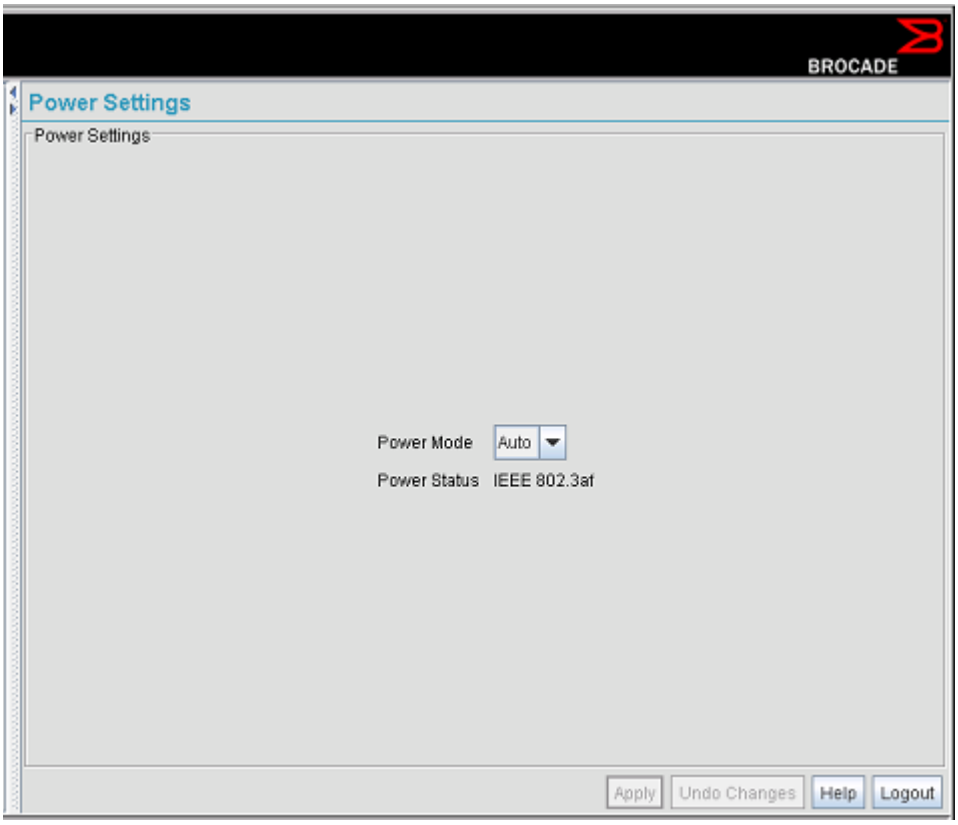
Rates (Mbps)	MCS Indices	EVM	Bandwidth	Maximum Transmit Power 2.4 GHz	Maximum Transmit Power 5 GH
1		-9	20MHz	20	NA
2		-9	20MHz	20	NA
5.5		-9	20MHz	20	NA
11		-9	20MHz	20	NA

Rates (Mbps)	MCS Indices	EVM	Bandwidth	Maximum Transmit Power 2.4 GHz	Maximum Transmit Power 5 GH
6		-5	20MHz	22	19
9		-8	20MHz	22	19
12		-10	20MHz	22	19
18		-13	20MHz	22	18
24		-16	20MHz	21	18
36		-19	20MHz	20	17
48		-22	20MHz	18	15
54		-25	20MHz	17	13
	MCS0/MCS8	-5	HT20/40	22	19
	MCS1/MCS9	-10	HT20/40	22	19
	MCS2/MCS10	-13	HT20/40	21	18
	MCS3/MCS11	-16	HT20/40	21	17
	MCS4/MCS12	-19	HT20/40	20	17
	MCS5/MCS13	-22	HT20/40	19	16
	MCS6/MCS14	-25	HT20/40	18	15
	MCS7/MCS15	-28	HT20/40	17	15

NOTE
The access point could allow the operation of only one radio depending on the POE power level provided. When only one radio is operational, it is configured as either a WIPS or WLAN radio. Consequently, if the access point transitions from dual to single radio operation, a WIPS radio might not be available.

To define the Brocade Mobility 7131 Series Access Point's power setting:

1. Select *System Configuration -> Power Settings* from the menu tree.



2. Refer to the following to assess the access point's current power state. Once known, determine how available power resources are applied to the access point's radios.

NOTE

Within the *Power Configuration* field, an installation professional selects a power mode based on the different power resources available to that access point's SKU. For 3af and 3at, choose between *Default* and *Option* as best suited to that hardware SKU. For example, if Option is selected for 3af Power, and the access point is a dual radio model, the following configuration is set:

LAN port ON (1000 BAST-T)
WAN port OFF
Radio 1 (2.4) on, 2x3 mode with maximum transmit power 18dBm
Radio 2 (5.0) on, 2x3 mode with maximum transmit power 18dBm

Contact Brocade Support if unsure of your access point's optimal power management settings, go to http://www.brocade.com/support/.

Power Status	Refer to the (read only) power status field to review the power available to the AP. The status for a Brocade Mobility 7131 Access Point and Brocade Mobility 7131N Access Point are slightly different. For a Brocade Mobility 7131 Access Point , the options are 3af, Mid Power or Full Power. For a Brocade Mobility 7131N Access Point, the options are 3at, 3af or Full Power.
Power Mode	When the access point is powered on for the first time, the system determines the power budget available to the access point. Using the *Auto* setting (default setting), the access point automatically determines the best power configuration based on the available power budget. If *3af* is selected, the AP assumes 12.95 watts are available. If the mode is changed, the access point requires a reset to implement the change.
3af Power	If 3af is selected, the AP is configured assuming 12.95 watts are available using a 3af power budget, even though there may actually be more power available. Set the 3af Power to either Default or Option. Changing the power option to 3af restarts the access point in order to implement the change. The access point's WAN port is turned off if the power mode is set to 3af.
3at Power	Set the power option for 3at to either Default or Option. Changing the power option to 3at restarts the access point in order to implement the change. With 3at power, both Ethernet ports are available using 1000BAST-T mode.
Default Radio	Define whether radio 1 or radio 2 is the default radio.With three radio models, this is especially important when the power budget can only accommodate one radio to be optimally powered. If using a dual radio access point, power is negotiated between the radios per the defined configuration. If deploying a three radio model Mobility 7131N, the third radio can never be the default radio.

3. Click *Apply* to save any changes to the Power Settings 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 Power Settings screen to the last saved configuration.
5. Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

Adaptive AP setup

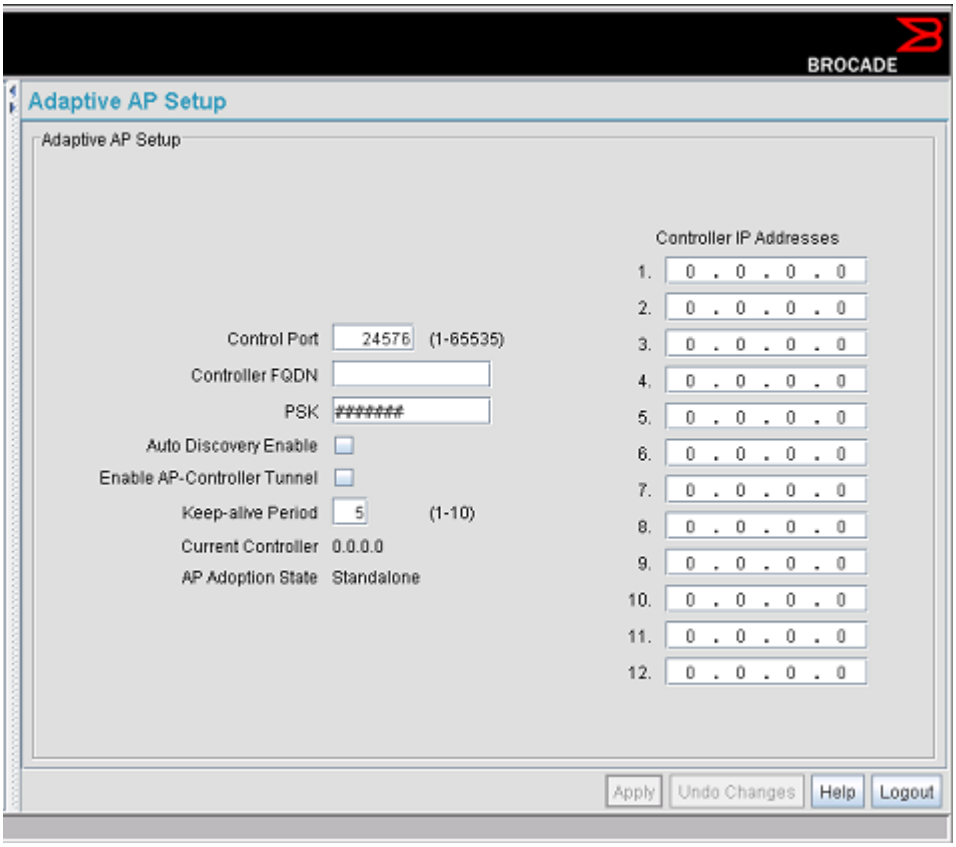
An access point needs settings defined to discover (and adopt) an available controller and establish a connection and data tunnel. It's through this controller adoption that the access point receives its *adaptive AP* (AAP) configuration. A Brocade Mobility 7131 Series Access Point has a screen to define the mechanisms used to adopt a controller and route AAP configuration information.

NOTE
For an AAP overview and a theoretical discussion of how an access point discovers a controller to creates a secure data tunnel for adaptive AP operation, see "Adaptive AP" on page 613.

NOTE
The Adaptive AP Setup screen does not display the AAP's adoption status or adopted controller. This information is available using the access point's CLI.

To configure the access point's controller discovery method and connection medium:

1. Select *System Configuration -> Adaptive AP Setup* from the menu tree.



2. Define the following to prioritize a controller connection scheme and AP interface used to adopt to the controller.

Control Port	Define the port used by the controller FQDN to transmit and receive with the AAP. The default control port is 24576.
Controller FQDN	Add a complete controller *fully qualified domain name* (FQDN) to add a controller to the 12 available controller IP addresses available for connection. The access point resolves the name to one or more IP addresses if a DNS IP address is present. This method is used when the access point fails to obtain an IP address using DHCP.
PSK	Before the access point sends a packet requesting its mode and configuration, the controller and the access point require a secure link using a pre-shared key.

Auto Discovery Enable	When the *Auto Discovery Enable* checkbox is selected, the access point begins the controller discovery (adoption) process using DHCP first, then a user provided domain name, lastly using static IP addresses. This setting is disabled by default. When disabled, the AP functions as a standalone access point without trying to adopt a controller. Consequently, the access point will not be able to obtain an AAP configuration.
Enable AP-controller Tunnel	This setting is required to enable an IPSec VPN from the AAP to the Wireless Controller.
Keep-Alive Period	The Keepalive interval defines a period (in seconds) the AAP uses to terminate its connection to the controller if no data is received.
Current Controller	Displays the IP address of the connected controller. This is the controller from which the Brocade Mobility 7131 Series Access Point receives its adaptive configuration.
AP Adoption State	Displays whether the Brocade Mobility 7131 Series Access Point has been adopted by the controller (whose IP address is listed in the Current Controller parameter). The Brocade Mobility 7131 Series Access Point cannot receive its adaptive configuration without association.

3. Refer to the 12 available *Controller IP Addresses* to review the addresses the access point uses to adopt with a controller.

   The access point contacts each controller on the list (from top to bottom) until a viable controller adoption is made. The access point first populates the list with the IP addresses received from its DHCP resource. If DHCP is not able to obtain IP addresses, the access point attempts to resolve the controller's Domain Name if provided within the Controller FQDN parameter. However, if the access point receives one or more IP addresses from the DHCP server, it will not solicit an IP address from a user provided domain name. Lastly, provide static (manually provided) IP addresses to the list as long as there is room. The access point will defer to these addresses if DHCP and a provided domain address fail to secure a controller adoption.

4. Click *Apply* to save any changes to the Adaptive AP Setup 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 Adaptive AP Setup screen to the last saved configuration.
6. Click *Logout* to securely exit the Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring data access

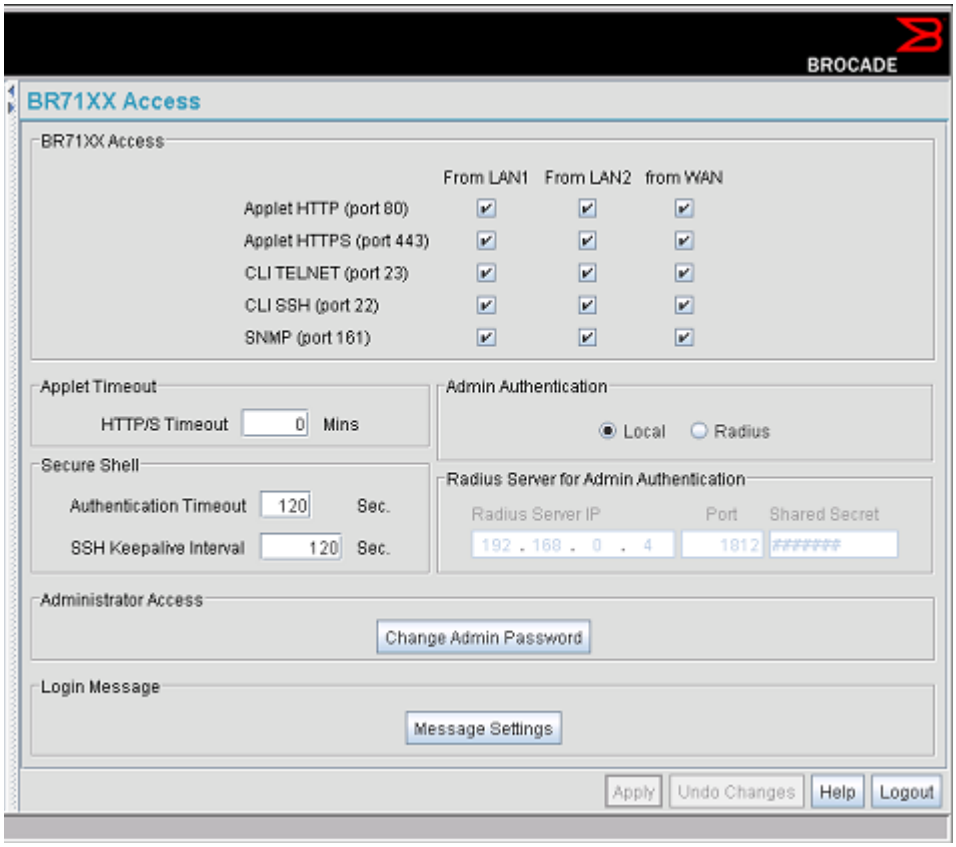
Use the Brocade Mobility 7131 Series Access Point *Access* screen to allow/deny management access to the access point from different subnets (LAN1, LAN2 or WAN) using different protocols such as HTTPS, Telnet, SSH or SNMP. The access options are either enabled or disabled. It is not meant to function as an ACL in routers or other firewalls, where you can specify and customize specific IPs to access specific interfaces.

Use the Access screen checkboxes to enable or disable LAN1, LAN2 and/or WAN access using the protocols and ports listed. If access is disabled, this effectively locks out the administrator from configuring the Brocade Mobility 7131 Series Access Point using that interface. To avoid jeopardizing the network data managed by the Brocade Mobility 7131 Series Access Point, Brocade recommends enabling only those interfaces used in the routine (daily) management of the network, and disabling all other interfaces until they are required.

The Access screen also has a new facility allowing customers to create a login message with customer generated text. When enabled (using either the access point Web UI or CLI), the login message displays when the user is logging into the access point. If the login message is disabled, the default login screen displays with no message.

To configure access for the Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration -> BR71XX Access* from the menu tree.



2. Use the Brocade Mobility 7131 Series Access Point *Access* field checkboxes to enable/disable the following on the access point's LAN1, LAN2 or WAN interfaces:

Applet HTTP (port 80)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the Brocade Mobility 7131 Series Access Point configuration applet using a Web browser.
Applet HTTPS (port 443)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the Brocade Mobility 7131 Series Access Point configuration applet using a *Secure Sockets Layer (SSL)* for encrypted HTTP sessions.

CLI TELNET (port 23)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the Brocade Mobility 7131 Series Access Point CLI via the TELNET terminal emulation TCP/IP protocol.
CLI SSH (port 22)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the Brocade Mobility 7131 Series Access Point CLI using the SSH (Secure Shell) protocol.
SNMP (port 161)	Select the LAN1, LAN2 and/or WAN checkboxes to enable access to the Brocade Mobility 7131 Series Access Point 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 access point 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 (between 30 - 120 seconds) allowed for SSH authentication to occur before executing a timeout. The minimum permissible value is 30 seconds.
SSH keepalive Interval	The SSH Keepalive Interval defines a period (in seconds) 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 Brocade Mobility 7131 Series Access Point verifies the authentication connection.
Radius	Designates that a Radius server is used in the authentication credential verification. If using this option, the connected PC is required to have its Radius credentials verified with an external Radius server. Additionally, the Radius Server's Active Directory should have a valid user configured and have a PAP based Remote Access Policy configured for Radius Admin Authentication to work.

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.

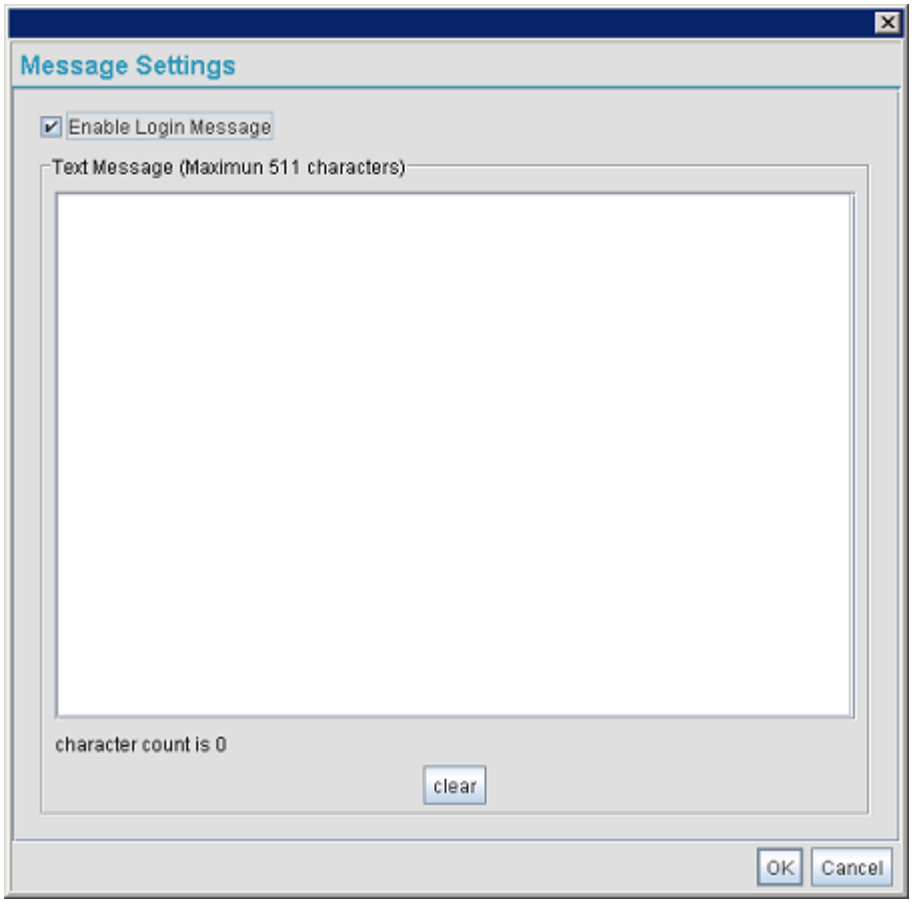
Port	Specify the port on which the server is listening. The Radius server typically listens on ports 1812 (default port).
Shared Secret	Define a shared secret for authentication on the server. The shared secret is required to be the same as the shared secret defined on the Radius server. Use shared secrets 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 and numbers. The default is brocade.

7. Update the *Administrator Access* field to change the administrative password used to access the 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. Refer to the *Login Message* field to optionally define a message displayed to the customer as they login into the access point.

Message Settings	Click the *Message Setting*s button to display a screen used to create a text message. Once displayed, select the *Enable Login Message* checkbox to allow your customized message to be displayed when the user is logging into the access point. If the checkbox is not selected (as is the case by default), the user will encounter the login screen with no additional message. When the login message function is enabled, the user can enter a (511 character maximum) message describing any usage caveat required (such as the authorization disclaimer displayed on the following page). Thus, the login message can serve an important function by discouraging unauthorized users from illegally managing the access point. As your message is entered, the character usage counter is updated to allow you to visualize how close you are coming to the maximum allowed number of characters. Click the *Clear* button at any time to remove the contents of the message and begin a new one. Once you have finished creating your message, click the *OK* button to return to the Access screen.



9. Click *Apply* to save any changes to the Brocade Mobility 7131 Series Access Point Access screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.
10. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Brocade Mobility 7131 Series Access Point Access screen to the last saved configuration.
11. Click *Logout* to securely exit the Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Managing certificate authority (CA) certificates

Certificate management includes the following sections:

- *Importing a CA certificate*
- *Creating self certificates for accessing the VPN*

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 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 Brocade Mobility 7131 Series Access Point 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 220.

CAUTION

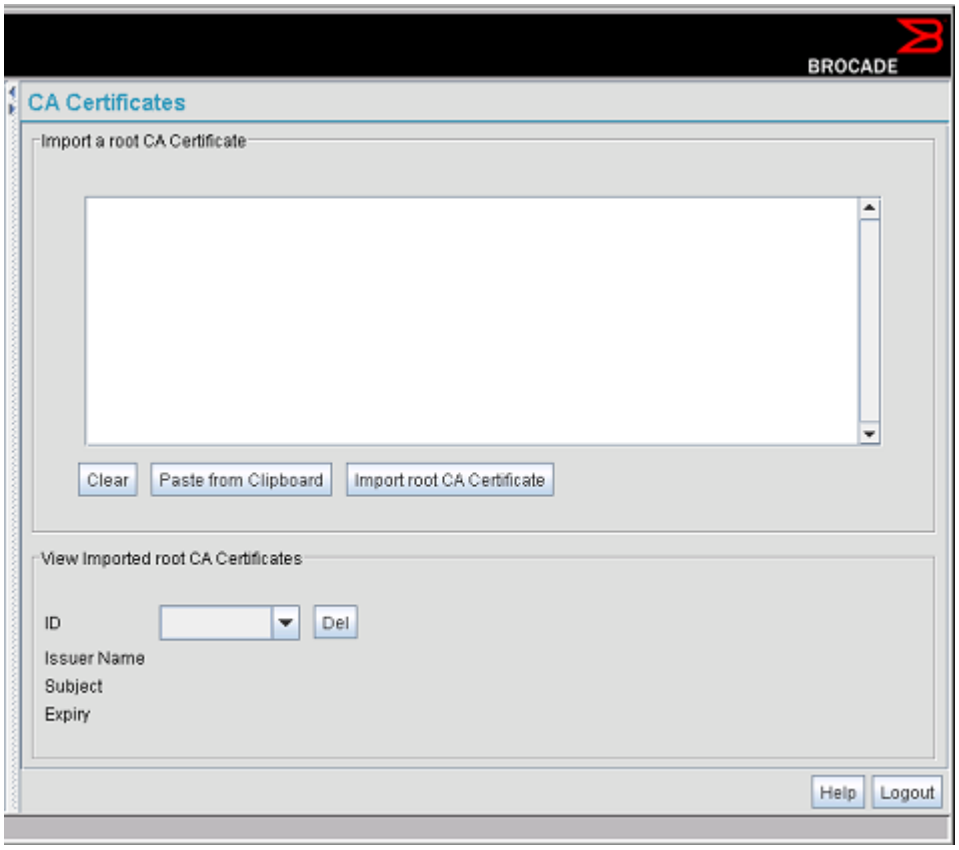
Loaded and signed CA certificates will be lost when changing the access point’s firmware version using either the GUI or CLI. After a certificate has been successfully loaded, export it to a secure location to ensure its availability after a firmware update.
If restoring the access point’s factory default firmware, you must export the certificate file BEFORE restoring the access point’s factory default configuration. Import the file back after the updated firmware is installed.

Refer to your network administrator to obtain a CA certificate to import into the Brocade Mobility 7131 Series Access Point.

NOTE
Verify the Brocade Mobility 7131 Series Access Point 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 99.

To import a CA certificate:

1. Select *System Configuration -> Certificate Mgmt -> CA Certificates* from the menu tree.



2. Copy the content of the CA Certificate message (using a text editor such as notepad) and 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.

Creating self certificates for accessing the VPN

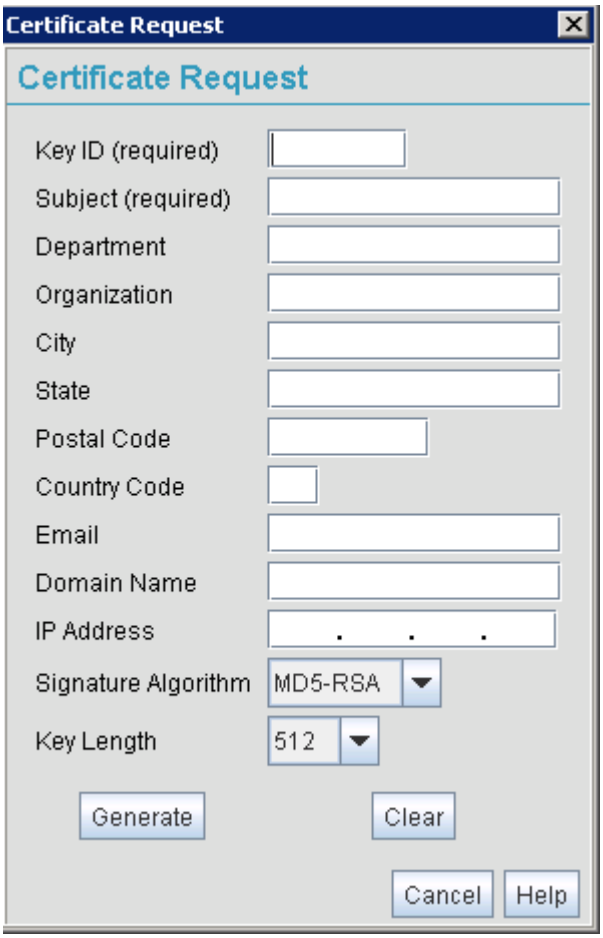
The Brocade Mobility 7131 Series Access Point requires two kinds of certificates for accessing the VPN, CA certificates and self certificates. Self certificates are certificate requests you create, send to a *Certificate Authority* (CA) to be signed, then import the signed certificate into the management system.

CAUTION

Self certificates can only be generated using the access point GUI and CLI interfaces. No functionality exists for creating a self-certificate using the access point's SNMP configuration option.

To create a self certificate:

1. Select *System Configuration -> Certificate Mgmt -> Self Certificates* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Click on the *Add* button to create the certificate request.



The *Certificate Request* screen displays.

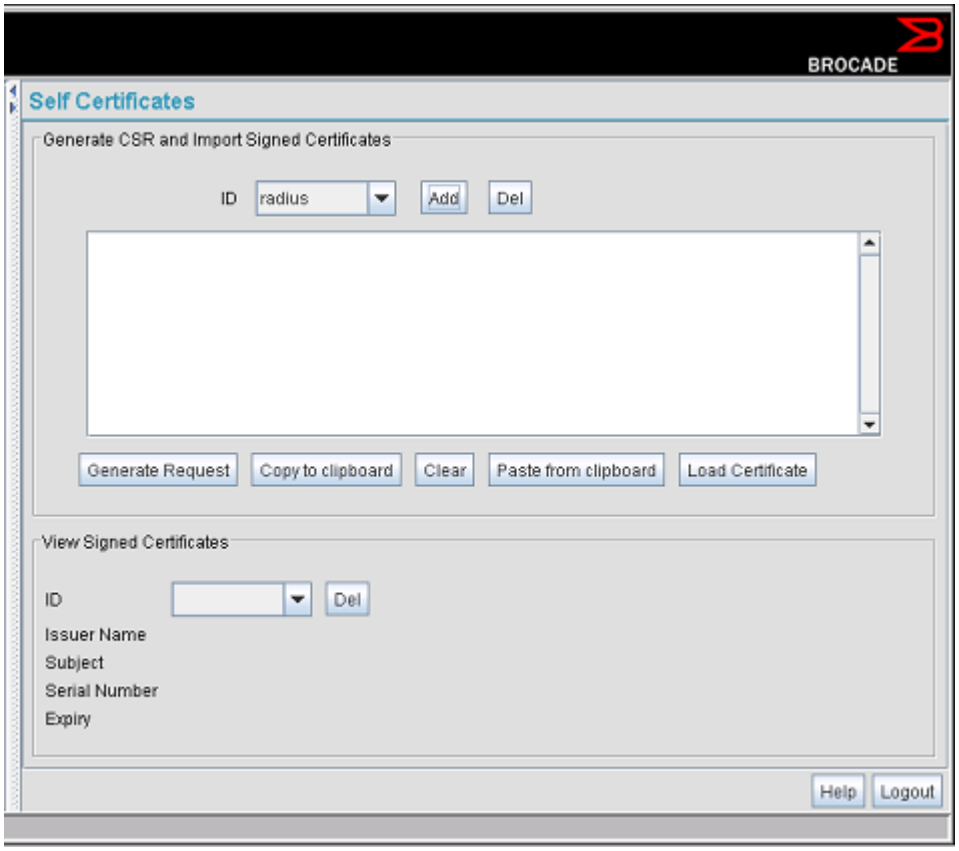
3. Complete the request form with the pertinent information. Only 4 values are required, the others optional.

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.
Key Length	Defines the length of the key. Possible values are 512, 1024, and 2048.

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 within the Self Certificates screen.

5. Click the *Generate 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.

   Click the *Load 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.

NOTE
If the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point during this process.

8. 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 220.

Creating a certificate for Onboard Radius Authentication

The Brocade Mobility 7131 Series Access Point can use its on-board Radius Server to generate certificates to authenticate Clients for use with the access point. In addition, a Windows 2000 or 2003 Server is used to sign the certificate before downloading it back to the access point's on-board Radius server and loading the certificate for use with the access point.

Both a CA and Self certificate are required for Onboard Radius Authentication. For information on CA Certificates, see "Importing a CA certificate" on page 79. Ensure the certificate is in a Base 64 Encoded format or risk loading an invalid certificate.

CAUTION
If using the Radius time-based authentication feature to authenticate access point user permissions, ensure the access point's time is synchronized with the CA server used to generate certificate requests.

CAUTION
Self certificates can only be generated using the access point GUI and CLI interfaces. No functionality exists for creating a self-certificate using the access point's SNMP configuration option.

To create a self certificate for on-board Radius authentication:

1. Select *System Configuration -> Certificate Mgmt -> Self Certificates* from the Brocade Mobility 7131 Series Access Point 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.

Key ID (required)	Enter a logical name for the certificate to help distinguish between certificates. The name can be up to 7 characters in length.
Subject (required)	The required *Subject* value contains important information about the certificate. Contact the CA signing the certificate to determine the content of the Subject parameter.
Department	Optionally enter a value for your organizations's department name if needing to differentiate the certificate from similar certificates used in other departments within your organization.
Organization	Optionally enter the name of your organization for supporting information for the certificate request.
City	Optionally enter the name of the City where the access point (using the certificate) resides.
State	Optionally enter the name of the State where the access point (using the certificate) resides.
Postal Code	Optionally enter the name of the Postal (Zip) Code where the access point (using the certificate) resides.
Country Code	Optionally enter the access point's Country Code.
Email	Enter a organizational email address (avoid using a personal address if possible) to associate the request with the proper requesting organization.
Domain Name	Ensure the Domain name is the name of the CA Server. This value must be set correctly to ensure the certificate is properly generated.
IP Address	Enter the IP address of this access point (as you are using the access point's onbard Radius server).
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.
Key Length	Defines the length of the key. Possible values are 512, 1024, and 2048. Brocade recommends setting this value to 1024 to ensure optimum functionality.

4. Complete as many of the optional values within the *Certificate Request* screen as possible.
5. When the form is completed, click the *Generate* button from within the Certificate Request screen.

   The Certificate Request screen disappears and the ID of the generated certificate request displays in the drop-down list of certificates within the Self Certificates screen.

NOTE
A Warning screen may display at this phase stating key information could be lost if you proceed with the certificate request. Click the *OK* button to continue, as the certificate has not been signed yet.

6. Click the *Generate Request* button from within the Self Certificates screen. The certificate content displays within the Self Certificate screen.
7. Click the *Copy to clipboard* button. Save the certificate content to a secure location.
8. Connect to the Windows 2000 or 2003 server used to sign the certificate.
9. Select the *Request a certificate* option. Click *Next* to continue.
10. Select the *Advanced request* checkbox from within the Choose Request Type screen and click Next to continue.
11. From within the Advanced Certificate Requests screen, select the *Submit a certificate request using a base 64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS file* option. Click *Next* to continue.
12. Paste the content of certificate in the *Saved Request* field (within the Submit a Saved Request screen).

NOTE
An administrator must make sure the *Web Server* option is available as a selectable option for those without administrative privileges.

If you do not have administrative privileges, ensure the *Web Server* option has been selected from the Certificate Template drop-down menu. Click Submit.

13. Select the *Base 64 encoded* checkbox option from within the Certificate Issued screen and select the *Download CA Certificate* link.

    A *File Download* screen displays prompting the user to select the download location for the certificate.
14. Click the *Save* button and save the certificate to a secure location.
15. Load the certificates on the access point.

CAUTION
Ensure the CA Certificate is loaded before the Self Certificate, or risk an invalid certificate load.

16. Open the certificate file and copy its contents into the CA Certificates screen by clicking the *Paste from Clipboard* button.

    The certificate is now ready to be loaded into the access point's flash memory.
17. Click the *Import root CA Certificate* button from within the CA Certificates screen.
18. Verify the contents of the certificate file display correctly within the CA Certificates screen.
19. Open the certificate file and copy its contents into the Self Certificates screen by clicking the *Paste from Clipboard* button.
20. Click the *Load Certificate* button.
21. Verify the contents of the certificate file display correctly within the Self Certificates screen.

    The certificate for the onboard Radius authentication of Clients has now been generated and loaded into the access point's flash memory.

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 access point's download site contains the following MIB files supporting the Brocade Mobility 7131 Series Access Point:

- BROCADE-CC-BR7131-MIB-2.0.mib (standard MIB file)
- BROCADE-BR7131-MIB.mib

The BROCADE-BR7131-MIB.mib contains the majority of the information contained within the BROCADE-CC-BR7131-MIB-2.0.mib file. This feature rich information has proven reliable for use with a Brocade Mobility 7131 Series Access Point model access point. The remaining portion of the BROCADE-BR7131-MIB.mib contains supplemental information unique to the access point feature set.

Use the table below to locate the MIB where the given feature can be configured.

Feature	MIB	Feature	MIB
LAN Configuration	BROCADE-BR7131-MIB.mib	Subnet Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
VLAN Configuration	BROCADE-BR7131-MIB.mib	DHCP Server Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
802.1x Port Authentication	BROCADE-BR7131-MIB.mib	Advanced DHCP Server configuration	BROCADE-CC-BR7131-MIB-2.0.mib
Ethernet Type Filter Configuration	BROCADE-BR7131-MIB.mib	WAN IP Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
Wireless Configuration	BROCADE-BR7131-MIB.mib	PPP Over Ethernet	BROCADE-CC-BR7131-MIB-2.0.mib
Security Configuration	BROCADE-BR7131-MIB.mib	NAT Address Mapping	BROCADE-CC-BR7131-MIB-2.0.mib
Client ACL Configuration	BROCADE-BR7131-MIB.mib	VPN Tunnel Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
QOS Configuration	BROCADE-BR7131-MIB.mib	VPN Tunnel status	BROCADE-CC-BR7131-MIB-2.0.mib
Radio Configuration	BROCADE-BR7131-MIB.mib	Content Filtering	BROCADE-CC-BR7131-MIB-2.0.mib
Bandwidth Management	BROCADE-BR7131-MIB.mib	Rogue AP Detection	BROCADE-CC-BR7131-MIB-2.0.mib
SNMP Trap Selection	BROCADE-BR7131-MIB.mib	Firewall Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
SNMP RF Trap Thresholds	BROCADE-BR7131-MIB.mib	LAN to WAN Access	BROCADE-CC-BR7131-MIB-2.0.mib
Config Import/Export	BROCADE-BR7131-MIB.mib	Advanced LAN Access	BROCADE-CC-BR7131-MIB-2.0.mib
Client Authentication Stats	BROCADE-BR7131-MIB.mib	Router Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
WNMP Ping Configuration	BROCADE-BR7131-MIB.mib	System Settings	BROCADE-CC-BR7131-MIB-2.0.mib
Known AP Stats	BROCADE-BR7131-MIB.mib	Mobility 7131 Access	BROCADE-CC-BR7131-MIB-2.0.mib

Flash LEDs	BROCADE-BR7131-MIB.mib	Certificate Mgt	BROCADE-CC-BR7131-MIB-2.0.mib
Automatic Update	BROCADE-BR7131-MIB.mib	SNMP Access Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
		SNMP Trap Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
		NTP Server Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
		Logging Configuration	BROCADE-CC-BR7131-MIB-2.0.mib
		Firmware Update	BROCADE-CC-BR7131-MIB-2.0.mib
		Wireless Stats	BROCADE-CC-BR7131-MIB-2.0.mib
		Radio Stats	BROCADE-CC-BR7131-MIB-2.0.mib
		Client Stats	BROCADE-CC-BR7131-MIB-2.0.mib
		Automatic Update	BROCADE-CC-BR7131-MIB-2.0.mib

SNMP allows a network administrator to manage network performance, find and solve network problems, and plan for network growth. The Brocade Mobility 7131 Series Access Point supports SNMP management functions for gathering information from its network components, communicating that information to specified users and configuring the access point. All the fields available within the access point are also configurable within the MIB.

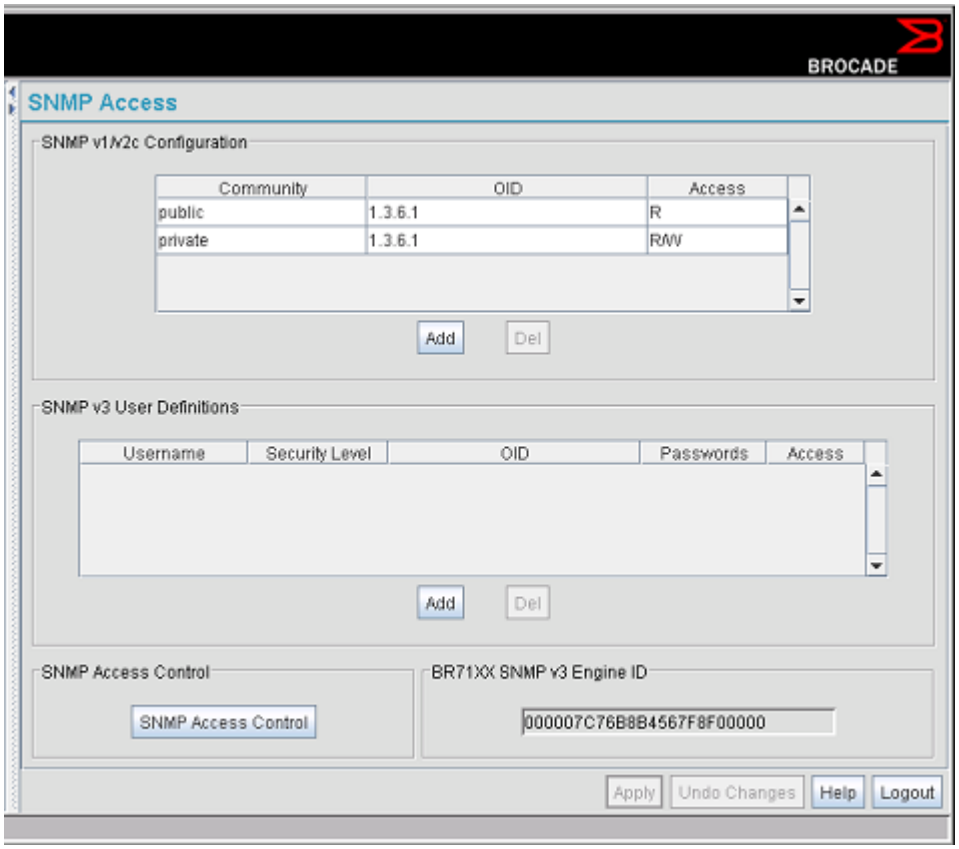
The Brocade Mobility 7131 Series Access Point SNMP agent functions as a command responder and is a multilingual agent responding to SNMPv1, v2c and v3 managers (command generators). The factory default configuration maintains SNMPv1/2c support of the community names, hence providing backward compatibility.

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 Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration - > SNMP Access* from the Brocade Mobility 7131 Series Access Point menu tree.



SNMP v1/v2c community definitions allow read-only or read/write access to Brocade Mobility 7131 Series Access Point 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. Brocade 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 Brocade Mobility 7131 Series Access Point 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 access point information, while read/write access allows a remote device to modify access point 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.
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 Brocade Mobility 7131 Series Access Point information, while read/write access allows a user to modify Brocade Mobility 7131 Series Access Pointsettings.

4. Specify the users who can read and optionally modify the SNMP-capable client.

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.

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

SNMP v3 Engine ID	The Brocade Mobility 7131 Series Access Point *SNMP v3 Engine ID* field lists the unique SNMP v3 Engine ID for the Brocade Mobility 7131 Series Access Point. 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 Brocade Mobility 7131 Series Access Point 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*

Configuring SNMP access control

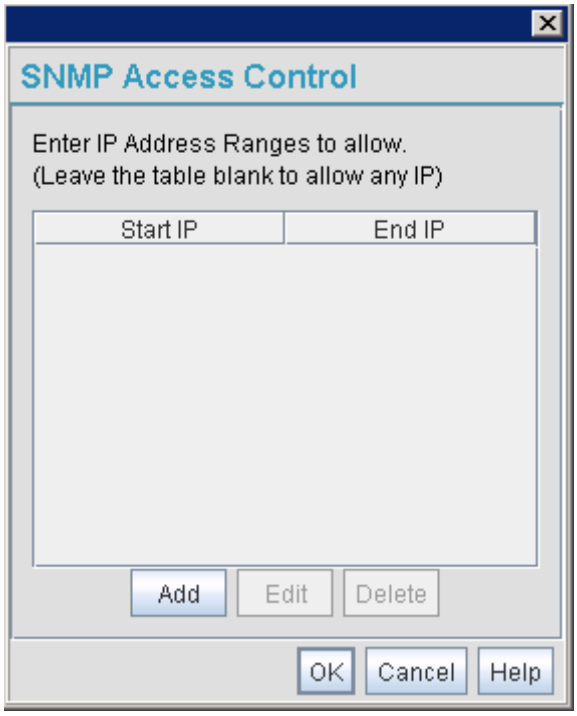
Use the *SNMP Access Control* screen (as launched from the SNMP Access screen) to specify which users can read SNMP generated information and, if capable, modify related settings from an SNMP-capable client.

Use the SNMP Access Control screen's *Access Control List (ACL)* to limit, by Internet Protocol (IP) address, who can access the Brocade Mobility 7131 Series Access Point SNMP interface.

NOTE
The ACL applies to both SNMP v3 user definitions and SNMP v1/v2c community definitions on the Brocade Mobility 7131 Series Access Point SNMP Access screen.

To configure SNMP user access control for the Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration - > SNMP Access* from the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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.

OK	Click *Ok* to return to the SNMP Access screen. Click *Apply* within the SNMP Access screen to save any changes made on the SNMP Access Control screen.
Cancel	Click *Cancel* to undo any changes made on the SNMP Access Control screen. This reverts all settings for this screen to the last saved configuration.

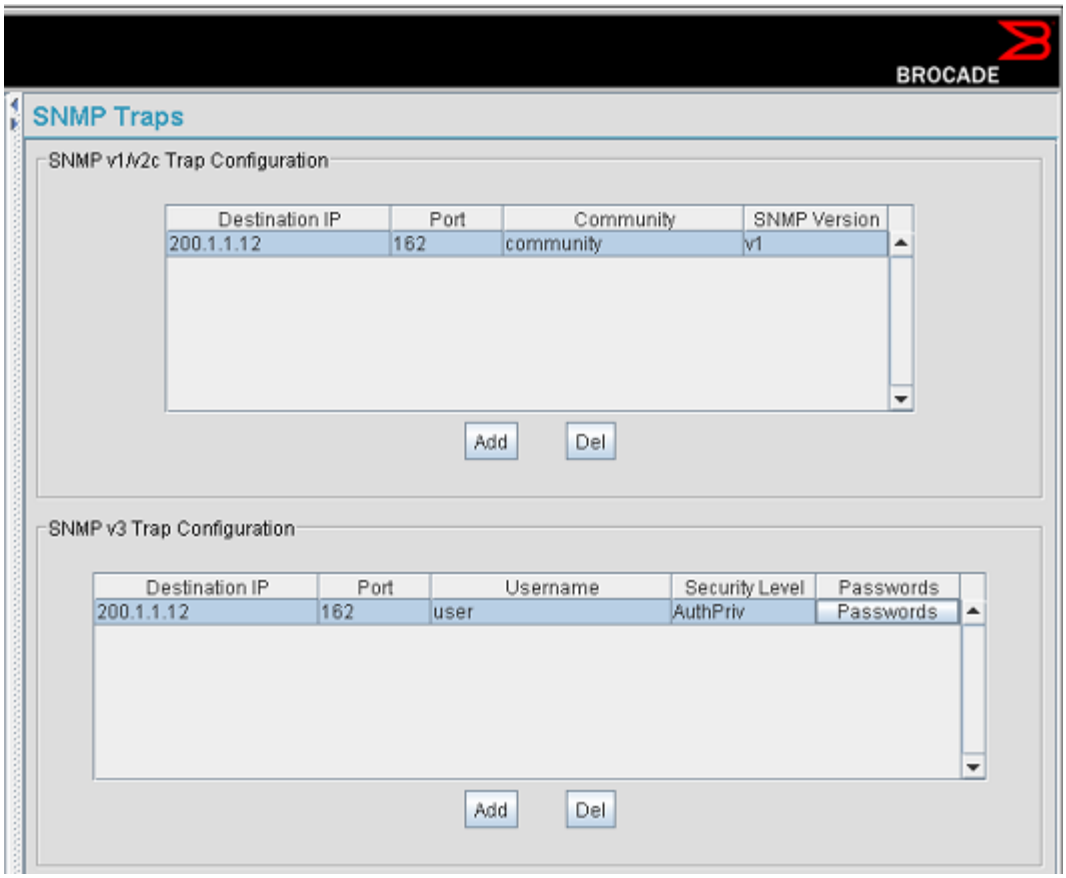
Enabling SNMP traps

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 Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration - > SNMP Access - > SNMP Trap Configuration* from the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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). 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)*.
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.

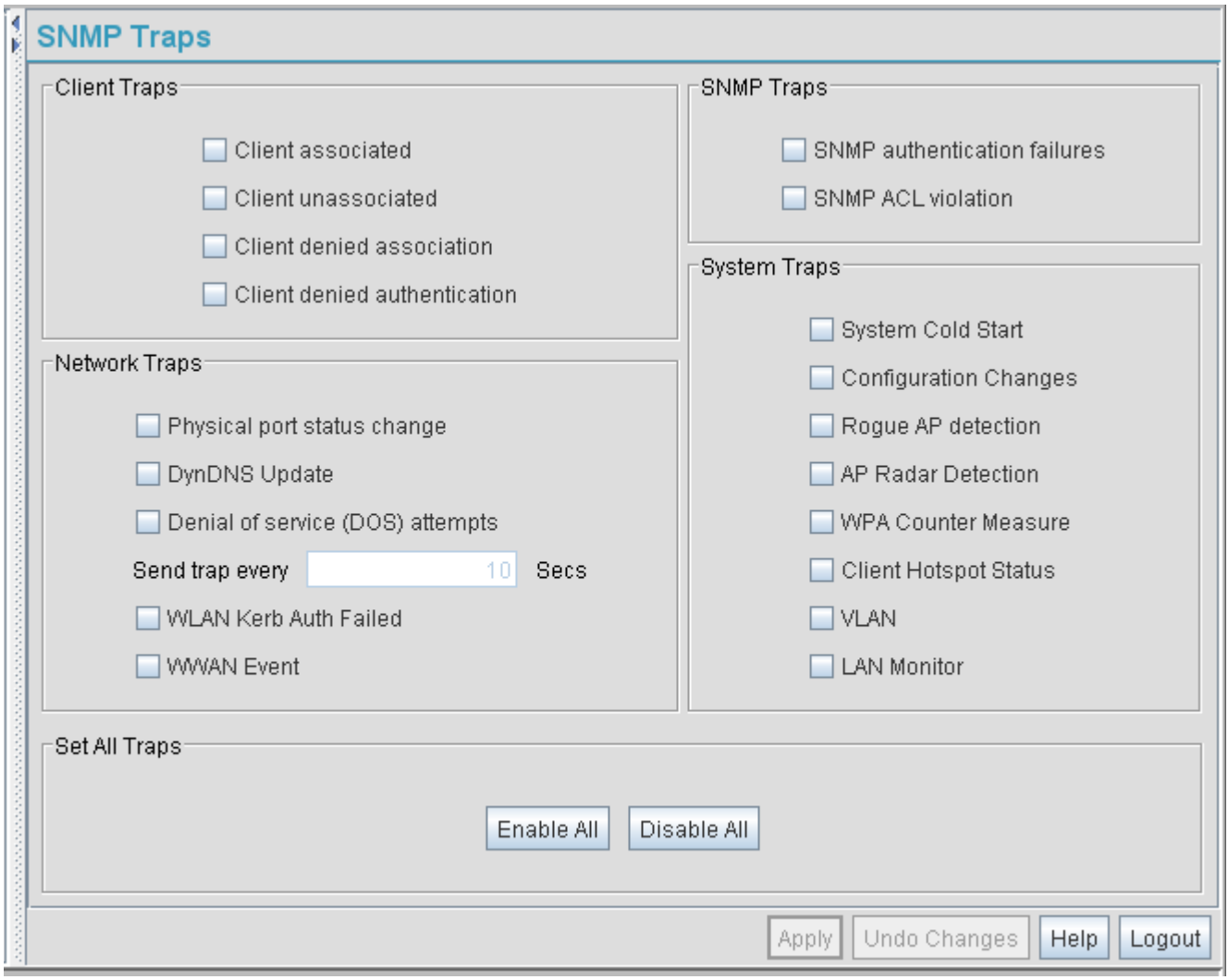
4. Click *Apply* to save any changes to the SNMP Trap Configuration screen. Navigating away from the screen without clicking the Apply button results in all changes being lost.

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 Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring specific SNMP traps

Use the *SNMP Traps* screen to enable specific traps on the Brocade Mobility 7131 Series Access Point. Brocade recommends defining traps to capture unauthorized devices operating within the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point:

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



2. Configure the *Client Traps* field to generate traps for Client associations, Client association denials and Client authentication denials. When a trap is enabled, a trap is sent every 10 seconds until the condition no longer exists.

Client Associated	Generates a trap when an Client becomes associated with one of the Brocade Mobility 7131 Series Access Point's WLANs.
Client Unassociated	Generates a trap when an Client becomes unassociated with (or gets dropped from) one of the Brocade Mobility 7131 Series Access Point's WLANs.
Client Denied Association	Generates a trap when an Client is denied association to a Brocade Mobility 7131 Series Access Point WLAN. Can be caused when the maximum number of clients for a WLAN is exceeded or when an Client violates the Brocade Mobility 7131 Series Access Point's *Access Control List (ACL).*
Client Denied Authentication	Generates a trap when an Client is denied authentication on one of the AP's WLANs. Can be caused by the Client being set for the wrong authentication type for the WLAN or by an incorrect key or password.

3. Configure the *SNMP Traps* field to generate traps when SNMP capable clients 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.

SNMP Authentication Failures	Generates a trap when an SNMP-capable client is denied access to the Brocade Mobility 7131 Series Access Point's SNMP management functions or data. This can result from an incorrect login, or missing/incorrect user credentials.
SNMP ACL Violation	Generates a trap when an SNMP client cannot access SNMP management functions or data due to an Access Control List (ACL) violation. This can result from a missing/incorrect IP address entered within the *SNMP Access Control* screen.

4. Configure the *Network Traps* field to generate traps when the Brocade Mobility 7131 Series Access Point'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 Brocade Mobility 7131 Series Access Point. The physical port status changes when a link is lost between the Brocade Mobility 7131 Series Access Point and a connected device.
DynDNS Update	Generates a trap whenever domain name information is updated as a result of the IP address associated with that domain being modified.
Denial of Service (DOS) Attempts	Generates a trap whenever a *Denial of Service (DOS)* attack is detected by the Brocade Mobility 7131 Series Access Point firewall. A new trap is sent at the specified interval until the attack has stopped.
Send Trap Every	Defines the interval in seconds the Brocade Mobility 7131 Series Access Point uses to generate a trap until the Denial of Service attack is stopped. Default is 10 seconds.

Physical Port Status Change	Generates a trap whenever the status changes on the Brocade Mobility 7131 Series Access Point. The physical port status changes when a link is lost between the Brocade Mobility 7131 Series Access Point and a connected device.
WLAN Kerb Auth Failed	Generates a trap when the access point detects a WLAN Kerberos authorization failure.
WWAN Event	Generates a trap when the access point detects the presence of a 3G WWAN card, the access point establishes (or fails to establish) a 3G WWAN connection, or the access point detects a 3G WWAN card disconnection, removal or resumed connection.

5. Configure the *System Traps* field to generate traps when the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point re-initializes while transmitting, possibly altering the SNMP agent's configuration or protocol entity implementation.
Configuration Changes	Generates a trap whenever changes to the Brocade Mobility 7131 Series Access Point's configuration file are saved.
Rogue AP Detection	Generates a trap if a Rogue AP is detected by the Brocade Mobility 7131 Series Access Point.
AP Radar Detection	Generates a trap if an AP is detected using a form of radar detection.
WPA Counter Measure	Generates a trap if an attack is detected against the WPA Key Exchange Mechanism.
Client Hotspot Status	Generates a trap when a change to the status of Client hotspot member is detected.
VLAN	Generates a trap when a change to a VLAN state is detected.
LAN Monitor	Generates a trap when a change to the LAN monitoring state is detected.

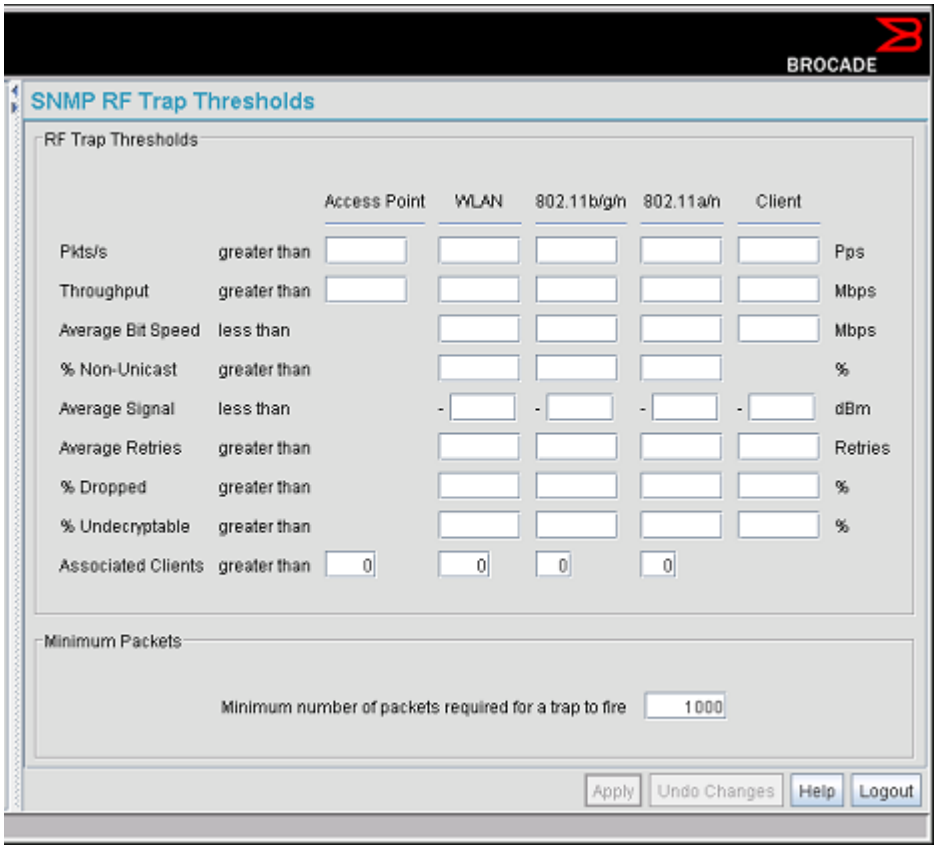
6. Click *Apply* to save any changes to the SNMP Traps screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.
7. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on SNMP Traps screen to the last saved configuration.
8. Click *Logout* to securely exit the Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring SNMP RF trap thresholds

Use the *SNMP RF Trap Threshold* screen as a means to track RF activity and the Brocade Mobility 7131 Series Access Point's radio and associated Client 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 Brocade Mobility 7131 Series Access Point, WLAN, selected radio and the associated Client.

To configure specific SNMP RF Traps on the Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration - > SNMP Access - > SNMP RF Trap Thresholds* from the menu tree.



2. Configure the *RF Trap Thresholds* field to define device threshold values for SNMP traps.

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).
Average Signal	Enter a minimum threshold for the average signal strength in dBm for each device.
Average Retries	Set a maximum threshold for the average number of retries for each device.
% Dropped	Enter a maximum threshold for the total percentage of packets dropped for each device. Dropped packets can be caused by poor RF signal or interference on the channel.
% Undecryptable	Define a maximum threshold for the total percentage of packets undecryptable for each device. Undecryptable packets can be the result of corrupt packets, bad CRC checks or incomplete packets.
Associated Clients	Set a maximum threshold for the total number of clients associated with each device.

NOTE
Average Bit Speed,% of Non-Unicast, Average Signal, Average Retries,% Dropped and % Undecryptable are not access point statistics.

3. Configure the *Minimum Packets* field to define a minimum packet throughput value for trap generation.

Minimum Number of Packets Required for a Trap to Fire	Enter the minimum number of packets that must pass through the device before an SNMP rate trap is sent. Brocade recommends using the default setting of 1000 as a minimum setting for the field.

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 Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring LLDP settings

A Radius server needs to know a password in clear text to support PEAP-MSCHAPv2 authentication. When the user database source is Active Directory, the Radius server is not be aware of a password and cannot proceed with the PEAP-MSCHAP authentication.

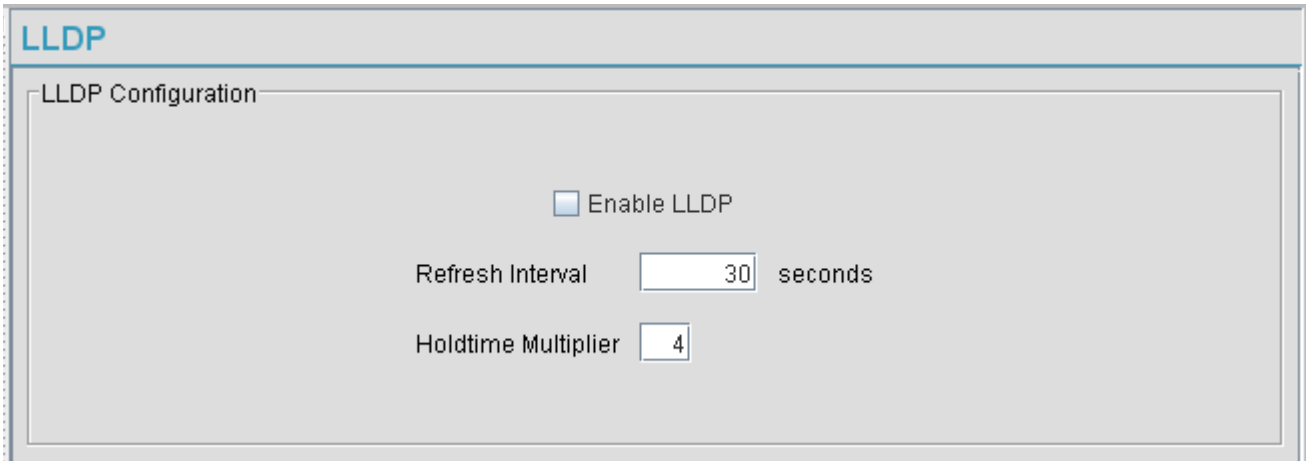
A Radius server initially attempts to connect with a primary LDAP server. If it fails to connect, the Radius server tries to connect with a secondary LDAP server. Afterwards, tries to connect and perform authentication with the primary and secondary LDAP servers in parallel.

While attempting authentication with the secondary LDAP server, the authentication procedure with primary LDAP server is initiated. This results in an authentication delay with the secondary LDAP server. As a result the procedure doesn't get completed with secondary LDAP server before the Radius timeout.

To address this issue, the unreachable LDAP server can be optionally designated as *unavailable* for a user-defined period. During this period, no attempt is made to connect with the unavailable server and the authentication procedure with the other server is carried out uninterrupted.

To configure LLDP support:

1. Select *System Configuration - > LLDP* from the menu tree.



2. Select the *Enable LLDP* radio button to designated a LDAP server as *unavailable* for a user-defined period.
3. Set a *Refresh Interval* (in seconds 5-32768) to define the interval at which LLDP frames are transmitted on behalf of a LLDP agent.
4. Set a *Holdtime Multipolar* (2-10) to define a multiplier on the refresh-interval that determines the actual TTL value used with LLDP.
5. Click *Apply* to save any changes to the LLDP screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.
6. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on LLDP screen to the last saved configuration.
7. Click *Logout* to securely exit the access point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring network time protocol (NTP)

Network Time Protocol (NTP) manages time and/or network clock synchronization in the Brocade Mobility 7131 Series Access Point-managed network environment. NTP is a client/server implementation. The Brocade Mobility 7131 Series Access Point (an NTP client) periodically synchronizes its clock with a master clock (an NTP server). For example, the Brocade Mobility 7131 Series Access Point 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 access point's network operations. For sites using Kerberos authentication, time synchronization is required. Use the *Date and Time Settings* screen to enable NTP and specify the IP addresses and ports of available NTP servers.

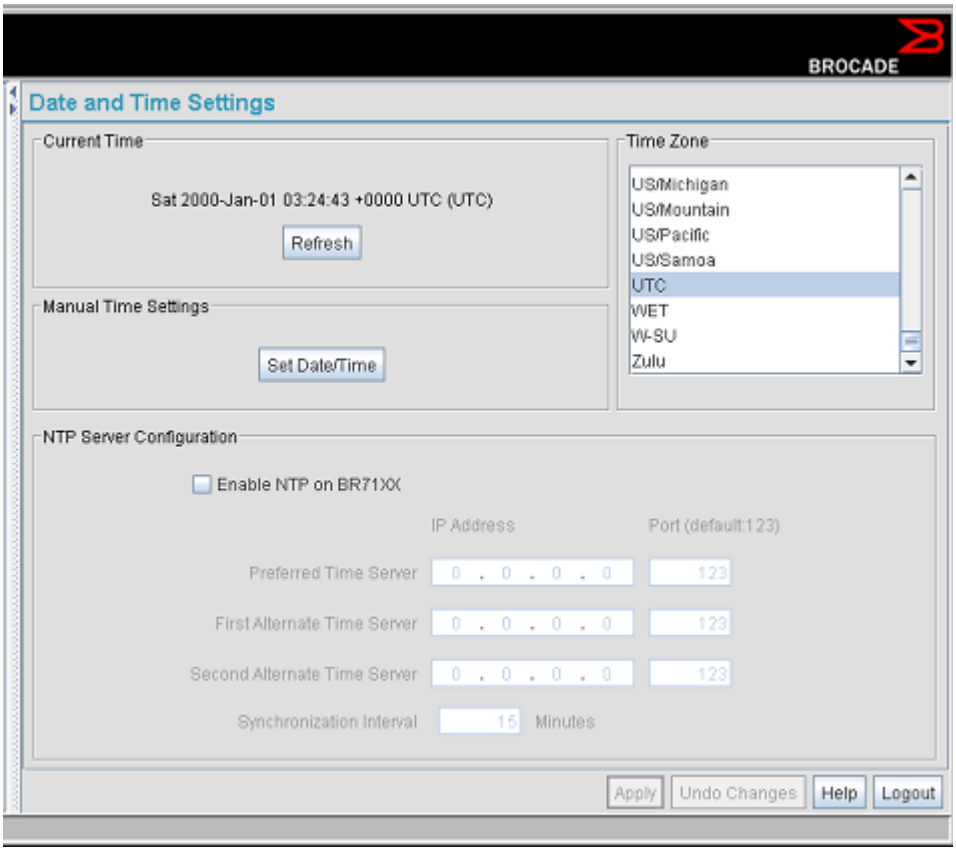
NOTE
The current time is not set accurately when initially connecting to the Brocade Mobility 7131 Series Access Point. Until a server is defined to provide the Brocade Mobility 7131 Series Access Point the correct time, or the correct time is manually set, the Brocade Mobility 7131 Series Access Point displays 1970-01-01 00:00:00 as the default time.

CAUTION

If using the Radius time-based authentication feature to authenticate access point user permissions, ensure *UTC* has been selected from the Date and Time Settings screen's *Time Zone* field. If UTC is not selected, time based authentication will not work properly. For information on configuring Radius time-based authentication, see "Defining user access permissions by group" on page 254.

To manage clock synchronization on the Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration - > Date/Time* from the Brocade Mobility 7131 Series Access Point menu tree.



2. From within the *Current Time* field, click the *Refresh* button to update the time since the screen was displayed by the user.

   The Current Time field displays the current time based on the Brocade Mobility 7131 Series Access Point system clock. If NTP is disabled or if there are no servers available, the system time displays the Brocade Mobility 7131 Series Access Point uptime starting at 1970-01-01 00:00:00, with the time and date advancing.

3. Select the *Set Date/Time* button to display the *Manual Date/Time Setting* screen.

   This screen enables the user to manually enter the access point's system time using a Year-Month-Day HH:MM:SS format.

This option is disabled when the Enable NTP checkbox has been selected, and therefore should be viewed as a second means to define the access point system time.

4. If using the Manual Date/Time Setting screen to define the access point's system time, refer to the *Time Zone* field to select the time used to use as complimentary information to the information entered within the Manual Date/Time Setting screen.

CAUTION

If using the Radius time-based authentication feature to authenticate access point user permissions, ensure *UTC* has been selected from the *Time Zone* field. If UTC is not selected, time based authentication will not work properly. For information on configuring Radius time-based authentication, see "Defining user access permissions by group" on page 254.

5. If using an NTP server to supply system time to the access point, configure the *NTP Server Configuration* field to define the server network address information required to acquire the Brocade Mobility 7131 Series Access Point network time.

Enable NTP on Brocade Mobility 7131 Series Access Point	Select the *Enable NTP on* Brocade Mobility 7131 Series Access Point checkbox to allow a connection between the Brocade Mobility 7131 Series Access Point and one or more specified NTP servers. A preferred, first alternate and second alternate NTP server cannot be defined unless this checkbox is selected. Disable this option (uncheck the checkbox) if Kerberos is not in use and time synchronization is not necessary. This option is disa bled by default.
Preferred Time Server	Specify the numerical (non DNS name) IP address and port of the primary NTP server. The default port is 123.
First Alternate Time Server	Optionally, specify the numerical (non DNS name) IP address and port of an alternative NTP server to use for time synchronization if the primary NTP server goes down.
Second Alternate Time Server	Optionally, specify the numerical (non DNS name) and port of yet another NTP server for the greatest assurance of uninterrupted time synchronization.
Synchronization Interval	Define an interval in minutes the Brocade Mobility 7131 Series Access Point uses to synchronize its system time with the NTP server. A synchronization interval value from 15 minutes to 65535 minutes can be specified. For implementations using Kerberos, a synchronization interval of 15 minutes (default interval) or sooner is recommended.

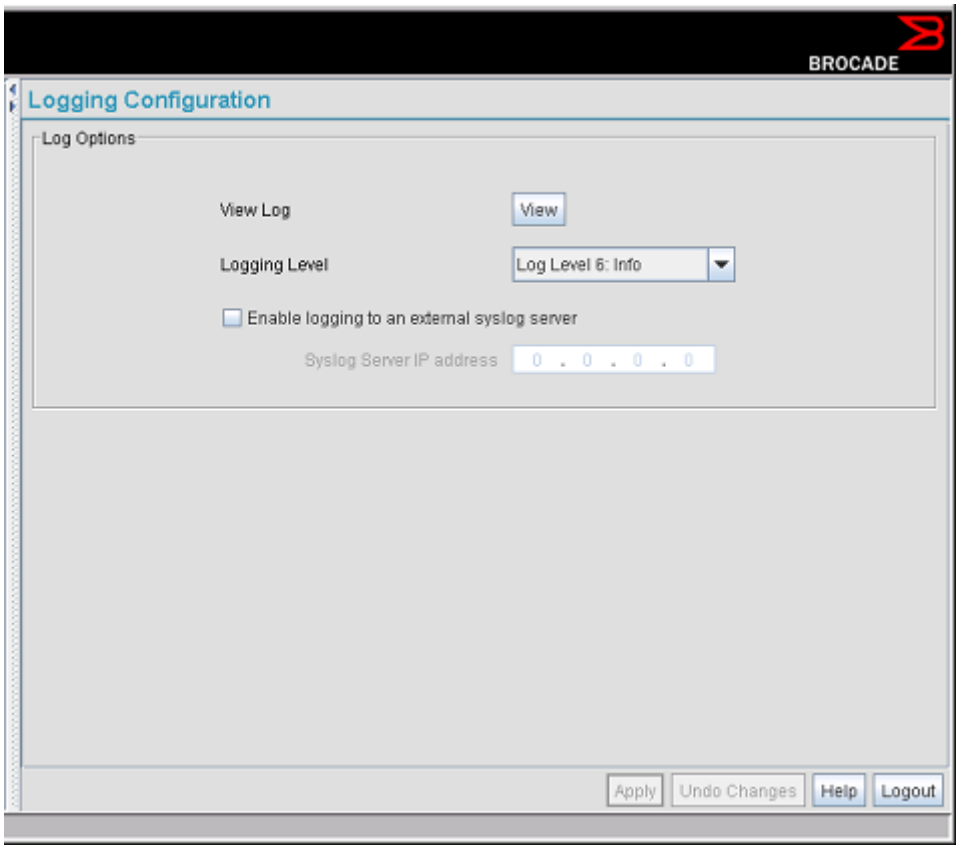
6. Click *Apply* to save any changes to the Date and time Settings screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost.
7. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on Date and Time Settings screen to the last saved configuration.
8. Click *Logout* to securely exit the Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Logging configuration

The Brocade Mobility 7131 Series Access Point provides the capability for periodically logging system events that prove useful in assessing the throughput and performance of the Brocade Mobility 7131 Series Access Point or troubleshooting problems on the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point system log.

To configure event logging for the Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration - > Logging Configuration* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the *Log Options* field to save event logs, set the log level and optionally port the Brocade Mobility 7131 Series Access Point's log to an external server.

View Log	Click *View* to save a log of events retained on the Brocade Mobility 7131 Series Access Point. 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 Brocade Mobility 7131 Series Access Point log file. Log entries are not saved in the Brocade Mobility 7131 Series Access Point. While the AP is in operation, log data temporarily resides in memory. AP memory is completely cleared each time the AP reboots.
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 Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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.

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 Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Importing/exporting configurations

All of the configuration settings for a Brocade Mobility 7131 Series Access Point can be obtained from another Brocade Mobility 7131 Series Access Point in the form of a text file. Additionally, all of the Brocade Mobility 7131 Series Access Point's settings can be downloaded to another Brocade Mobility 7131 Series Access Point. Use the file-based configuration feature to speed up the setup process significantly at sites using multiple Brocade Mobility 7131 Series Access Points.

Another benefit is the opportunity to save the current AP configuration before making significant changes or restoring the default configuration. All options on the access point are deleted and updated by the imported file. Therefore, the imported configuration is not a merge with the configuration of the target access point. The exported file can be edited with any document editor if necessary.

NOTE
Use the *System Settings* screen as necessary to restore a Brocade Mobility 7131 Series Access Point's default configuration. For more information on restoring configurations, see "Configuring system settings" on page 63.

The export function will always export the encrypted Admin User password. The import function will import the Admin Password only if the access point is set to factory default. If the access point is not configured to factory default settings, the Admin User password WILL NOT get imported.

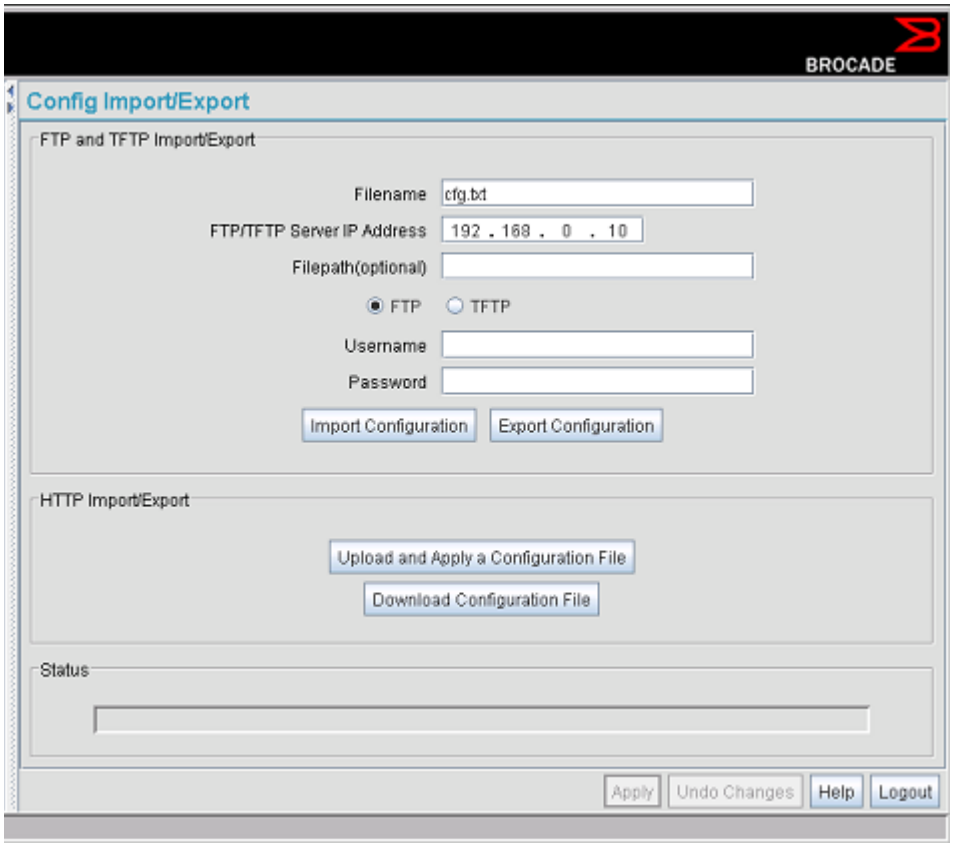
NOTE
When modifying the text file manually and spaces are used for wireless, security, Client policy names etc., ensure you use "\20" between the spaces. For example, "Second\20Floor\20Lab". When imported, the name would display as "Second Floor Lab".

CAUTION
A single-radio model access point cannot import/export its configuration to a dual-radio model access point. In turn, a dual-radio model access point cannot import/export its configuration to a single-radio access point.

Use the *Config Import/Export* screen to configure an import or export operation for Brocade Mobility 7131 Series Access Point configuration settings.

To create an importable/exportable Brocade Mobility 7131 Series Access Point configuration file:

1. Select *System Configuration - > Config Import/Export* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the *FTP and TFTP Import/Export* field to import/export configuration settings.

Filename	Specify the name of the configuration file to be written to the server.
Server IP	Enter the numerical (non DNS name) IP address of the destination SFTP, FTP or TFTP server where the configuration file is imported or exported.
Filepath (optional)	Defines the optional path name used to import/export the target configuration file.
SFTP	Select the SFTP radio button if using an SFTP server to import or export the configuration.
TFTP	Select the TFTP radio button if using an FTP server to import or export the configuration.
FTP	Select the FTP radio button if using an FTP server to import or export the configuration.
TFTP	Select the TFTP radio button if using an FTP server to import or export the configuration.
Username	Specify a username to be used when logging in to the FTP server. A username is not required for TFTP server logins.

Password	Define a password allowing access to the server for the import or export operation.
Import Configuration	Click the *Import Configuration* button to import the configuration file from the server with the assigned filename and login information. The system displays a confirmation window indicating the administrator must log out of the Brocade Mobility 7131 Series Access Point after the operation completes for the changes to take effect. Click *Yes* to continue the operation. Click *No* to cancel the configuration file import.
Export Configuration	Click the *Export Configuration* button to export the configuration file from the server with the assigned filename and login information. If the IP mode is set to DHCP Client, IP address information is not exported (true for both LAN1, LAN2 and the WAN port). For LAN1 and LAN2, IP address information is only exported when the IP mode is set to either static or DHCP Server. For the WAN port, IP address information is only exported when the *This interface is a DHCP Client* checkbox is not selected. The system displays a confirmation window prompting the administrator to log out of the Brocade Mobility 7131 Series Access Point after the operation completes for the changes to take effect. Click *Yes* to continue the operation. Click *No* to cancel the configuration file export.

3. Configure the *HTTP Import/Export* field to import/export Brocade Mobility 7131 Series Access Point configuration settings using HTTP.

CAUTION

For HTTP downloads (exports) to be successful, pop-up messages must be disabled.

Upload and Apply a Configuration File	Click the *Upload and Apply A Configuration File* button to upload a configuration file to this access point using HTTP.
Download Configuration File	Click the *Download Configuration File* button to download this access point's configuration file using HTTP.

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.

CAUTION

If errors occur when importing the configuration file, a parsing message displays defining the line number where the error occurred. The configuration is still imported, except for the error. Consequently, it is possible to import an invalid configuration. The user is required to fix the problem and repeat the import operation until an error-free import takes place.

NOTE

Brocade recommends importing configuration files using the CLI. If errors occur during the import process, they display all at once and are easier to troubleshoot. The access point GUI displays errors one at a time, and troubleshooting can be a more time-consuming process.

NOTE

When importing the configuration, a *xxxxxbytes loaded* status message indicates the file was downloaded successfully. An *Incompatible Hardware Type Error* message indicates the configuration was not applied due to a hardware compatibility issue between the importing and exporting devices.

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 Brocade Mobility 7131 Series Access Point Brocade Access Point applet. A prompt displays confirming the logout before the applet is closed.

Updating device firmware

Brocade periodically releases updated versions of the Brocade Mobility 7131 Series Access Point device firmware to the Brocade Web site. If the Brocade Mobility 7131 Series Access Point firmware version displayed on the *System Settings* page (see "Configuring system settings" on page 63) is older than the version on the Web site, Brocade recommends updating the Brocade Mobility 7131 Series Access Point to the latest firmware version for full feature functionality.

The access point's automatic update feature updates the access point's firmware and configuration file automatically when the access point is reset or when the access point initiates a DHCP request.

The firmware is automatically updated each time firmware versions are found to be different between what is running on the access point and the firmware file located on the server. The configuration file is automatically updated when the configuration file name on the server is different than the name of the file previously loaded on the access point or when the file version (on the server) is different than the version currently in use on the access point.

Additionally, the configuration version can be manually changed in the text file to cause the configuration to be applied when required. The parameter name within the configuration file is *"cfg-version-1.1-01."* The access point only checks the two characters after the third hyphen (01) when making a comparison. Change the last two characters to update the access point's configuration. The two characters can be alpha-numeric.

Upgrading from a legacy to a new firmware version is a two step process requiring the same upgrade procedure to be repeated twice. The first upgrade will result in a bootloader change, and the second upgrade will result in the actual firmware update. For subsequent upgrades, a single download will suffice. Using Auto Update, the access point will automatically update itself twice when upgrading.

Upgrading to a new access point firmware baseline does not retain the configuration of the previous (lower version) firmware. Brocade recommends users export their 1.0 configuration for backup purposes prior to upgrading.

CAUTION

When downloading to a lower firmware version, all configuration settings are lost and the access point returns to factory default settings of the lower version.**If downgrading firmware from to a lower version, the access point automatically reverts to default settings of the lower version, regardless of whether you are downloading the firmware manually or using the automatic download feature. The automatic feature allows the user to download the configuration file at the same time, but since the firmware reverts to the default settings of the lower version, the configuration file is ignored.Loaded and signed CA certificates will be lost when changing the access point's firmware version using either the GUI or CLI. After a certificate has been successfully loaded, export it to a secure location to ensure its availability after a firmware update.**

If restoring the access point's factory default firmware, you must export the certificate file BEFORE restoring the access point's factory default configuration. Import the file back after the updated firmware is installed.

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 a SFTP, FTP or TFTP site to perform the update.

CAUTION

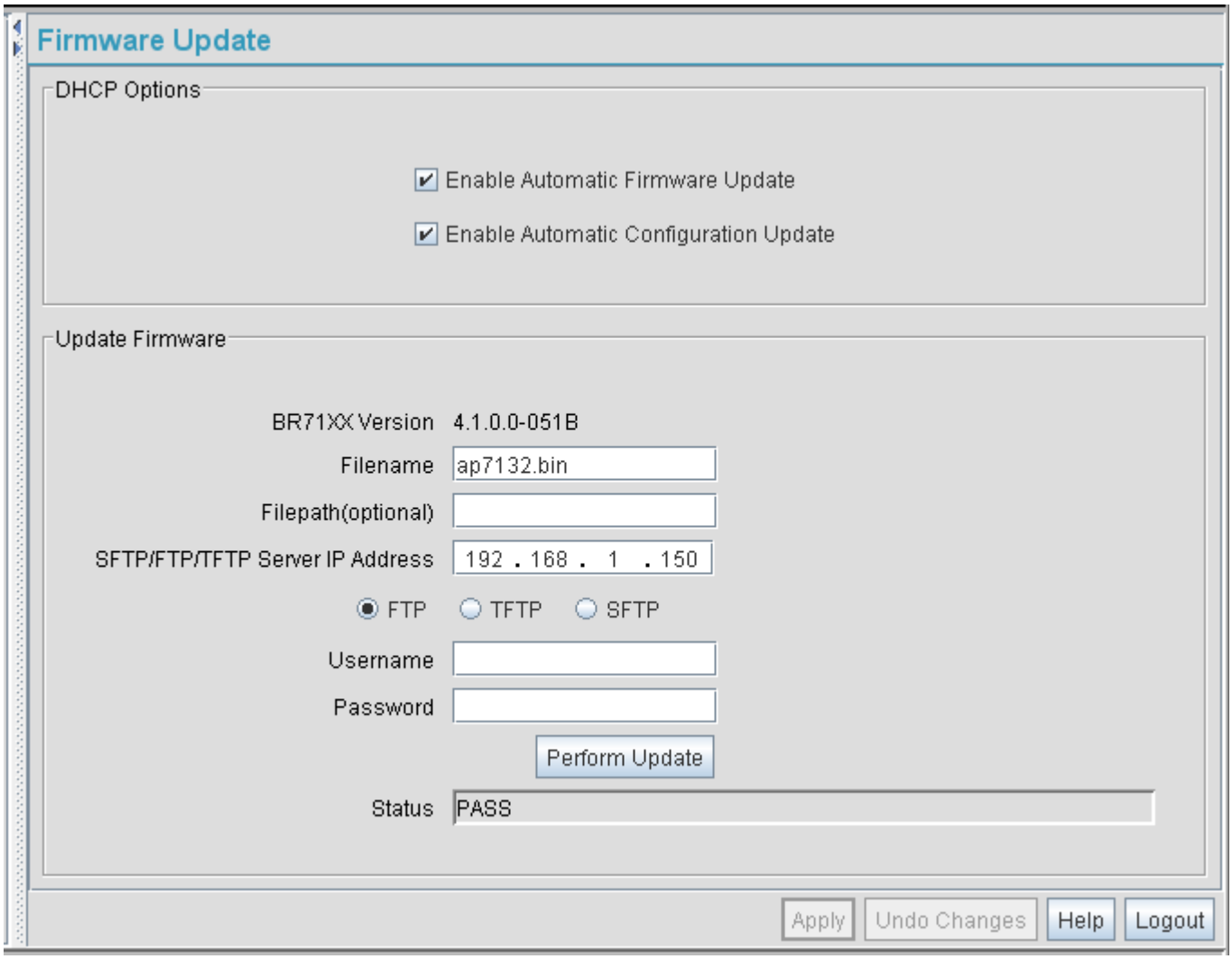
Make sure a copy of the Brocade Mobility 7131 Series Access Point's configuration is exported before updating the firmware.

To conduct a firmware update on the Brocade Mobility 7131 Series Access Point:

1. Export the Brocade Mobility 7131 Series Access Point 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 103 for instructions on exporting the Brocade Mobility 7131 Series Access Point's current configuration to have it available after the firmware is updated.

2. Select *System Configuration - > Firmware Update* from the Brocade Mobility 7131 Series Access Point menu tree.



3. Configure the *DHCP Options* checkboxes to enable/disable automatic firmware and/or configuration file updates.

   DHCP options are used for out-of-the-box rapid deployment for Brocade wireless products. The following are the two options available on the access point:

   - Enable Automatic Firmware Update
   - Enable Automatic Configuration Update

   Both DHCP options are enabled by default.

   These options can be used to update newer firmware and configuration files on the access point.

   The update is conducted over the LAN or WAN port depending on which server responds first to the access point's request for an automatic update.

Enable Automatic Firmware Update	Enable this checkbox to allow an automatic firmware update when firmware versions are found to be different between what is running on the access point and the firmware that resides on the server. A firmware update will only occur if the access point is reset or when the access point does a DHCP request. This feature is used in conjunction with DHCP/BootP options configured on a DHCP or BootP server. If this checkbox is not enabled, the firmware update is required to be conducted manually.
Enable Automatic Configuration Update	Select this checkbox to allow an automatic configuration update when the configuration filenames are found to be different between the filename loaded on the access point and the configuration filename that resides on the server or when the configuration file versions are found to be different between the configuration file version loaded on the access point and the configuration file that resides on server. A configuration update will only occur if the access point is reset or when the access point does a DHCP request. This feature is used in conjunction with DHCP/BootP options configured on a DHCP or BootP server. . If this checkbox is not enabled, the configuration update is required to be done manually.

CAUTION

If using a Linux server configured to support the "bf" option, an automatic firmware update is not be triggered unless both the *Enable Automatic Firmware Update* and *Enable Automatic Configuration Update* options are selected. If the Configuration Update option is disabled, the access point will not download the configuration file. Without the configuration file, the access point cannot parse for the firmware file name required to trigger the firmware update.

If updating the access point manually, configure the *Update Firmware* fields as required to set a filename and target firmware file upload location for 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 SFTP, FTP or TFTP server used for the update. Only numerical IP address names are supported, no DNS can be used.
7. Select *FTP* or *TFTP* or *SFTP* to define whether the firmware file resides on a FTP or TFTP server.
8. Set the following FTP, TFTP or SFTP parameters:
   - *Username* - Specify a username for the FTP or SFTP server login.
   - *Password* - Specify a password for FTP or SFTP server login. Default is Brocade. A blank password is not supported.

NOTE

Click *Apply* to save the settings before performing the firmware update. The user is not able to navigate the Brocade Mobility 7131 Series Access Point user interface while the firmware update is in process.

9. Click the *Perform Update* button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update.

NOTE
The access point must complete the reboot process to successfully update the device firmware, regardless of whether the reboot is conducted using the GUI or CLI interfaces.

10. 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

11. Confirm the Brocade Mobility 7131 Series Access Point configuration is the same as it was before the firmware update. If they are not, restore the settings. Refer to "Importing/exporting configurations" on page 103 for instructions on exporting the configuration back to the Brocade Mobility 7131 Series Access Point.
12. 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.
13. 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.
14. Click *Logout* to securely exit the Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Chapter

Network Management 5

In this chapter

- Configuring the LAN interface. 113
- Configuring WAN settings 125
- Enabling wireless LANs (WLANs) 137
- Configuring router settings 178
- Configuring IP filtering. 182

Configuring the LAN interface

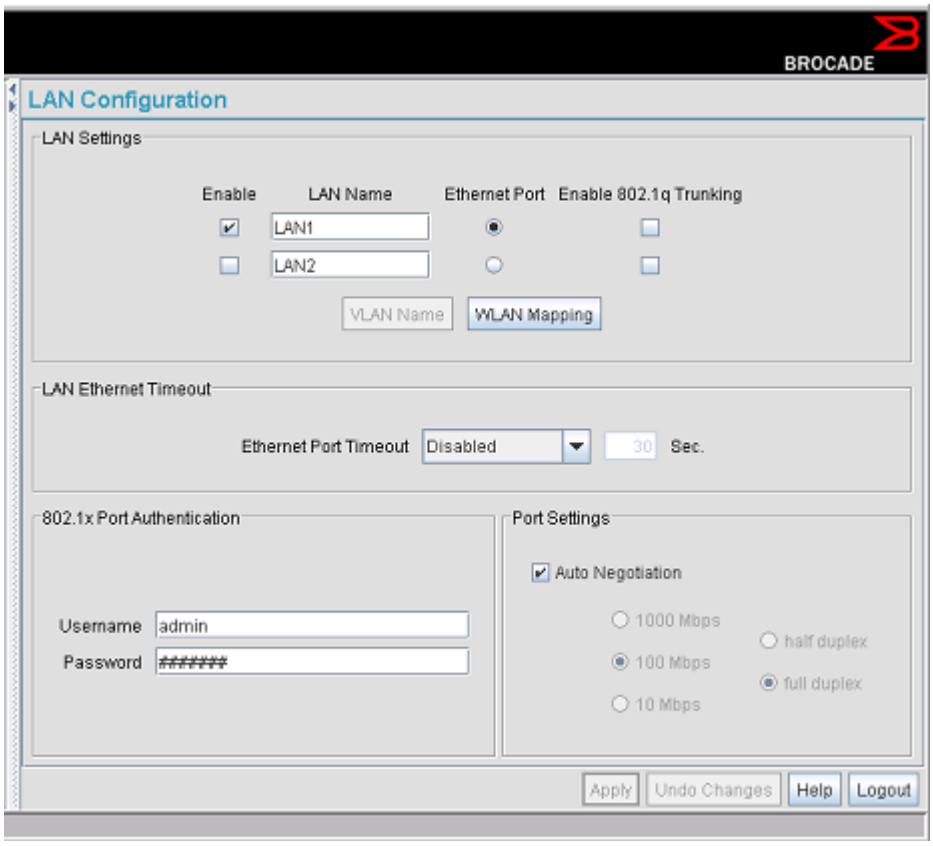
The Brocade Mobility 7131 Series Access Point has one physical LAN port supporting two unique LAN interfaces. The Brocade Mobility 7131 Series Access Point LAN port has its own MAC address. The LAN port MAC address is always the value of the Brocade Mobility 7131 Series Access Point WAN port MAC address plus 1. The LAN and WAN port MAC addresses can be located within the LAN and WAN Stats screens.

For information on locating the access point's MAC addresses, see "Viewing WAN statistics" on page 259 and "Viewing LAN statistics" on page 263.

Use the *LAN Configuration* screen to enable one (or both) of the access point's LAN interfaces, assign them names, define which LAN is currently active on the access point Ethernet port and assign a timeout value to disable the LAN connection if no data traffic is detected within a defined interval.

To configure the Brocade Mobility 7131 Series Access Point LAN interface:

1. Select *Network Configuration -> LAN* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the *LAN Setting*s field to enable the Brocade Mobility 7131 Series Access Point LAN1 and/or LAN2 interface, assign a timeout value, enable 802.1q trunking, configure WLAN mapping and enable 802.1x port authentication.

Enable	Select the LAN1 and/or LAN2 checkbox to allow the forwarding of data traffic over the specified LAN connection. The LAN1 connection is enabled by default, but both LAN interfaces can be enabled simultaneously. The LAN2 setting is disabled by default.
LAN Name	Use the *LAN Name* field to modify the existing LAN name. LAN1 and LAN2 are the default names assigned to the LANs until modified by the user.
Ethernet Port	The *Ethernet Port* radio buttons allow you to select one of the two available LANs as the LAN actively transmitting over the access point's LAN port. Both LANs can be active at any given time, but only one can transmit over the access point's physical LAN connection, thus the selected LAN has priority.
Enable 802.1q Trunking	Select the *Enable 802.1q Trunking* checkbox to enable the LAN to conduct VLAN tagging. If selected, click the *WLAN Mapping* button to configure mappings between individual WLANs and LANs. If enabled, the access point is required to be connected to a trunked port.

VLAN Name	Click the *VLAN Name* button to launch the *VLAN Name* screen to create VLANs and assign them VLAN IDs.
WLAN Mapping	Click the *WLAN Mapping* button to launch the *VLAN Configuration* screen to map existing WLANs to one of the two LANs and define the WLAN's VLAN membership (up to 16 mappings are possible per access point).

3. Refer to the *LAN Ethernet Timeout* field to define how LAN Ethernet inactivity is processed by the access point.

   Use the *Ethernet Port Timeout* drop-down menu to define how the access point interprets inactivity for the LAN assigned to the Ethernet port. When *Enabled* is selected, the access point uses the value defined in the *Sec.* box (default is 30 seconds). Selecting *Disabled* allows the LAN to use the Ethernet port for an indefinite timeout period. Select the *Hardware Detect* option to use the pyhsical LAN port to detect activity. If the LAN port does not detect a physical connection, the radio is unavailable to the access point.

4. Refer to the *802.1x Port Authentication* field if using port authentication over the access point's LAN port.

   The access point only supports 802.1x authentication over its LAN port. The access point behaves as an 802.1x supplicant to authenticate to a server on the network. If using 802.1x authentication, enter the authentication server user name and password. The default password is "*admin123*." For information on enabling and configuring authentication schemes on the access point, see "Enabling authentication and encryption schemes" on page 194.

5. Use the *Port Settings* field to define how the access point manages throughput over the LAN port.

Auto Negotiation	Select the *Auto Negotiation* checkbox to enable the access point to automatically exchange information (over its LAN port) about data transmission speed and duplex capabilities. Auto negotiation is helpful when using the access point in an environment where different devices are connected and disconnected on a regular basis. Selecting Auto Negotiate disables the Mbps and duplex checkbox options.
100 Mbps	Select this option to establish a 100 Mbps data transfer rate for the selected half duplex or full duplex transmission over the access point's LAN port. This option is not available if Auto Negotiation is selected.
10 Mbps	Select this option to establish a 10 Mbps data transfer rate for the selected half duplex or full duplex transmission over the access point's LAN port. This option is not available if Auto Negotiation is selected.
Half Duplex	Select this option to transmit data to and from the access point, but not at the same time. Using a half duplex transmission, the access point can send data over its LAN port then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time.
Full Duplex	Select this option to transmit data to and from the access point at the same time. Using full duplex, the access point can send data over its LAN port while receiving data as well.

6. 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 if the prompts are ignored.
7. 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.
8. Click *Logout* to securely exit the Brocade Mobility 7131 Series Access Point Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring VLAN support

A *Virtual Local Area Network (VLAN)* is a means to electronically separate data on the same Brocade Mobility 7131 Series Access Point from a single broadcast domain into separate broadcast domains. The Brocade Mobility 7131 Series Access Point 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 access point (regardless of the access point being single or dual-radio model). An administrator can map 16 WLANs to 16 VLANs and enable or disable dynamic VLAN assignment.

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 clients even when they are not members of the same network segment.

NOTE
Ensure the IKE authentication Passphrase is the same as the Pre-shared key on the Cisco PIX device.

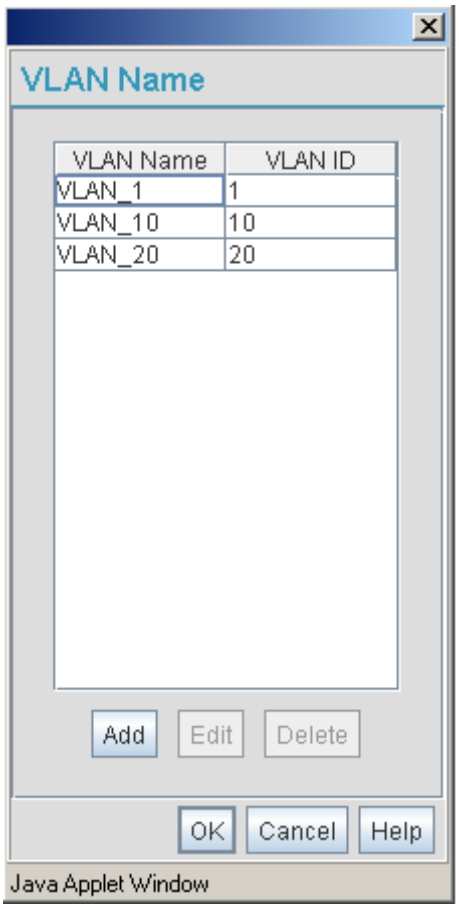
The Brocade Mobility 7131 Series Access Point assignment of VLANs can be implemented using Static or Dynamic assignments (often referred to as memberships) for individual WLANs. Both methods have their advantages and disadvantages. Static VLAN membership is perhaps the most widely used method because 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 Brocade Mobility 7131 Series Access Point sending a DHCP request for device information (such as an IP address). Additional information (such as device MAC address information) is sent to the Brocade Mobility 7131 Series Access Point. The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point. The Brocade Mobility 7131 Series Access Point 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:

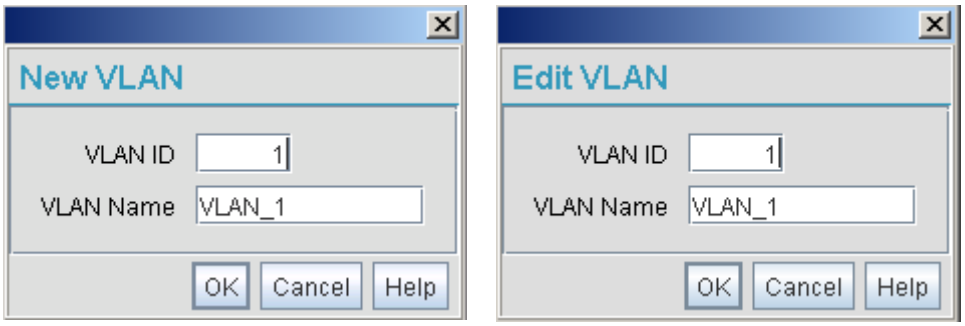
1. Select *Network Configuration -> LAN* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Ensure the *Enable 802.1q Trunking* button is selected from within the LAN Setting field.

   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 Brocade Mobility 7131 Series Access Point 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 *Add* 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 Brocade Mobility 7131 Series Access Point 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.

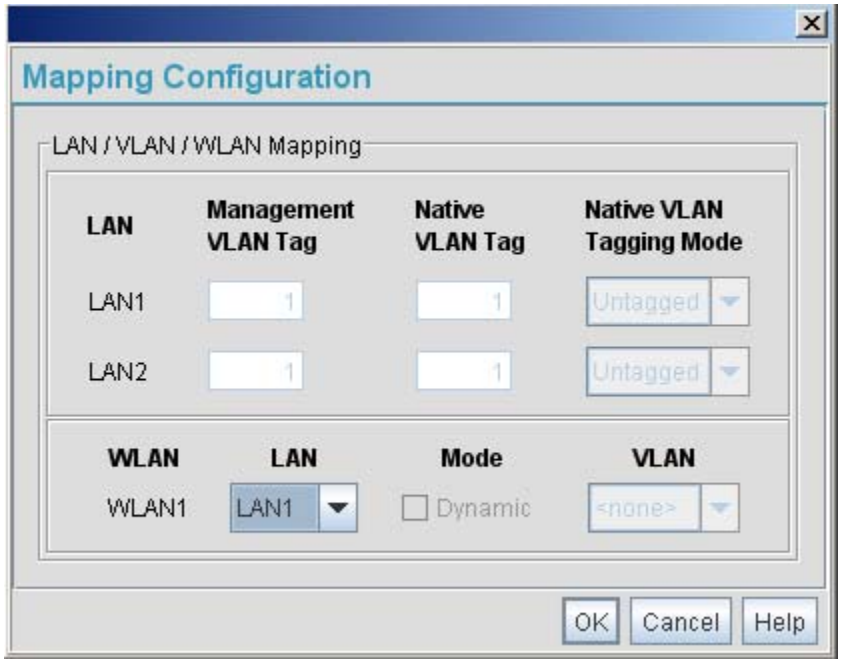
   A business may have offices in different locations and want to extend an internal LAN between the locations. A Brocade Mobility 7131 Series Access Point managed infrastructure could provide this connectivity, but it requires VLAN numbering be managed carefully to avoid conflicts between two VLANs with the same ID.

5. Define a 32 character maximum *VLAN Name*.

   Enter a unique name that identifies members of the VLAN. Brocade 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.

7. From the LAN Configuration screen, click the *WLAN Mapping* button. The *Mapping Configuration* screen displays.



8. Enter a *Management VLAN Tag* for LAN1 and LAN2.

   The Management VLAN uses a default tag value of 1. The Management VLAN is used to distinguish VLAN traffic flows for the LAN. The trunk port marks the frames with special tags as they pass between the Brocade Mobility 7131 Series Access Point 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* for LAN1 and LAN2.

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

10. Use the *Native VLAN Tagging Mode* drop-down menu to define whether the native VLAN applies a tag to traffic.

    A tagged VLAN uses an extra tag in the MAC header to identify a frame's VLAN membership. This tag helps define the VLAN and QoS priority. A tagged frame is four bytes longer than an untagged frame and contains two bytes of *Tag Protocol Identifier* (TPID) information within the type and length field of an Ethernet frame and two bytes of *Tag Control Information* (TCI) after the Ethernet frame's source address field.

    When *Tagged* is selected from the drop-down menu, the access point forwards all tagged frames in the native VLAN and admits only tagged frames on trunks. When Tagged is selected the access point drops any untagged traffic, including untagged traffic in the native VLAN. *Untagged* is selected by default.

11. Use the *LAN* drop-down menu to map one of the two LANs to the WLAN listed to the left. With this assignment, the WLAN uses this assigned LAN interface.

12. Select the *Dynamic* checkboxes (under the *Mode* column) to configure the VLAN mapping as a dynamic VLAN.

    Using Dynamic VLAN assignments, a *VMPS (VLAN Management Policy Server)* dynamically assigns VLAN ports. The Brocade Mobility 7131 Series Access Point uses a separate server as a VMPS server. When a frame arrives on the Brocade Mobility 7131 Series Access Point, 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 configured. Otherwise, the checkbox is disabled.

13. Use the *VLAN* drop-down menu to select the name of the target VLAN to map to the WLAN listed on the left-hand side of the screen.

    Brocade recommends mapping VLANs strategically in order to keep VLANs tied to the discipline they most closely match. For example, If WLAN1 is comprised of clients supporting the sales area, then WLAN1 should be mapped to sales if a sales VLAN has been already been created.

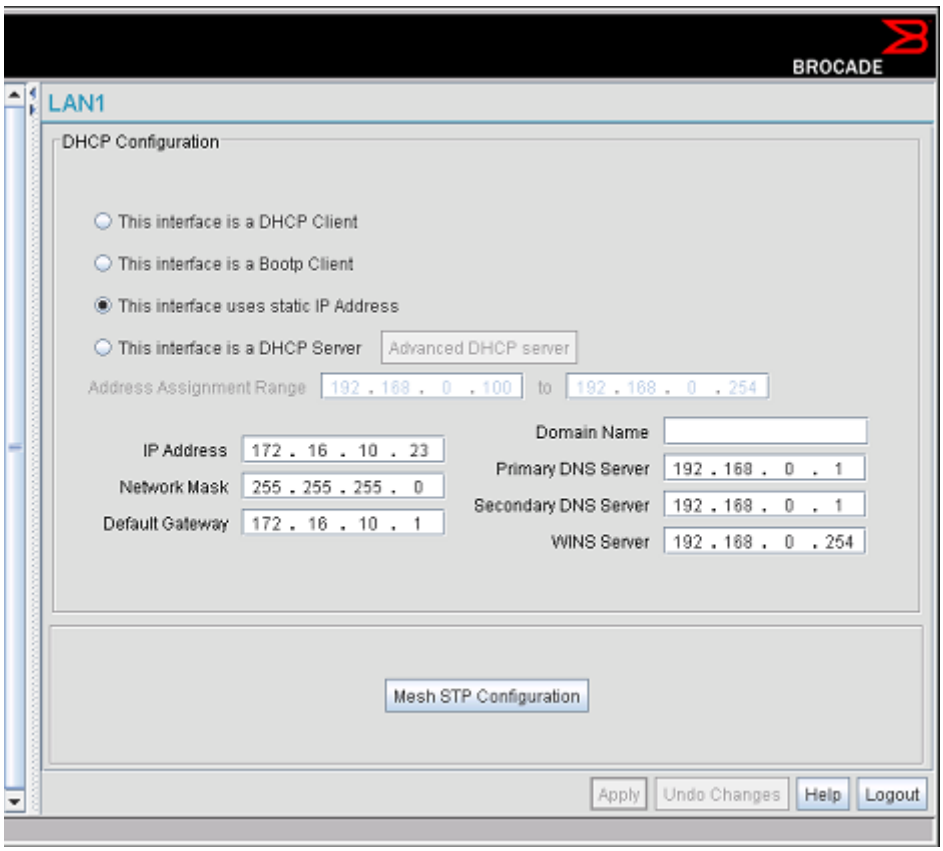
14. Click *Apply* to return to the *VLAN Name* screen. Click *OK* to return to the LAN screen. Once at the LAN screen, click *Apply* to re-apply your changes.

Configuring LAN1 and LAN2 settings

Both LAN1 and LAN2 have separate sub-screens to configure the DHCP settings used by the LAN1 and LAN2 interfaces. Within each LAN screen is a button to access a sub-screen to configure advanced DHCP settings for that LAN. For more information, see "Configuring advanced DHCP server settings" on page 122. Additionally, LAN1 and LAN2 each have separate *Type Filter* submenu items used to prevent specific (an potentially unneccesary) frames from being processed, for more information, see "Setting the type filter configuration" on page 124.

To configure unique settings for either LAN1 or LAN2:

1. Select *Network Configuration -> LAN -> LAN1 (or LAN2)* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the *DHCP Configuration* field to define the DHCP settings used for the LAN.

NOTE
When setting the LAN interface to be a DHCP Server and adding an IP address, the primary DNS IP address might not be updated, with only the secondary address getting updated. Ensure the primary address is the same as the IP address of the LAN.

NOTE
Brocade recommends 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 network address information via this LAN1 or LAN2 connection. This is recommended if the Brocade Mobility 7131 Series Access Point resides within a large corporate network or the *Internet Service Provider (ISP)* uses DHCP. This setting is enabled for LAN1 by default. 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 Brocade Mobility 7131 Series Access Point network address information via this LAN1 or LAN2 connection. When selected, only BOOTP responses are accepted by the Brocade Mobility 7131 Series Access Point. 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 Brocade Mobility 7131 Series Access Point can be configured to function as a DHCP server over the LAN1 or LAN2 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. A separate screen exists for each of the LANs.
IP Address	The network-assigned numerical (non DNS name) IP address of the Brocade Mobility 7131 Series Access Point.
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 Brocade Mobility 7131 Series Access Point 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	Brocade 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.
Mesh STP Configuration	Click the *Mesh STP Configuration* button to define bridge settings for this specific LAN. Each of the access point's two LANs can have a separate mesh configuration. As the *Spanning Tree Protocol* (STP) mentions, each mesh network maintains hello, forward delay and max age timers. These settings can be used as is using the current default settings, or be modified. However, if these settings are modified, they need to be configured for the LAN connecting to the mesh network WLAN.

3. Refer to the *IP Filtering* field to optionally enable the IP filtering feature, and (if enabled) apply existing IP filters (and their rules and permissions) to LAN1 or LAN2.

Enable IP Filtering	Selecting this checkbox allows the LAN to employ filter policies and rules to determine which IP packets are processed normally over the LAN and which are discarded. If discarded, a packet is deleted and ignored (as if never received).
IP Filtering	Select the IP Filtering button to display a screen where existing IP filter policies can be applied to the LAN to allow or deny IP packets in either an incoming or outgoing direction based on the rules defined for the policy.

NOTE
For an overview of IP Filtering and how to create a filter, see "Configuring IP filtering" on page 182. For information on applying an existing filter to the IP packet flow of a WLAN, see "Applying a filter to LAN1, LAN2 or a WLAN (1-16)" on page 184.

4. Click *Apply* to save any changes to the LAN1 or LAN2 screen. Navigating away from the screen without clicking the Apply button results in all changes to the screen being lost if the prompts are ignored.
5. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the LAN1 or LAN2 screen to the last saved configuration.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

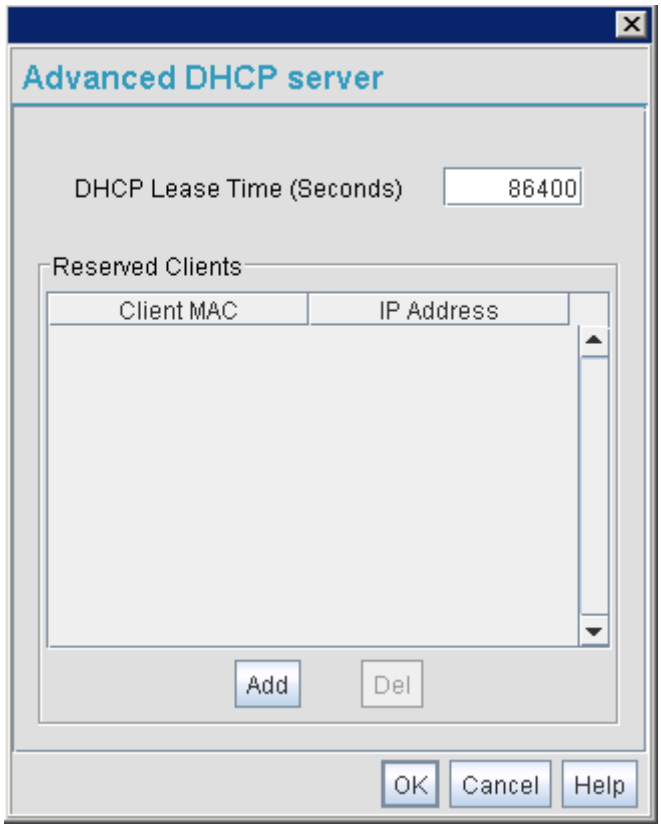
Configuring advanced DHCP server settings

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 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 Client 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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> LAN -> LAN1 (or LAN2)* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Click the *Advanced DHCP Server* button from within the *LAN1* or *LAN2* 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 LAN1 or LAN2 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.

Setting the type filter configuration

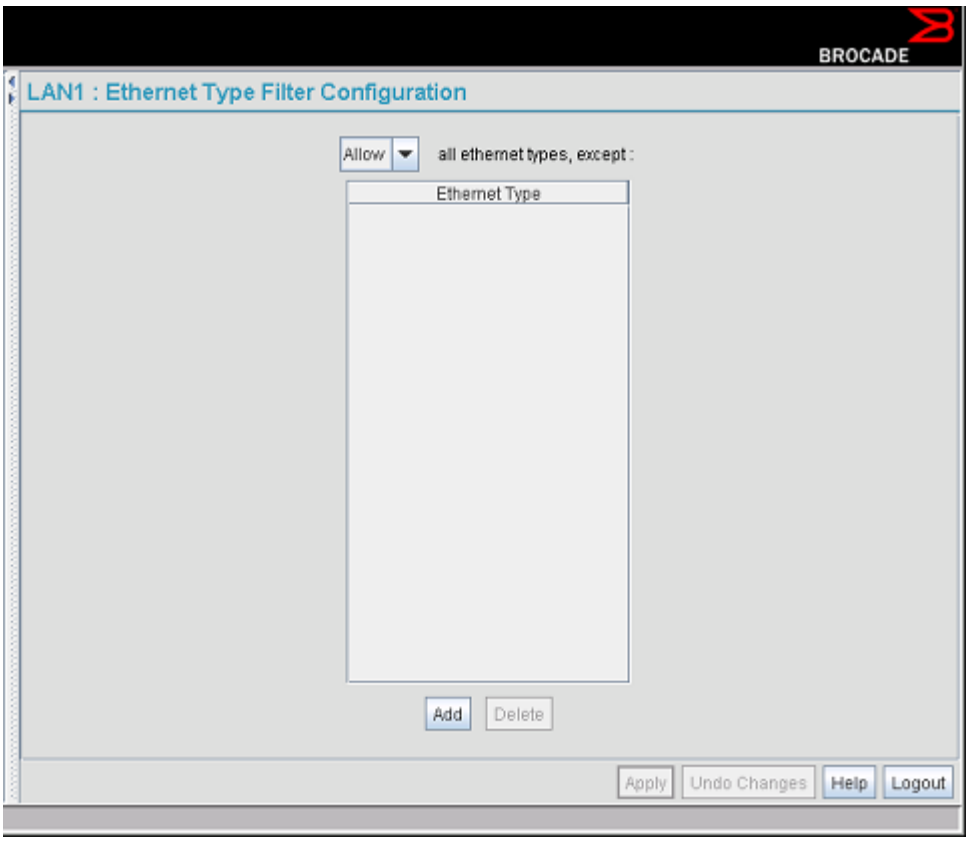
Each Brocade Mobility 7131 Series Access Point LAN (either LAN1 or LAN2) can keep a list of frame types that it forwards or discards. The Type Filtering feature prevents specific (a potentially unneccesary) frames from being processed by the Brocade Mobility 7131 Series Access Point in order to improve throughput. These include certain broadcast frames from devices that consume bandwidth, but are unnecessary to Brocade Mobility 7131 Series Access Point 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 this particular LAN.

To configure type filtering on the Brocade Mobility 7131 Series Access Point:

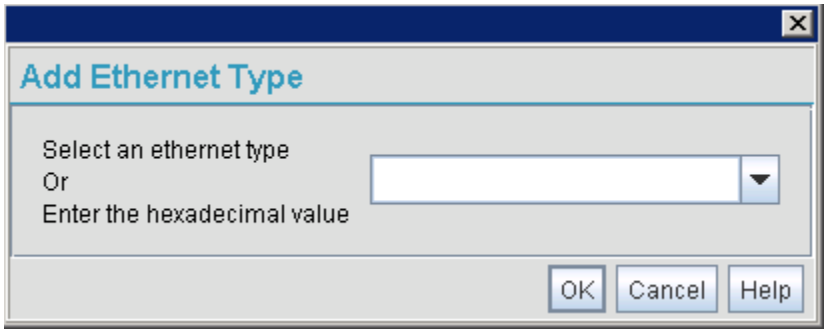
1. Select *Network Configuration-> LAN -> LAN1 (or LAN2)-> Type Filter* from the Brocade Mobility 7131 Series Access Point menu tree.

   The *Ethernet Type Filter Configuration* screen displays for the LAN. 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 for the LAN are allowed or denied for use by the Brocade Mobility 7131 Series Access Point.
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 Brocade proprietary types. Select an Ethernet type from the drop down menu, or enter the Ethernet type's hexadecimal value. See your System Administrator if unsure of the implication of adding or omitting a type from the list for either LAN1 or LAN2.

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 LAN1 or LAN2 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 LAN1 or LAN2 Ethernet Type Filter Configuration screen without saving your changes.
7. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring WAN settings

A *Wide Area Network (WAN)* is a widely dispersed telecommunications network. The Brocade Mobility 7131 Series Access Point includes one WAN port. The Brocade Mobility 7131 Series Access Point 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.

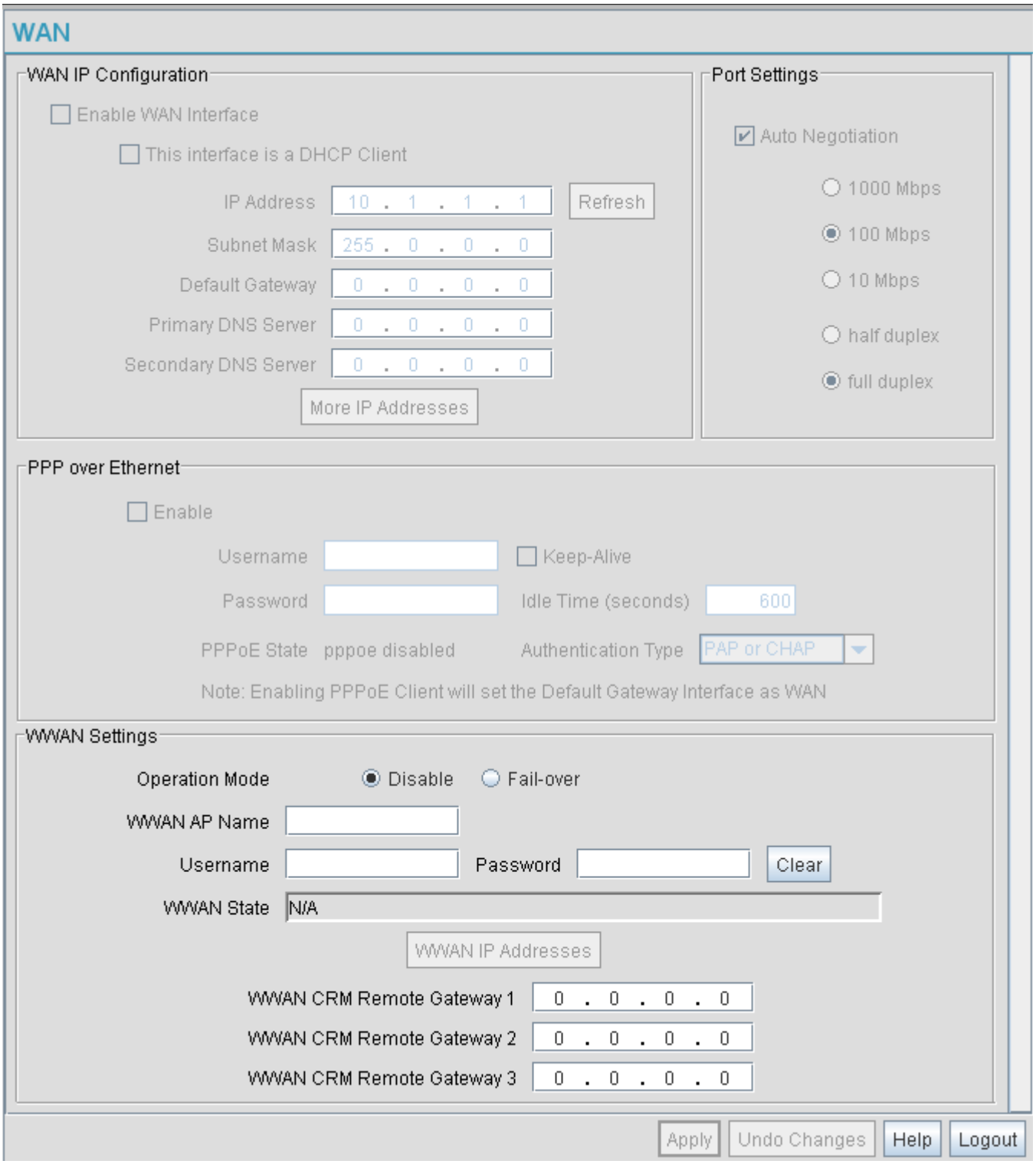
Certain Mobility 7131N SKUs support an express card slot that can provide a secondary link in the event of a wired WAN failure. The Mobility 7131N's wired WAN is the primary WAN link, as long as it's enabled and connected, and the WWAN interface functions as the secondary link.

For the WWAN to be a viable recovery solution, a Brocade Mobility 7131N Access Point must monitor the link status of the wired WAN and check the health of the connection. If the Mobility 7131N detects the loss of the wired WAN connection, it establishes the WWAN connection and updates the default gateway to the WWAN interface. Additionally, the NAT rule is changed dynamically from the wired WAN interface to the wireless WAN interface. All traffic that used go to the wired WAN is redirected to the WWAN. If the Mobility 7131N detects the wired WAN link is restored and up for at least 1 minute, the operation is reversed. The wired WAN becomes the default WAN link once again.

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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN* from the Brocade Mobility 7131 Series Access Point 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
Brocade 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 Brocade Mobility 7131 Series Access Point and a larger network or outside world through the WAN port. Disable this option to effectively isolate the Brocade Mobility 7131 Series Access Point's WAN. No connections to a larger network or the Internet are possible. Clients cannot communicate beyond the LAN. By default, the WAN port is static with an IP address of 10.1.1.1.
This Interface is a DHCP Client	This checkbox enables DHCP for the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point'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 Brocade Mobility 7131 Series Access Point's WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point'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.brocade.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.

More IP Addresses	Click the *More IP Addresses* button to specify additional static IP addresses for the Brocade Mobility 7131 Series Access Point. Additional IP addresses are required when users within the WAN need dedicated IP addresses, or when servers need to be accessed (addressed) by the outside world. The More IP Addresses screen allows the administrator to enter up to seven additional WAN IP addresses for the Brocade Mobility 7131 Series Access Point WAN. Only numeric, non-DNS names can be used. If PPP over Ethernet is enabled from within the WAN screen, the *VPN WAN IP Configuration* portion of the More IP Addresses screen is enabled. Enter the IP address and subnet mask used to provide the PPPoE connection over the access point's WAN port. Ensure the IP address is a numerical (non DNS) name.
Refresh	Click the *Refresh* button to update the network address information displayed within the WAN IP Configuration field.

3. Use the *Port Setting*s field to define how the access point manages throughput over the WAN port.

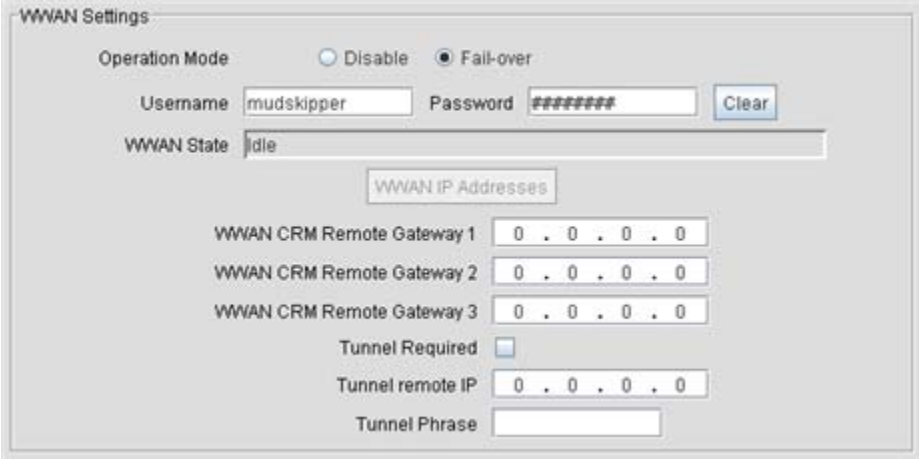
Auto Negotiation	Select the *Auto Negotiation* checkbox to enable the access point to automatically exchange information (over its WAN port) about data transmission speed and duplex capabilities. Auto negotiation is helpful when using the access point in an environment where different devices are connected and disconnected on a regular basis. Selecting Auto Negotiate disables the Mbps and duplex checkbox options.
100 Mbps	Select this option to establish a 100 Mbps data transfer rate for the selected half duplex or full duplex transmission over the access point's WAN port. This option is not available if Auto Negotiation is selected.
10 Mbps	Select this option to establish a 10 Mbps data transfer rate for the selected half duplex or full duplex transmission over the access point's WAN port. This option is not available if Auto Negotiation is selected.
Half Duplex	Select this option to transmit data to and from the access point, but not at the same time. Using a half duplex transmission, the access point can send data over its WAN port then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time.
Full Duplex	Select this option to transmit data to and from the access point at the same time. Using full duplex, the access point can send data over its WAN port while receiving data as well.

4. Configure the *PPP over Ethernet* field to enable high speed dial-up connections to the Brocade Mobility 7131 Series Access Point WAN port.

NOTE
Be aware that the access point can (incorrectly) carry over previously configured static IP information and maintain two connected routes once it gets an IP address from a PPPOE connection.

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.
PPPoE State	Displays the current connection state of the PPPoE client. When a PPPoE connection is established, the status displays *Connected.* When no PPPoE connection is active, the status displays *Disconnected*.
Keep-Alive	Select the *Keep-Alive* checkbox to maintain the WAN connection indefinitely (no timeout interval). Some ISPs terminate inactive connections. Enabling Keep-Alive keeps the Brocade Mobility 7131 Series Access Point's WAN connection active, even when there is no traffic. If the ISP drops the connection after an idle period, the Brocade Mobility 7131 Series Access Point automatically re-establishes the connection to the ISP. Enabling Keep-Alive mode disables (grays out) the *Idle Time* field.
Idle Time (Seconds)	Specify an idle time in seconds to limit how long the Brocade Mobility 7131 Series Access Point's WAN connection remains active after outbound and inbound traffic is not detected. The Idle Time field is grayed out if *Keep-Alive* is enabled.
Authentication Type	Use the *Authentication Type* menu to specify the authentication protocol(s) for the WAN connection. Choices include *None, PAP or CHAP, PAP,* or *CHAP.* *Password Authentication Protocol (PAP)* and *Challenge Handshake Authentication Protocol (CHAP)* are competing identify-verification methods. *PAP* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized. WatchGuard products do not support the PAP protocol because the username and password are sent as clear text that a hacker can read. *CHAP* uses secret information and mathematical algorithms to send a derived numeric value for login. The login server knows the secret information and performs the same mathematical operations to derive a numeric value. If the results match, server access is authorized. After login, one of the numbers in the mathematical operation is changed to secure the connection. This prevents any intruder from trying to copy a valid authentication session and replaying it later to log in.

5. Refer to the *WWAN Setting*s field (located at the bottom of the WAN screen) to enable WWAN failover operation and define user names and passwords for WWAN card users.



The following express cards can be used with a Brocade Mobility 7131N Access Point to support the WAN failover feature:

- Verizon Wireless V740 ExpressCard
- GlobeTrotter Express HSUPA from Options
- Novatel Merlin 870
- Vodafone (Options) E3730 3G Broadband Express Card
- Telstra Turbo 7 Series Express Card (Aircard 880E)

NOTE
Brocade recommends express cards be initially activated on a Windows machine using a SIM card subscribed to an appropriate service plan.

NOTE
Failover from LAN to 3G is also supported.

Operation Mode	Enable WWAN failover by selecting the Fail-over radio button. Disable is selected by default, meaning there's no WWAN card failover to the Mobility 7131N's express card until Fail-over is selected and the Mobility 7131N can read the express card's modules during a boot up runtime operation.
Username	Specify a username entered when connecting to the ISP supporting the express card. When the Internet session begins, the ISP authenticates the username. The username cannot exceed 48 characters.
Password	Specify a password entered when connecting to the ISP supporting the express card. When the Internet session starts, the ISP authenticates the password. The password cannot exceed 40 characters.
WWAN State	Refer to the WWAN State field to discern whether the current Mobility 7131N power budget supports WWAN failover support.
WWAN IP Addresses	Click the *WWAN IP Addresses* button to specify additional static IP addresses for the WWAN. Additional IP addresses are required when users within the WWAN need dedicated IP addresses, or when servers need to be accessed (addressed) by the outside world. Only numeric, non-DNS names can be used.

WWAN CRM Remote Gateway 1	Define a numerical IP address for this first WWAN remote gateway. If the access point detects the loss of the wired WAN connection, it establishes the WWAN connection and uses a remote gateway to route traffic. Traffic that used go to the wired WAN is redirected to the WWAN over this first choice remote gateway.
WWAN CRM Remote Gateway 2	Optionally define a numerical IP address for a second WWAN remote gateway. If the access point detects the loss of the wired WAN connection, it establishes the WWAN connection and uses a remote gateway to route traffic. Traffic that used go to the wired WAN is redirected to the WWAN over this second choice remote gateway, if the first gateway is unavailable.
WWAN CRM Remote Gateway 3	Optionally define a numerical IP address for a third WWAN remote gateway. If the access point detects the loss of the wired WAN connection, it establishes the WWAN connection and uses a remote gateway to route traffic. Traffic that used go to the wired WAN is redirected to the WWAN over this third choice remote gateway, if the first two gateways addresses prove unavailable.
Tunnel Required	Select this option to use a remote tunnel with the access point's WWAN failover operations if the wired WAN connection is lost.
Tunnel Remote IP	If using a tunnel, provide a numerical IP address for the remote tunnel used by the access point's WWAN.
Tunnel Phrase	If using a tunnel, provide a passphrase used to secure the tunnel's connection to the access point's WWAN.

CAUTION

Both the Mobility 7131N's WAN port and express card slot are disabled if the power mode is set to 3af, or if the Mobility 7131N defines its power budget as 3af. Refer to the Power Settings screen (go to "Configuring power settings" on page 67) or check the WWAN State (within the WAN screen) to determine whether the AP has sufficient power for the express card operation.

6. 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.
7. 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.
8. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

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 Brocade Mobility 7131 Series Access Point 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

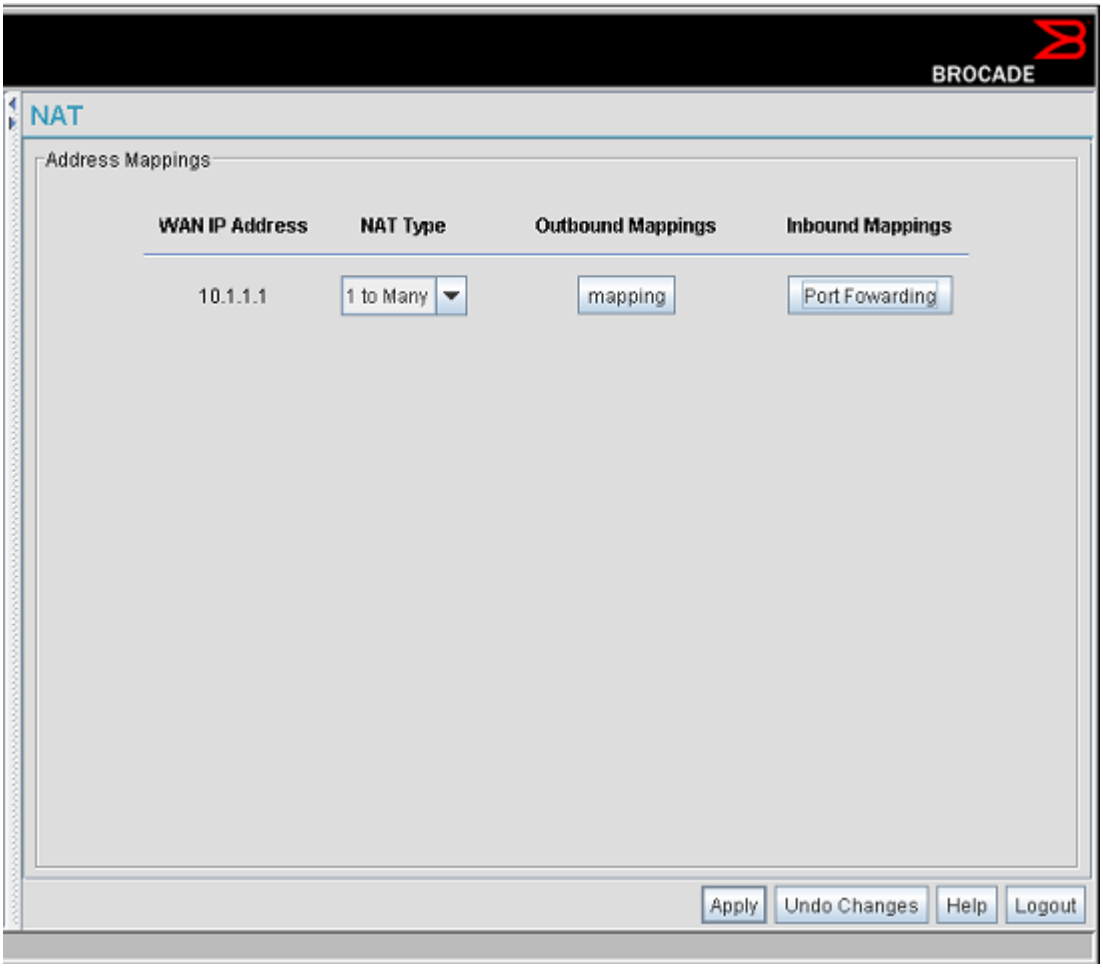
  The private side IP address can belong to any of the private side subnets.

- One-to-many mapping with a configurable range of private side IP addresses

  Ranges can be specified from each of the private side subnets.

To configure IP address mappings for the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> NAT* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the *Address Mappings* 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 Brocade Mobility 7131 Series Access Point. Set the NAT Type as *1 to Many* to map a WAN IP address to multiple local IP addresses. This displays the *mapping*s 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.
Outbound Mappings	When *1 to 1* NAT is selected, a single IP address can be entered in the *Outbound Mapping*s area. This address provides a 1 to 1 mapping of the WAN IP address to the specified IP address. When *1 to Many* is selected as the NAT Type, the Outbound Mappings area displays a *1 to Many Mapping*s button. Click the button to select the LAN1 or LAN2 IP address used to set the outbound IP address or select *none* to exclude the IP address. If *none* is selected as the NAT Type, The Outbound Mappings area is blank.
Inbound Mappings	When *1 to 1* or *1 to Many* is selected, the *Inbound Mapping*s option displays a *Port Forwarding* button.
Port Forwarding	Click the *Port Forwarding* button to display a screen of port forwarding parameters for inbound traffic from the associated WAN IP address.

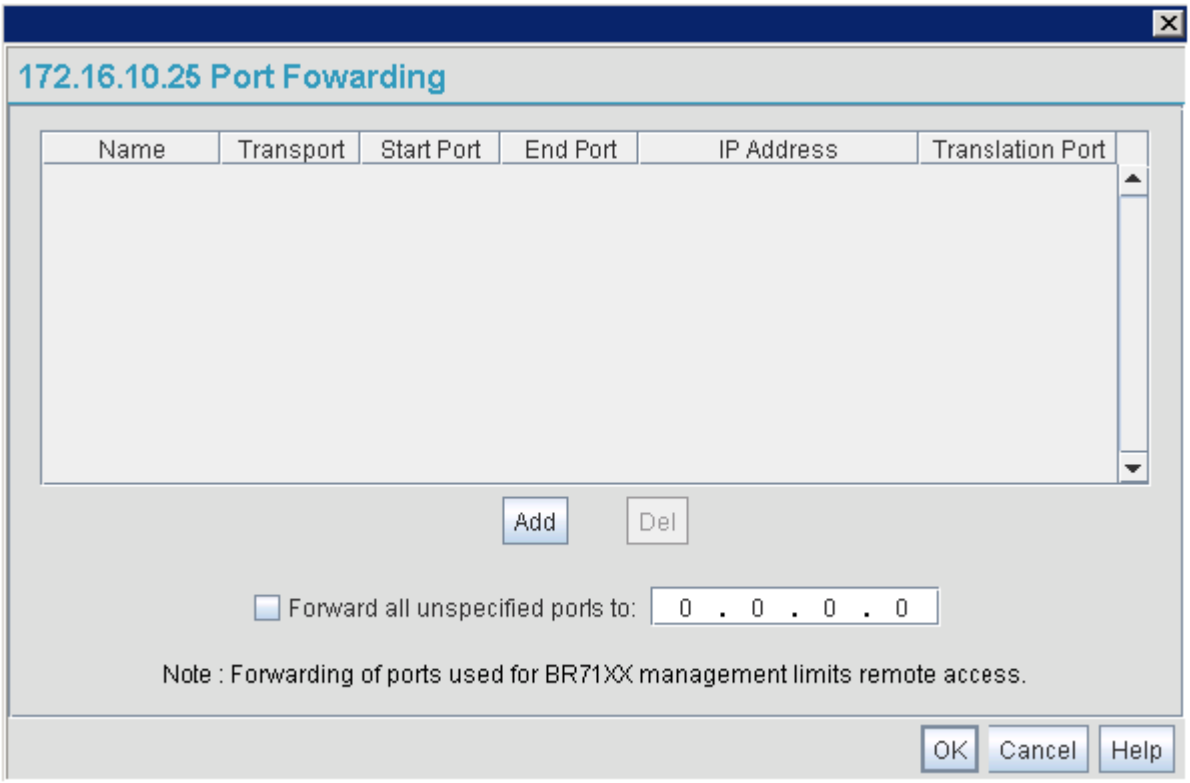
3. Click *Apply* to save any changes to the NAT screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.
4. Click *Undo Change*s (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the NAT screen to the last saved configuration.
5. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> NAT* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Select *1 to 1* or *1 to Many* from the NAT Type drop-down menu.
3. Click on the *Port Forwarding* button within the *Inbound Mapping*s area.



4. 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, IP address and Translation Port 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.
Forward all Unspecified Ports to	Use the *Forward all unspecified ports to* checkbox to enable port forwarding for incoming packets with unspecified ports. In the adjacent area, enter a target forwarding IP address for incoming packets. This number must be within the specified NAT range for the associated WAN IP address.

5. Click *OK* to return to the NAT screen. Within the NAT screen, click *Apply* to save any changes made on the Port Forwarding screen.
6. 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.

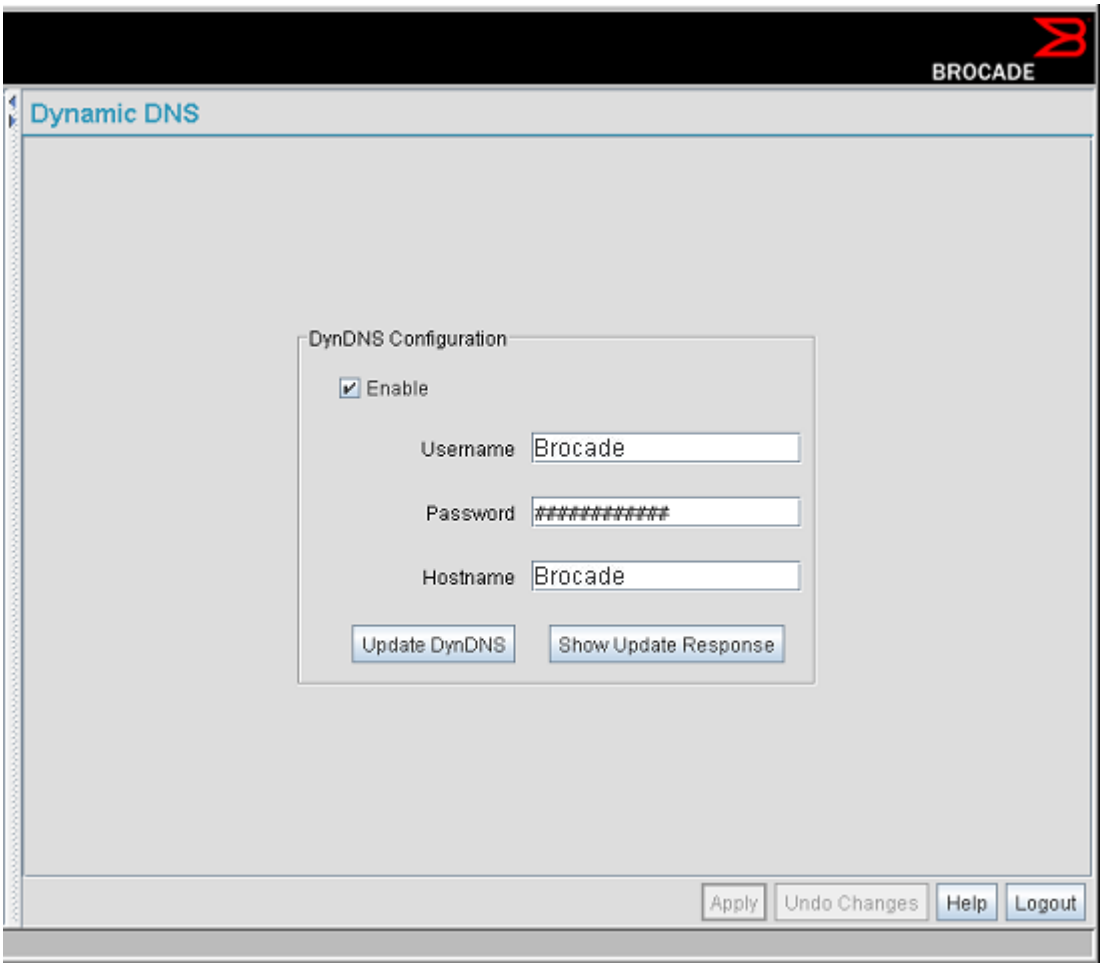
Configuring Dynamic DNS

The access point supports the Dynamic DNS service. *Dynamic DNS* (or DynDNS) is a feature offered by *www.dyndns.com* which allows the mapping of domain names to dynamically assigned IP addresses via the WAN port. When the dynamically assigned IP address of a client changes, the new IP address is sent to the DynDNS service and traffic for the specified domain(s) is routed to the new IP address.

NOTE
DynDNS supports only the primary WAN IP address.

To configure dynamic DNS for the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> DynDNS* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Select the *Enable* checkbox to allow domain name information to be updated when the IP address associated with that domain changes.

   A username, password and hostname must be specified for domain name information to be updated.

NOTE
The username, password and hostname are required to be registered at *http://www.dyndns.com*.

3. Enter the DynDNS *Username* for the account you wish to use for the access point.
4. Enter the DynDNS *Password* for the account you wish to use for the access point.
5. Provide the *Hostname* for the DynDNS account you wish to use for the access point.
6. Click the *Update DynDNS* button to update the access point's current WAN IP address with the DynDNS service.

NOTE
DynDNS supports devices directly connected to the Internet. Having VPN enabled, and the DynDNS Server on the other side of the VPN is not supported.

7. Once the DynDNS configuration has been updated, click the *Show Update Response* button to open a sub-screen displaying the hostname, IP address and any messages received during an update from the DynDNS Server.
8. Click *Apply* to save any changes to the Dynamic DNS screen. Navigating away from the screen without clicking the Apply button results in all changes to the screens being lost.
9. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the screen to the last saved configuration.

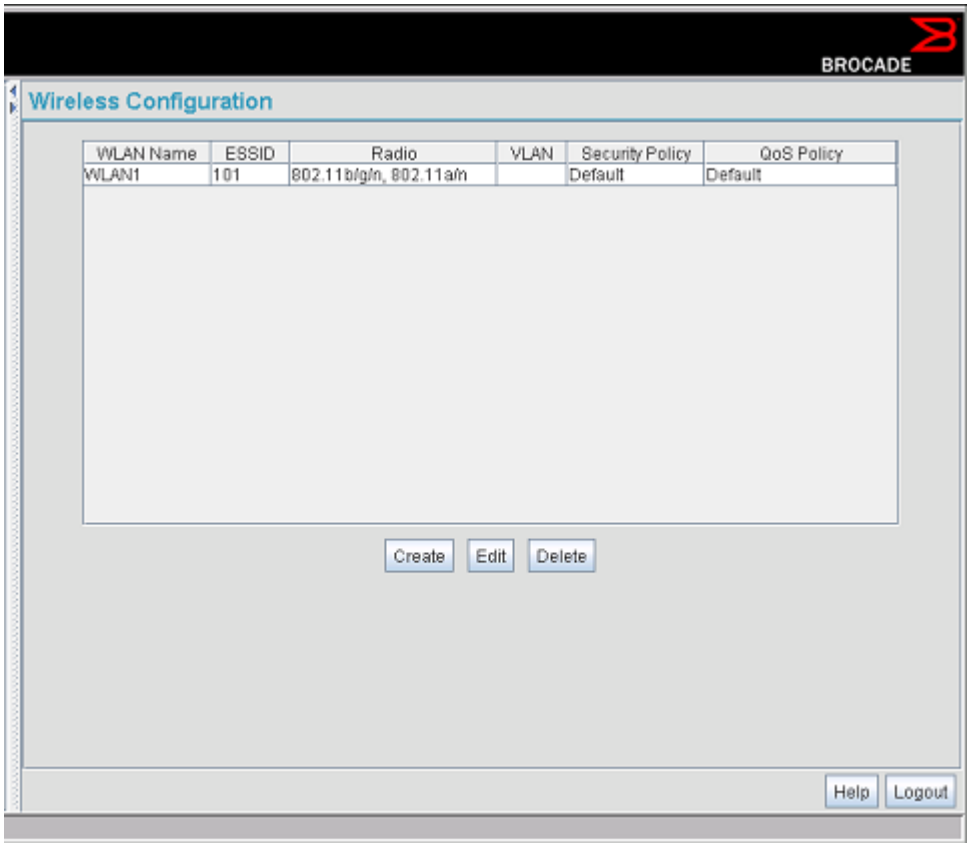
Enabling wireless LANs (WLANs)

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 Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point'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 access point (regardless of single or dual-radio model).

To configure WLANs on the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless* from the Brocade Mobility 7131 Series Access Point menu tree.



If a WLAN is defined, that WLAN displays within the *Wireless Configuration* screen. When the Brocade Mobility 7131 Series Access Point 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, Brocade Mobility 7131 Series Access Point 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.
ESSID	Displays the *Extended Services Set Identification (ESSID)* associated with each WLAN. The ESSID can be modified within individual WLAN configuration screens.
Radio	The *Radio* field displays the name of the Brocade Mobility 7131 Series Access Point radio the WLAN is mapped to (either the 802.11a/n radio or the 802.11b/g/n radio).
VLAN	The *VLAN* field displays the specific VLAN the target WLAN is mapped to.

Security Policy	The *Security Policy* field displays the security profile configured for the target WLAN.
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.

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 139.
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 139.
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 Brocade Mobility 7131 Series Access Point.
6. Refer to the *Proxy-ARP Disable* field to enable/disable Proxy AP support. Proxy ARP is disabled by default.

   When enabled, any system on the wireless network that ARPs for the IP address of an associated client receives an ARP reply from the access point stating the requesting system should be sending packets destined for the client to access point instead. In turn, the access point forwards the requesting packets to the target client. Through this process, the access point can pass ARP requests in both directions, making an client appear to be connected to a public network even though it's on a private network, hidden behind the access point.

   Select the following options as required:

   a. Select *Dynamic* for the access point to respond to an ARP request for its client IP addresses using an ARP response and drop the original ARP request packet.

   b. Select *Strict* for the access point to respond to ARP request for its client IP addresses using an ARP response and drop the original ARP request packet (like the dynamic option). However, with the strict option, the access point will drop the ARP request to wireless (WLAN interfaces not the mesh interface) if the ARP request is for the IP address of non-clients or if gratuitous ARP requests are coming from the client. This helps reduce unnecessary ARP traffic and improve throughput within the access point managed wireless network.
7. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

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.

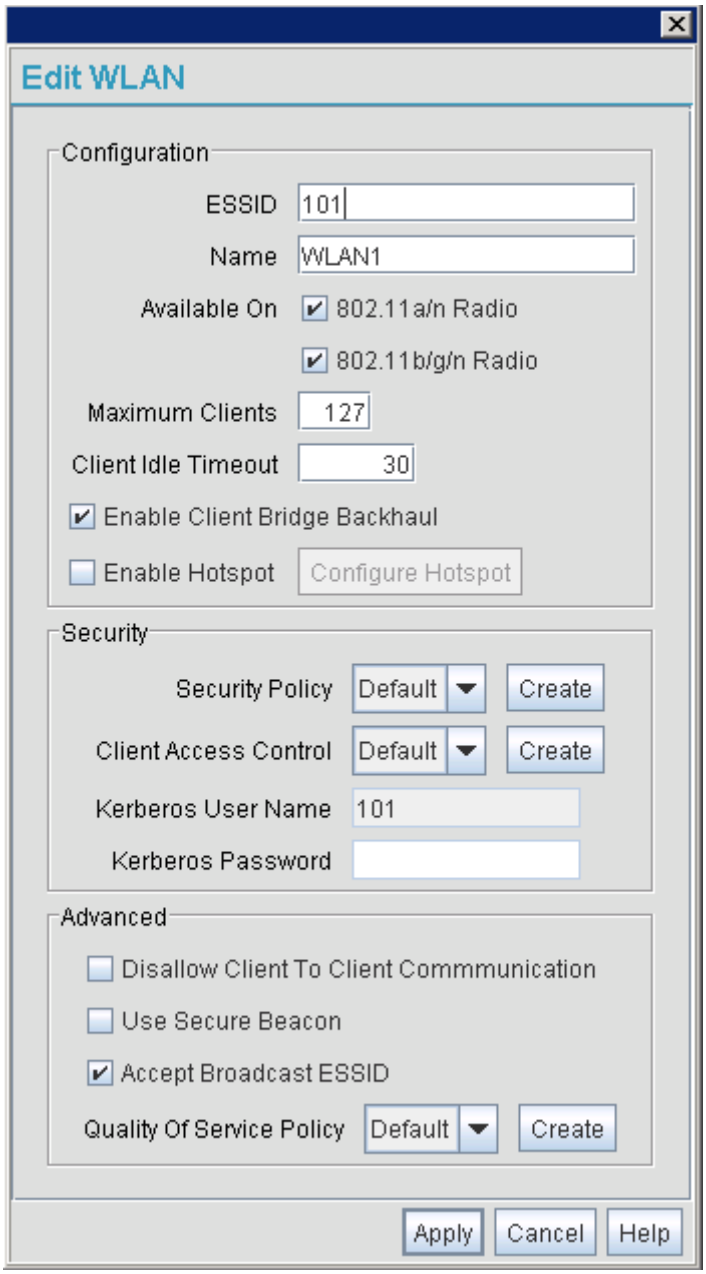
NOTE
Before editing the properties of an existing WLAN, ensure it is not being used by a Brocade Mobility 7131 Series Access Point radio, or is a WLAN that is needed in its current configuration. Once updated, the previous configuration is not available unless saved.

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 Brocade Mobility 7131 Series Access Point 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. Do not use any of the following characters for an ESSID < > | " & \ ? ,
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 whether the WLAN you are creating or editing is available to clients on either the 802.11a/n or 802.11b/g/n radio (or both radios). The Available On checkbox should only be selected for a mesh WLAN if this target access point is to be configured as a base bridge or repeater (base and client bridge) on the radio. If the radio for the WLAN is to be defined as a client bridge only, the Available On checkbox should not be selected.
Max Clients	Use the *Max Clients* field to define the number of clients permitted to interoperate within the new or revised WLAN. The maximum (and default) is 127. However, each access point can only support a maximum 127 clients spanned across its 16 available WLANs. If you intend to define numerous WLANs, ensure each is using a portion of the 127 available clients and the sum of the supported clients across all WLANs does not exceed 127.
Client Idle Timeout	Set an *Client Idle Timeout* the access point uses to timeout idle wireless clients from WLAN inclusion. When exceeded, the Client must re-establish its credentials to assume operation within the WLAN. Set a value between 1 - 65535 minutes. the default value is 30 minutes.
Enable Client Bridge Backhaul	Select the Enable *Client Bridge Backhaul* checkbox to make the WLAN available in the *WLAN* drop-down menu within the *Radio Configuration* screen. This checkbox can be ignored for WLANs not supporting mesh networking, to purposely exclude them from the list of WLANs available in the Radio Configuration page selected specifically for mesh networking support. Only WLANs defined for mesh networking support should have this checkbox selected.
Enable Hotspot	Select the Enable Hotspot checkbox to allow this WLAN (whether it be a new or existing WLAN) to be configured for hotspot support. Clicking the Configure Hotspot button launches a screen wherein the parameters of the hotspot can be defined.For information on configuring a target WLAN for hotspot support, see "Configuring WLAN hotspot support" on page 152. For an overview of what a hotspot is and what it can provide your wireless network, see "Hotspot support" on page 20.

CAUTION

A WLAN cannot be enabled for both mesh and hotspot support at the same time. Only one of these two options can be enabled at one time, as the GUI and CLI will prevent both from being enabled.

NOTE
If 802.11a/n 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.

NOTE
A WLAN configured to support Mesh should not have a Kerberos or 802.1x EAP security policy defined for it, as these two authentication schemes are not supported within a Mesh network.

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.
Client Access Control	Select an ACL policy suiting the WLAN's Client intropera bility 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.
Kerberos User Name	Displays the read-only Kerboros User Name used to associate the wireless client. This value is the ESSID of the access point.
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.

5. Configure the *Advanced* field as required to set Client interoperability permissions, secure beacon transmissions, broadcast ESSID acceptance and *Quality of Service (QoS)* policies.

Disallow Client to Client Communication	The Client-Client Disallow feature prohibits clients from communicating with each other even if they are on different WLANs, assuming one of the WLAN's is configured to disallow Client-Client communication. Therefore, if an Client's WLAN is configured for Client-Client disallow, it will not be able to communicate with any other clients connected to this access point.
Use Secure Beacon	Select the *Use Secure Beacon* checkbox to not transmit the access point's ESSID. If a hacker tries to find an ESSID via an Client, the ESSID does not display since the ESSID is not in the beacon. Brocade recommends keeping the option enabled to reduce the likelihood of hacking into the WLAN.
Accept Broadcast ESSID	Select the *Accept Broadcast ESSID* checkbox to associate an Client that has a blank ESSID (regardless of which ESSID the access point is currently using). Sites with heightened security requirements may want to leave the checkbox unselected and configure each Client with an ESSID. The default is unselected, thus not allowing the acceptance of broadcast ESSIDs.
Quality of Service Policy	If QoS policies are undefined (none), select the *Create* button to launch the *New QoS Policy* 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 Client transmissions within that WLAN.

CAUTION

When using the access point's hotspot functionality, ensure clients are re-authenticated when changes are made to the characteristics of a hotspot enabled WLAN, as clients within the WLAN will be dropped from device association.

6. Refer to the *IP Filtering* field to optionally enable the IP filtering feature, and (if enabled) apply existing IP filters (and their rules and permissions) to the WLAN.

Enable IP Filtering	Selecting this checkbox allows the WLAN to employ filter policies and rules to determine which IP packets are processed normally over the WLAN and which are discarded. If discarded, a packet is deleted and ignored (as if never received).
IP Filtering	Select the IP Filtering button to display a screen where existing IP filter policies can be applied to the WLAN to allow or deny IP packets in either an incoming or outgoing direction based on the rules defined for the policy.

NOTE

For an overview of IP Filtering and how to create a filter, see "Configuring IP filtering" on page 182. For information on applying an existing filter to the IP packet flow of a WLAN, see "Applying a filter to LAN1, LAN2 or a WLAN (1-16)" on page 184.

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

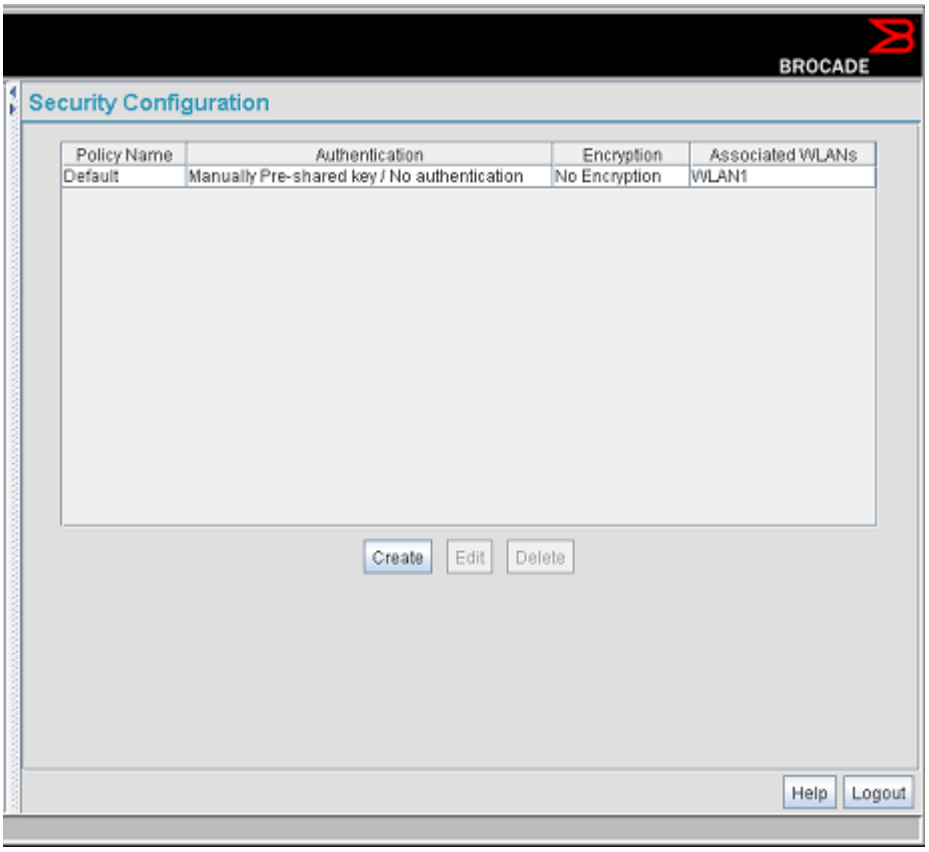
Configuring WLAN security policies

As WLANs are being defined for a Brocade Mobility 7131 Series Access Point, 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:

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point menu tree.

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



NOTE
When the Brocade Mobility 7131 Series Access Point 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 . See "Configuring Access Point Security" on page 191 for more details on configuring Brocade Mobility 7131 Series Access Point security.

For detailed information on the authentication and encryption options available to the Brocade Mobility 7131 Series Access Point and how to configure them, see to "Configuring security options" on page 192 and locate the section that describes your intended security scheme.

2. Click *Logout* to exit the Security Configuration screen.

Configuring a WLAN Access Control List (ACL)

An *Access Control List (ACL)* affords a system administrator the ability to grant or restrict Client access by specifying a Client MAC address or range of MAC addresses to either include or exclude from Brocade Mobility 7131 Series Access Point connectivity. Use the *Client Access Control List Configuration* screen to create new ACL policies (using the *New Client ACL Policy* sub-screen) or edit existing policies (using the *Edit Client 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 Client interoperability requirements.

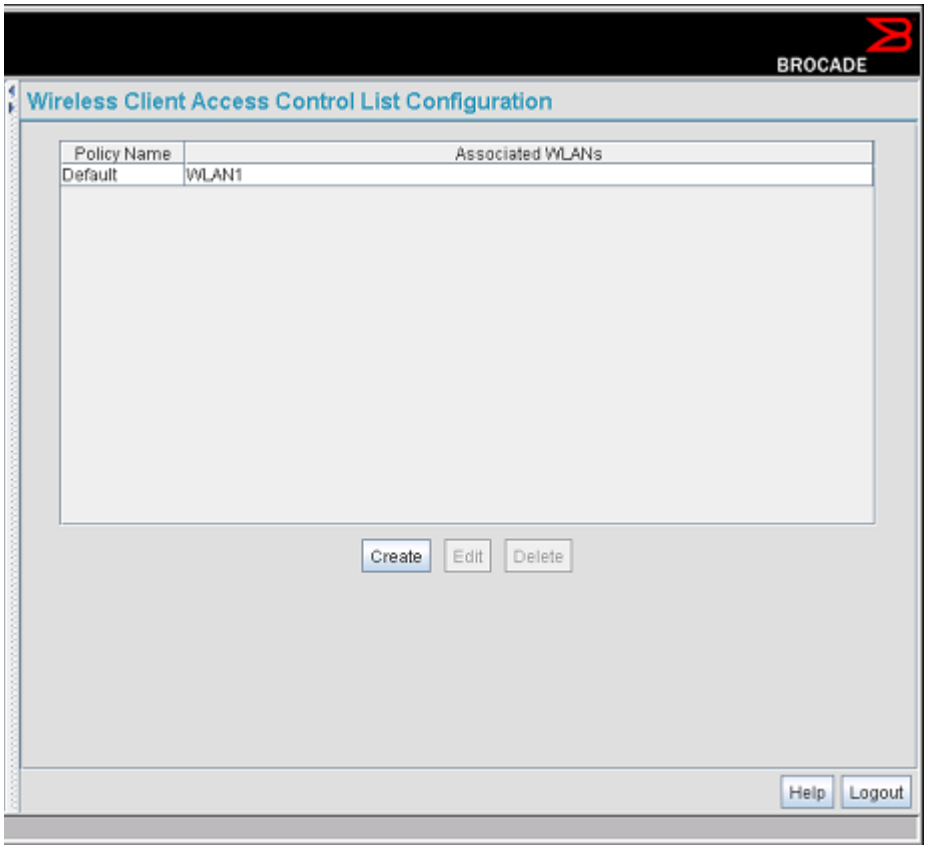
Brocade recommends using the New Client ACL Policy or Edit Client ACL Policy screens strategically to name and configure ACL policies meeting the requirements of the particular WLANs they may map to. However, be careful not to name policies after specific WLANs, as individual ACL policies can be used by more than one WLAN. For detailed information on assigning ACL policies to specific WLANs, see "Creating/editing individual WLANs" on page 139.

To create or edit ACL policies for WLANs:

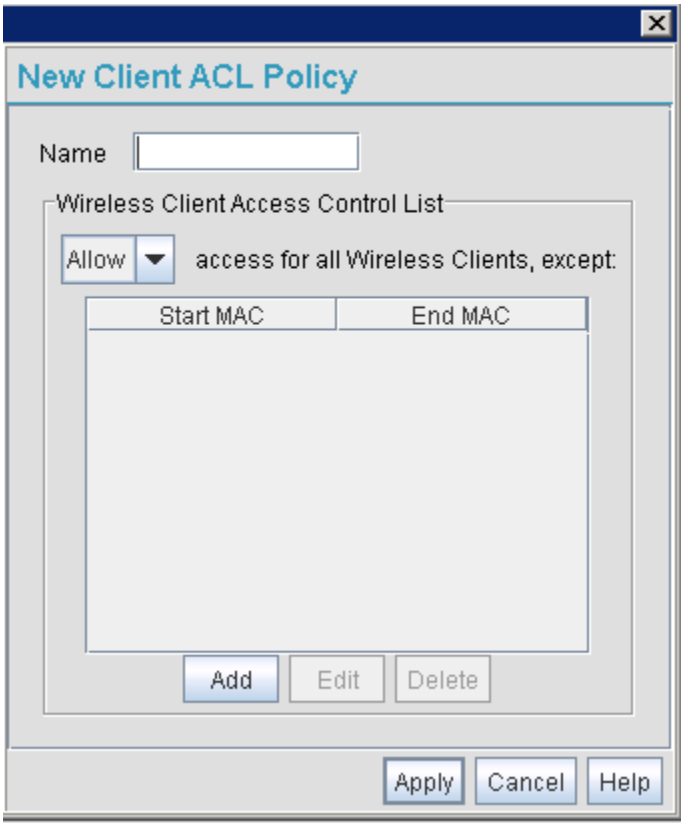
1. Select *Network Configuration -> Wireless -> Client ACL* from the Brocade Mobility 7131 Series Access Point menu tree.

   The *Client Access Control List Configuration* screen displays with existing ACL policies and their current WLAN (if mapped to a WLAN).

NOTE
When the Brocade Mobility 7131 Series Access Point 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 access point supports a maximum of 16 Client ACL policies.



Either the *New Client ACL Policy* or *Edit Client 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 Client 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 *Client Access Control List* field to allow or deny Client access to the Brocade Mobility 7131 Series Access Point.

   The Client adoption list identifies clients by their MAC address. The MAC address is the Client'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 Client MAC addresses can be added to the New/Edit Client ACL Policy screen.

Access for the Listed Wireless Clients	Use the drop-down list to select *Allow* or *Deny.* This rule applies to the clients listed in the table. For example, if the adoption rule is to Allow, access is granted for all clients except those listed in the table.
Add	Click the *Add* button to create a new entry using only the *Start MAC* column to specify a MAC address, or uses both the *Start MAC* and *End MAC* columns to specify a range of MAC addresses.
Delete	Click the *Delete* button to remove a selected list entry.

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

6. Click *Cancel* to securely exit the New Client ACL Policy or Edit Client ACL Policy screen and return to the Client Access Control List Configuration screen.
7. Click *Logout* within the Client Access Control List Configuration screen to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Setting the WLAN Quality of Service (QoS) policy

The Brocade Mobility 7131 Series Access Point 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 Client interoperability requirements.

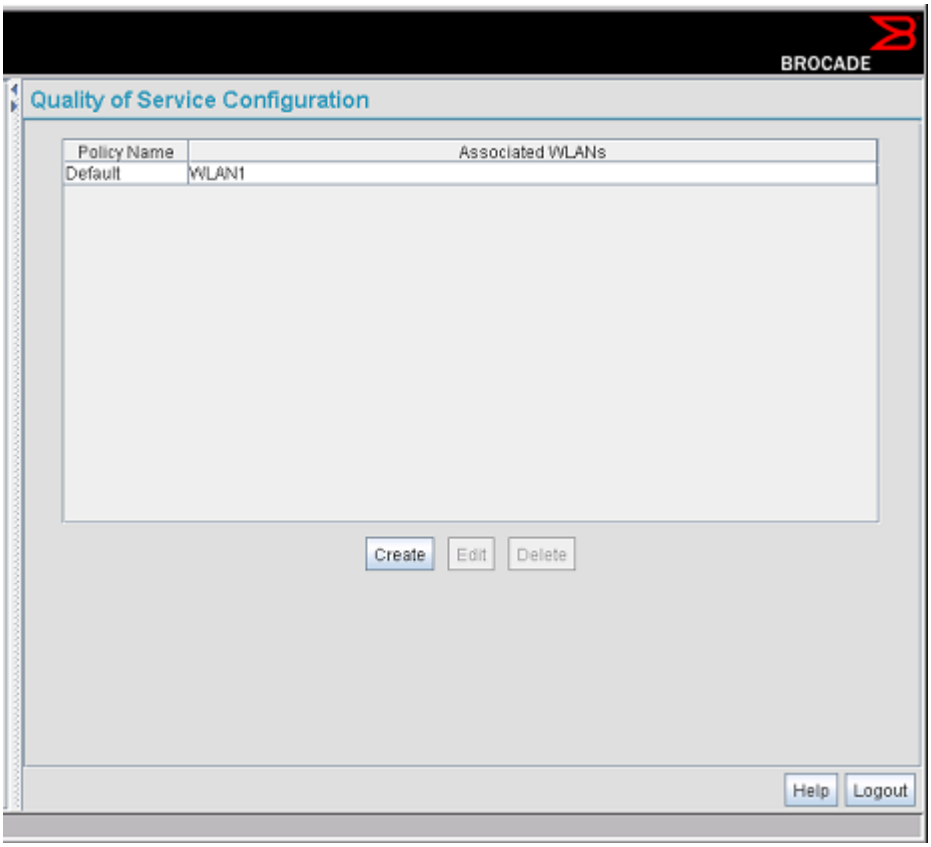
Brocade recommends using the New QoS Policy and Edit QoS Policy screens strategically to name and configure QoS policies meeting the requirements of the particular WLANs they may to. However, be careful not to name policies after specific WLANs, as individual QoS policies can be used by more than one WLAN. For detailed information on assigning QoS policies to specific WLANs, see "Creating/editing individual WLANs" on page 139.

To configure QoS policies:

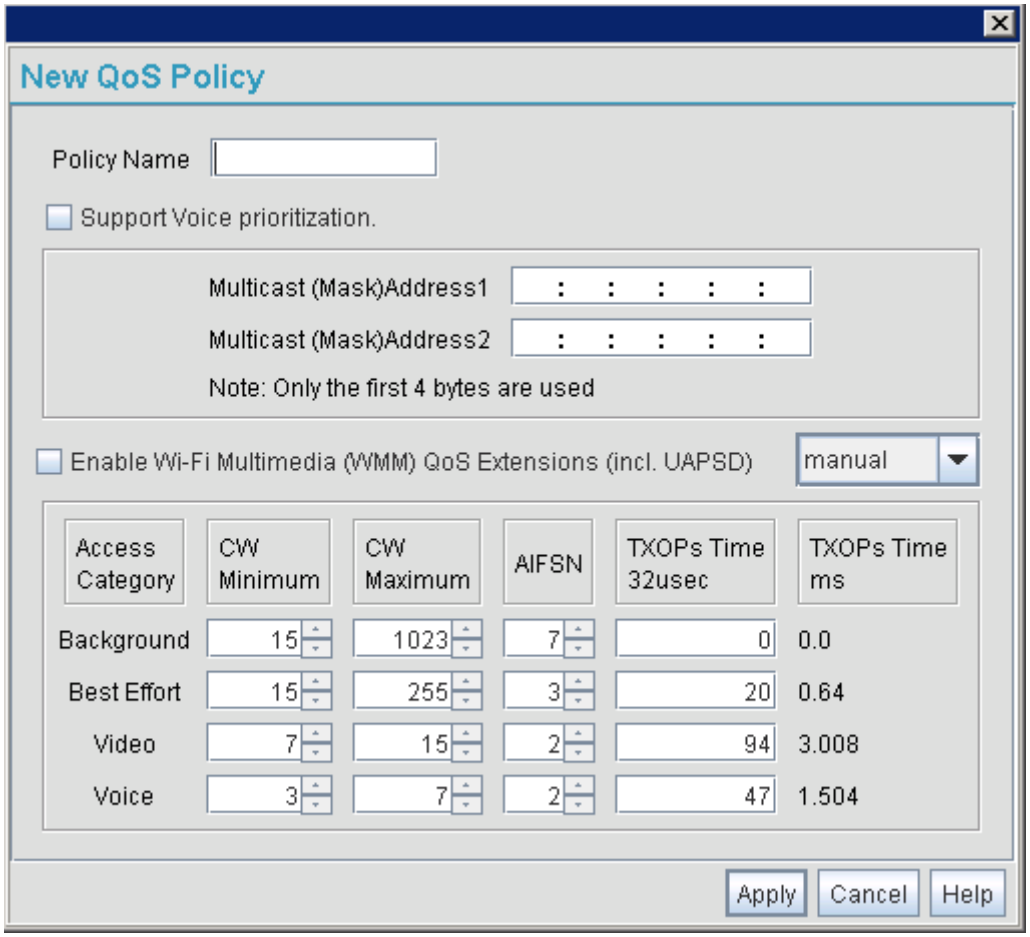
1. Select *Network Configuration -> Wireless -> QoS* from the Brocade Mobility 7131 Series Access Point menu tree.

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

NOTE
When the Brocade Mobility 7131 Series Access Point 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 access point supports a maximum of 16 QoS policies.



3. Assign a name to the new or edited QoS policy that makes sense to the Brocade Mobility 7131 Series Access Point 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 access point will detect non-WMM capable (legacy) phones that connect to the access point and provide priority queueing for their traffic over normal data.

NOTE
Wi-fi functionality requires both the access point and its associated clients are WMM-capable and have WMM enabled. WMM enabled devices can take advantage of their QoS functionality only if using applications that support WMM, and can assign an appropriate priority level to the traffic streams they generate.

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. Use the drop-down menu to select the radio traffic best representing the network requirements of this WLAN. Options include:

manual	Select the *manual* option if intending to manually set the Access Categories for the radio traffic within this WLAN. Only advanced users should manually configure the Access Categories, as setting them inappropriately could negatively impact the access point's performance.
11ag - wifi	Use this setting for high-end multimedia devices that using the high rate 802.11a or 802.11g radio.
11b - wifi	Use this setting for high-end devices multimedia devices that use the 802.11b radio.
11ag - Default	Use this setting for typical "data-centric" Client traffic over the high rate 802.11a or 802.11g radio.
11b - Default	Use this setting for typical "data-centric" Client traffic over the 802.11b radio.
11ag Voice	Use this setting for "Voice-Over-IP" traffic over the high rate 802.11a or 802.11g radio.
11b Voice	Use this setting for "Voice-Over-IP" traffic over the 802.11b radio.

CAUTION

Brocade recommends using the drop-down menu to define the intended radio traffic within the WLAN. Once an option is selected, you do not need to adjust the values for the Access Categories, unless qualified to do so. Changing the Access Category default values could negatively impact the performance of the access point.

7. Select the *Enable Wi-Fi Multimedia (WMM) QoS Extensions* checkbox to configure the Brocade Mobility 7131 Series Access Point'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 ect.). 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.

8. 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 as follows.

CW Min	The contention window minimum value is the least amount of time the Client 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.
CW Max	The contention window maximum value is the maximum amount of time the Client waits before transmitting when there is no other data traffic on the network. The longer the interval, the lesser likelihood of collision, but the greater propensity for longer transmit periods.
AIFSN	The AIFSN is the minimum interframe space between data packets transmitted for the selected Access Category. This value should be set to a smaller increment for higher priority traffic to reduce packet delay time.
TXOPs Time 32usec	The *TXOPs Time* is the interval the transmitting Client is assigned for transmitting. The default for Background traffic is 0. The same TXOPs values should be used for either the 802.11a/n or 802.11b/g/n radio, there is no difference.
TXOPs Time ms	TXOP times range from 0.2 ms (background priority) to 3 ms (video priority) in a 802.11a/n network, and from 1.2 ms to 6 ms in an 802.11b/g/n network. The TXOP bursting capability greatly enhances the efficiency for high rate traffic such as streaming video.

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

U-APSD (WMM Power Save) Support

The access point now supports *Unscheduled Automatic Power Save Delivery* (U-APSD), often referred to as WMM Power Save. U-APSD provides a periodic frame exchange between a voice capable Client and the access point during a VoIP call, while legacy power management is still utilized for typical data frame exchanges. The access point and its associated Client activate the new U-APSD power save approach when a VoIP traffic stream is detected. The Client then buffers frames from the voice traffic stream and sends a VoIP frame with an implicit "poll" request to its associated access point. The access point responds to the poll request with buffered VoIP stream frame(s). When a voice-enabled Client wakes up at a designated VoIP frame interval, it sends a VoIP frame with an implicit "poll" request to its associated access point. The access point responds to the poll request with buffered VoIP stream frame(s).

NOTE
The access point ships with the U-APSD feature disabled by default. It is automatically enabled when WMM is enabled for a WLAN. Thus, U-APSD is only functional when WMM is enabled. If WMM is disabled, then
U-APSD is disabled as well.

Configuring WLAN hotspot support

The access point enables hotspot operators to provide user authentication and accounting without a special client application. The access point uses a traditional Internet browser as a secure authentication device. Rather than rely on built-in 802.11security features to control access point association privileges, configure a WLAN with no WEP (an open network). The access point issues an IP address to the user using a DHCP server, authenticates the user and grants the user to access the Internet.

When a user visits a public hotspot and wants to browse to a Web page, they boot up their laptop and associate with the local Wi-Fi network by entering the correct SSID. They then start a browser. The hotspot access controller forces this un-authenticated user to a Welcome page from the hotspot Operator that allows the user to login with a username and password.

NOTE
Beginning with this most recent 4.1 release of the access point firmware, users now have the ability to customize the appearance of an access point's hotspot pages. The access point's hotspot feature is supported by three customer accessible pages (login page, welcome page and failure page) displayed on the client attempting to access the AP's supported hotspot. These three pages can be unique to each hotspot supported by one of the access point's 16 WLANs. For more information, see "Customizing a hotspot display" on page 156.

The access point hotspot functionality requires the following:

- *HTTP Redirection* - Redirects unauthenticated users to a specific page specified by the Hotspot provider.
- *User authentication* - Authenticates users using a Radius server.
- *Walled garden support* - Enables a list of IP address (not domain names) accessed without authentication.
- *Billing system integration* - Sends accounting records to a Radius accounting server.

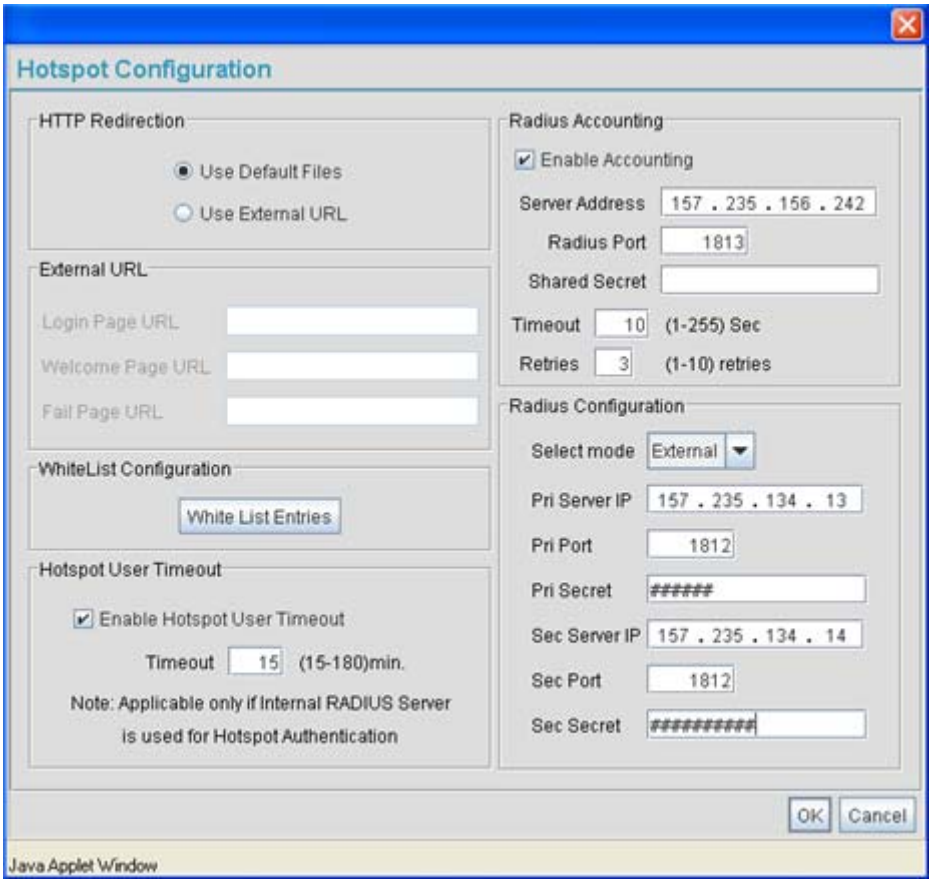
CAUTION
When using the access point's hotspot functionality, ensure clients are re-authenticated when changes are made to the characteristics of a hotspot enabled WLAN, as clients within the WLAN will be dropped from access point device association.

To configure hotspot functionality for an access point WLAN:

1. Ensure the *Enable Hotspot* checkbox is selected from within the target WLAN screen, and ensure the WLAN is properly configured.

   Any of the sixteen WLANs on the access point can be configured as a hotspot. For hotspot enabled WLANs, DHCP, DNS, HTTP and HTTPS traffic is allowed (before you login to the hotspot), while TCP/IP packets are redirected to the port on the subnet to which the WLAN is mapped. For WLANs not hotspot-enabled, all packets are allowed.

2. Click the *Configure Hotspot* button within the WLAN screen to display the *Hotspot Configuration* screen for that target WLAN.



3. Refer to the *HTTP Redirection* field to specify how the Login, Welcome, and Fail pages are maintained for this specific WLAN. The pages can be hosted locally or remotely.

Use Default Files	Select the *Use Default Files* checkbox if the login, welcome and fail pages reside on the access point.
Use External URL	Select the *Use External URL* checkbox to define a set of external URLs for hotspot users to access the login, welcome and fail pages. To create a redirected page, you need to have a TCP termination locally. On receiving the user credentials from the login page, the access point connects to a radius server, determines the identity of the connected wireless user and allows the user to access the Internet based on successful authentication.

4. Use the *External URL* field to specify the location of the login page, welcome page and fail page used for hotspot access. Defining these settings is required when the *Use External URL* checkbox has been selected within the HTTP Redirection field

NOTE
If an external URL is used, the external Web pages are required to forward user credentials to the access point, which in turn forwards them to the authentication Server (either onboard or external server) in order to grant users Web access.

Login Page URL	Define the complete URL for the location of the Login page. The Login screen will prompt the hotspot user for a username and password to access the Welcome page.
Welcome Page URL	Define the complete URL for the location of the Welcome page. The Welcome page asserts the hotspot user has logged in successfully and can access the Internet.
Fail Page URL	Define the complete URL for the location of the Fail page. The Fail screen asserts the hotspot authentication attempt failed, you are not allowed to access the Internet and you need to provide correct login information to access the Internet.

5. Select the *Enable Hotspot User Timeout* checkbox to define a timeout interval forcing users (when exceeded) to re-establish their login credentials to continue using the access point supported hotspot.

   Leaving the checkbox unselected is not recommended unless you plan to provide unlimited hotspot support to users.

   If this option is selected, enter an interval (between 15 and 180 minutes). When the provided interval is exceeded, the user is logged out of their hotspot session and forced to login to the hotspot again to access to the hotspot supported WLAN. The default timeout interval is 15 minutes.

   NOTE
   The Enable Hotspot User Timeout option is only available if using the access point's internal Radius Server for user authentication.

6. Click the *White List Entries* button (within the *WhiteList Configuration* field) to create a set of allowed destination IP addresses. These allowed destination IP addresses are called a White List. Ten configurable IP addresses are allowed for each WLAN. For more information, see "Defining the hotspot White List" on page 155.

   NOTE
   If using an external Web Server over the WAN port, and the hotspot's HTTP pages (login or welcome) redirect to the access point's WAN IP address for CGI scripts, the IP address of the external Web server and the access point's WAN IP address should be entered in the White List.

7. Refer to the *Radius Accounting* field to enable Radius accounting and specify the a timeout and retry value for the Radius server.

Enable Accounting	Select the *Enable Accounting* checkbox to enable a Radius Accounting Server used for Radius authentication for a target hotspot user.
Server Address	Specify an IP address for the external Radius Accounting server used to provide Radius accounting for the hotspot. If using this option, an internal Radius server cannot be used. The IP address of the internal Radius server is fixed at 127.0.0.1 and cannot be used for the external Radius server.
Radius Port	Specify the port on which the Radius accounting server is listening.
Shared Secret	Specify a shared secret for accounting authentication for the hotspot. The shared secret is required to match the shared secret on the external Radius accounting server.
Timeout	Set the timeout value in seconds (1-255) used to timeout users accessing the Radius Accounting server if they have not successfully accessed the Accounting Server.
Retries	Define the number of retries (1-10) the user is allowed to access the Radius Accounting Server if the first attempt fails. The default is 1.

8. Refer to the *Radius Configuration* field to define a primary and secondary Radius server port and shared secret password.

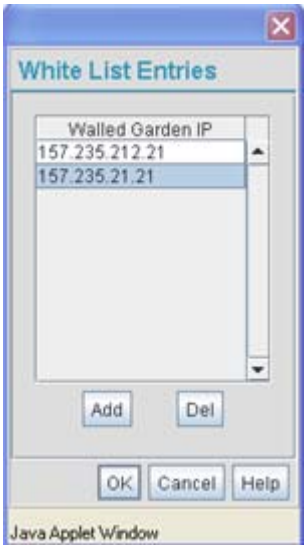
Select Mode	Use the *Select mode* drop-down menu to define whether an Internal or External server is to be used for the primary server.
Pri Server IP	Define the IP address of the primary Radius server. This is the address of your first choice for Radius server.
Pri Port	Enter the TCP/IP port number for the server acting as the primary Radius server. The default port is 1812.
Pri Secret	Enter the shared secret password used with the primary Radius Server.
Sec Server IP	Define the IP address of the secondary Radius server. This is the address of your second choice for Radius server.
Sec Port	Enter the TCP/IP port number for the server acting as the secondary Radius server. The default port is 1812.
Sec Secret	Enter the shared secret password used with the secondary Radius Server.

9. Click *OK* to save any changes to the Hotspot Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
10. Click *Cancel* (if necessary) to undo any changes made. Cancel reverts the settings displayed on the Hotspot Configuration screen to the last saved configuration.

Defining the hotspot White List

To host a Login, Welcome or Fail page on the external Web server, the IP address of that Web server should be in access point's White List.

NOTE
If using an external Web Server over the WAN port, and the hotspot's HTTP pages (login or welcome) redirect to the access point's WAN IP address for CGI scripts, the IP address of the external Web server and the access point's WAN IP address should be entered in the White List.



When a client requests a URL from a Web server, the login handler returns an HTTP redirection status code (for example, 301 Moved Permanently), which indicates to the browser it should look for the page at another URL. This other URL can be a local or remote login page (based on the hotspot configuration). The login page URL is specified in the location's HTTP header.

To host a Login page on the external Web server, the IP address of the Web server should be in the White list (list of IP addresses allowed to access the server) configuration. Ensure the Login page is designed so the submit action always posts the login data on the access point.

To define the White List for a target WLAN:

1. Click the *White List Entries* button from within the WLAN's Hotspot Config screen.
2. Click the *Add* button to define an IP address for an allowed destination IP address.
3. Select a White List entry and click the *Del* button to remove the address from the White List.
4. Click *OK* to return to the Hotspot Config screen where the configuration can be saved by clicking the Apply button.

   Now user enters his/her credentials on Login page and submits the page. Login Handler will execute a CGI script, which will use this data as input.
5. Click *Cancel* to return to the Hotspot Config screen without saving any of the White List entries defined within the White List Entries screen.

Customizing a hotspot display

Each access point WLAN can have a unique hotspot configured and mapped to that WLAN. This enables each access point WLAN to have an optimized hotspot configuration and applet display in respect to the WLAN's client support needs.

The hotspot's login, welcome and fail (login failure) pages are separate HTML files that can be content customized for each WLAN using a *cascading style sheet* (css). These screens can be customized in one of two ways:

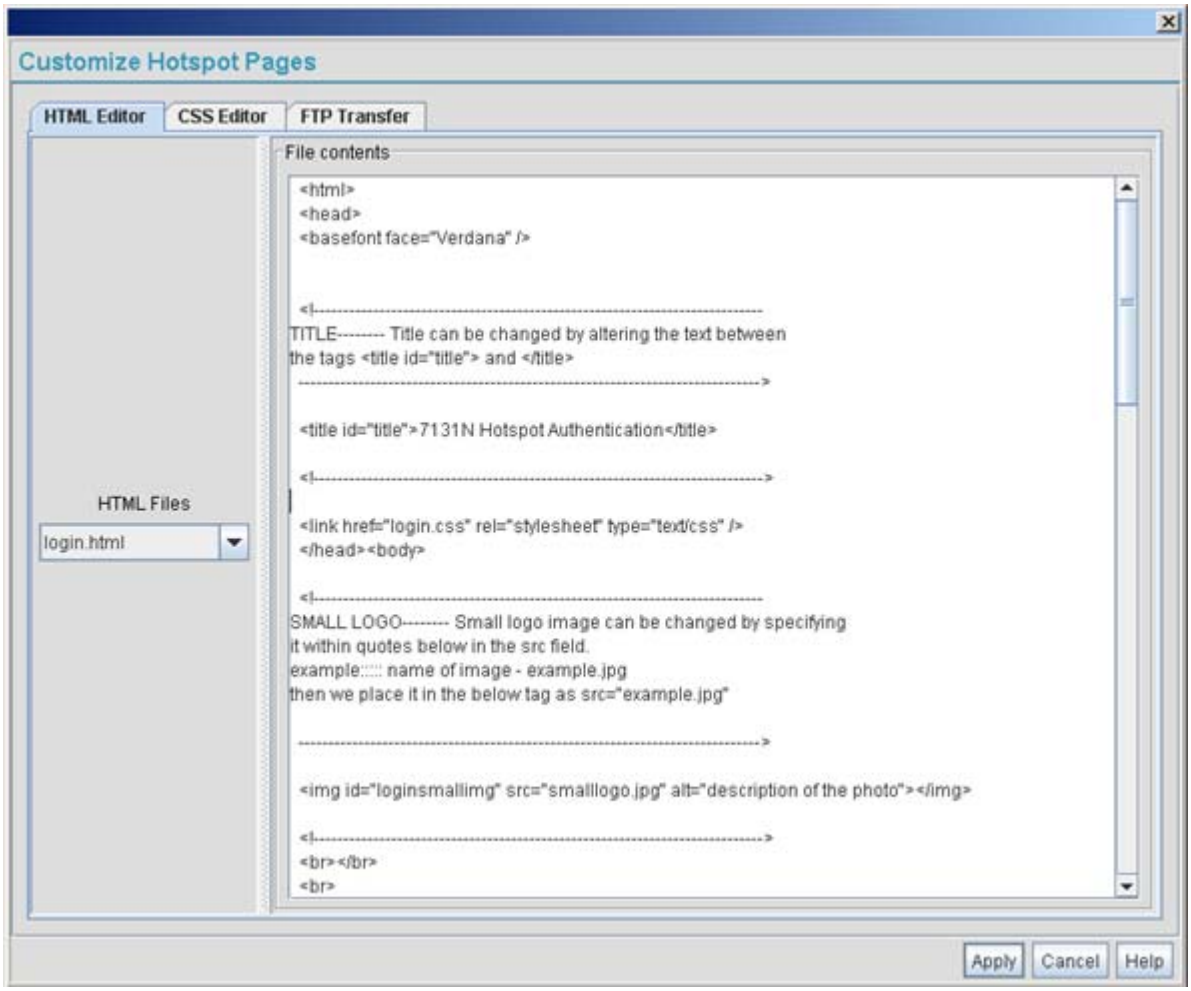
- By customizing the text and fonts displaying within the screens
- By customizing the properties (background color, logos etc.) of the screens themselves

The css contains the styling information for all the elements on the screens. This includes the font of displayed text as well as image placement and sizing. The css contains an exhaustive list of text and image properties which can altered by professional installer to customize the appearance of the hotspot.

Brocade provides a default set of HTML files for the login, welcome and fail pages, and one css file that's referenced by these HTML files. The professional installer is also provided two default images which can be manipulated as required. Thus by default, each hotspot directory contains 3 HTML files, 1 css file and 2 images (small and large logos). Of these 5 files, the css file is used to customize the other pages. The files are hosted on the access point and imported to clients via an FTP download option provided by the access point's applet and the CLI. Once the css and HTML file editing is completed, they can be exported back to the access using FTP again.

To configure a customized WLAN hotspot:

1. Ensure the *Enable Hotspot* checkbox is selected from within the target WLAN screen, and ensure the WLAN is properly configured.
2. Click the *Configure Hotspot* button within the WLAN screen to display the *Hotspot Configuration* screen for that target WLAN.
3. Select *Customize Hotspot Pages* from within the *Internal Web Page Configuration* field.
4. Define the customized text you would like displayed for this WLAN's login, welcome and failure pages by selecting each page from the *HTML Files* drop-down menu.



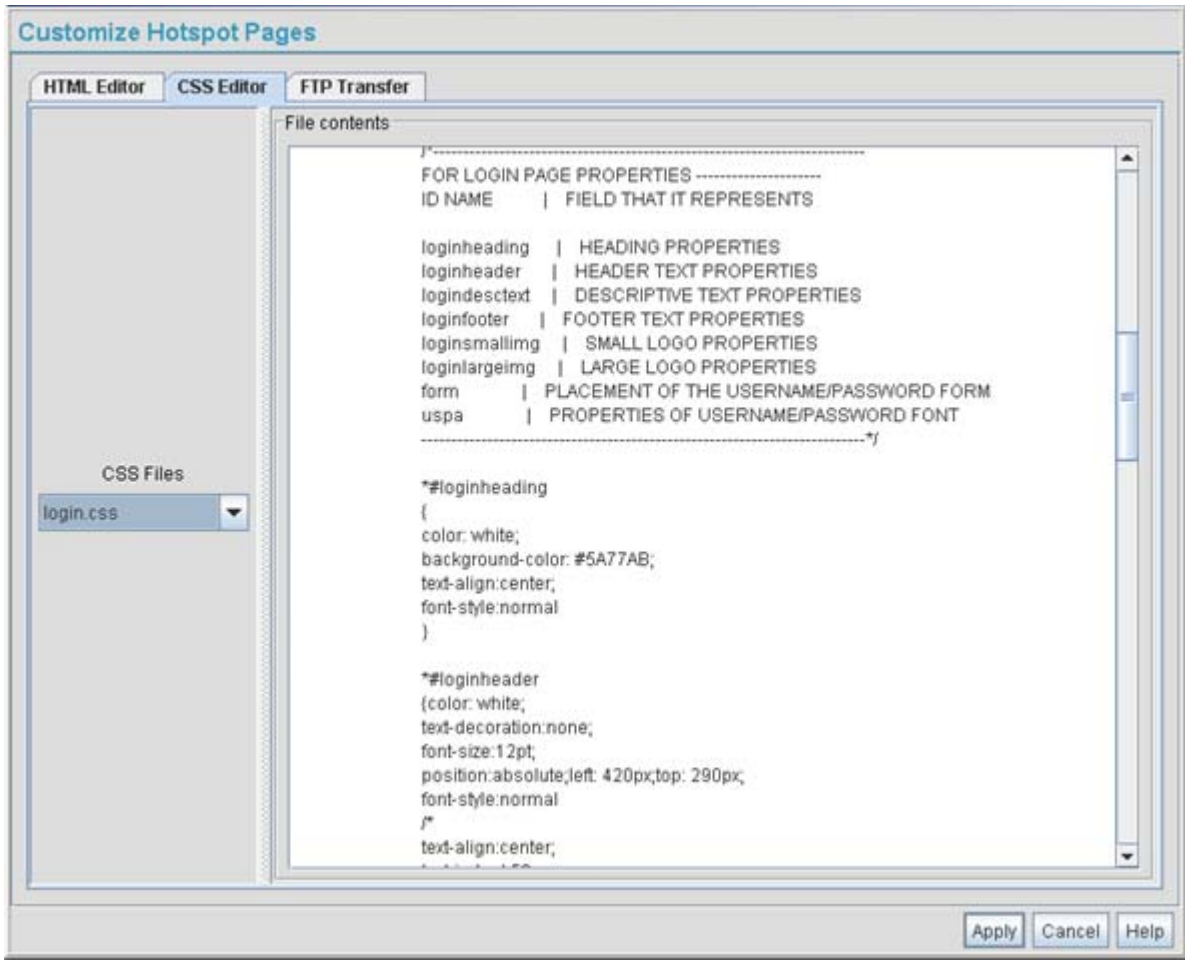
The HTML Editor enables you to customize the hotspot html code. It displays the login.html, welcome.html and fail.html files (depending on user selection) in an editable text area.

CAUTION

No file in a hotspot directory can exceed 10 kb. The maximum number of characters that can be entered into the text area is 10240.

5. Select *Apply* to save the updates made thus far.
6. Select the *CSS Editor* tab to review a guide describing css file customizations impacting how screens display for this WLAN's hotspot.

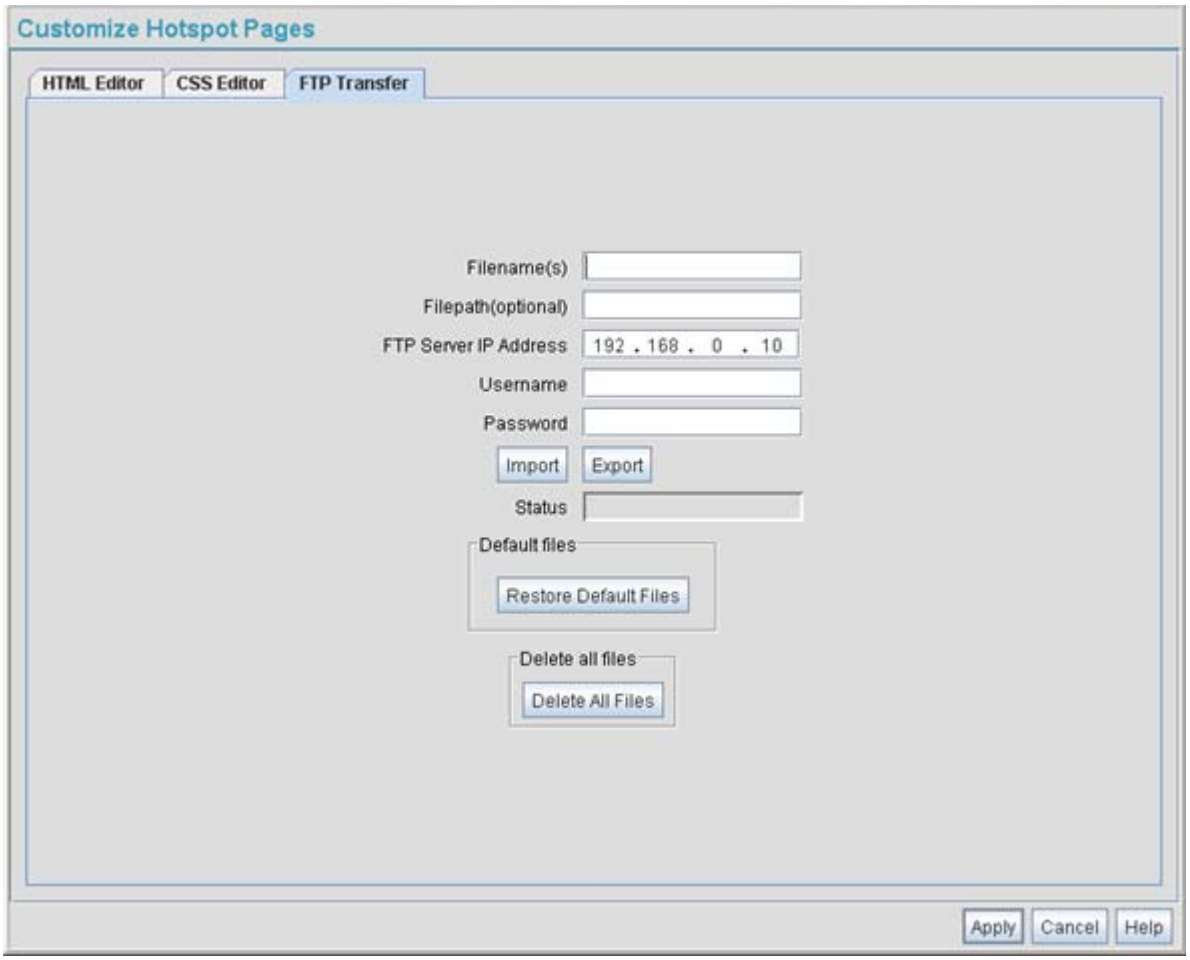
   The CSS Editor tab contains descriptions of each field that can be manipulated within the css file. It also contains parameter options that can be used to change the appearance of the HTML screens. Thus, the CSS Editor tab is like a help file available as customizations are made to the css file.



CAUTION

Once updated, the CSS file must not exceed 12500 bytes, or it cannot be exported back onto the access point for effective deployment with the hotspot.

7. Select the *FTP Transfer* tab to define the configuration of the FTP server configuration and target filename used to import or export the CSS and logo banners to and from the hosting access point.



Filename(s)	Provide the name of the target file either imported or exported from the FTP server. Up to 10 files can be used, and each must not exceed 39 characters.
Filepath(optional)	Optionally provide the path to the hotspot files specified within the Filenames field. The path cannot exceed 39 characters.
FTP Server IP Address	Enter the IP address of the FTP server used by the access point to import and export hotspot file information to the clients providing hotspot access.
Username	Specify a username to be used when logging in to the FTP server.
Password	Define a password allowing access to the FTP server for the hotspot import or export operation.
Import	Select the *Import* button to begin an FTP transfer from the hosting access point to the hotspot enabled client. Refer to the Status field for the results of the import operation. Selecting Import also saves the configuration before performing the import operation.

Export	Select the *Export* button to begin an FTP transfer from the hotspot enabled client to the hosting access point. Refer to the Status field for the results of the export operation. Selecting Export also saves the configuration before performing the export operation.
Status	Displays the Pass or Fail designation of the most recent import or export operation.

8. Select the *Restore Default Files* button to overwrite the customized files created on behalf of this WLAN and replace them with the default files provided with the access point firmware.

CAUTION

Brocade recommends exporting any file present required for further development on to an external FTP server since they will all be lost during the restore operation.

9. Select the *Delete All Files* button to clear (delete) the hotspot directory for that particular WLAN so the user can better utilize the space in that hotspot's directory.
10. Click *Apply* to save the changes made within the FTP Transfer tab.

Setting the WLAN's radio configuration

Each Brocade Mobility 7131 Series Access Point WLAN can have a separate 802.11a/n or 802.11b/g/n radio configured and mapped to that WLAN. The first step is to enable the radio.

The access point displays one of three different radio configuration pages depending on which model SKU is purchased. If the access point is a single-radio model, the *Radio Configuration* screen enables you to configure the single radio for either 802.11a/n or 802.11b/g/n support (not both). If the access point is a dual-radio model, the *Radio Configuration* screen enables you to configure one radio for 802.11a/n use and the other for 802.11b/g/n (no other alternatives exist for the dual-radio model).

The new Brocade Mobility 7131N Access Point is available in single, dual and three radio models. The third Mobility 7131N radio is never a WLAN radio. The third radio is either disabled or set to WIPS mode depending on the radio configuration option selected from the Quick Setup screen. With three-radio Mobility 7131N models, a third tab (Radio 3) has been added to the Radio Configuration screen. All of the other WLAN configurable elements available in either of the Radio 1 and Radio 2 tabs have been removed from the Radio 3 tab as they do not apply to WIPS support.

NOTE

The WIPS Server designation and radio configuration is set as part of the access point's quick setup. For more information on the quick setup configuration and how to define WIPS radio support, see "Configuring device settings" on page 53. For a description of WIPS functionality and how it relates to access point operation, see "Sensor support" on page 7.

Mobility 7131 SKU	Description
Single Radio	One radio supporting either WLAN or WIPS
Dual Radio	Two radios supporting either WLAN or WIPS (mutually exclusive)

Mobility 7131N SKU	Description
Single Radio	One radio supporting either WLAN or WIPS
Dual Radio	Two radios supporting either WLAN or WIPS (mutually exclusive)
Three Radios	Two radios supporting either WLAN or WIPS. Radio three dedicated to WIPS.

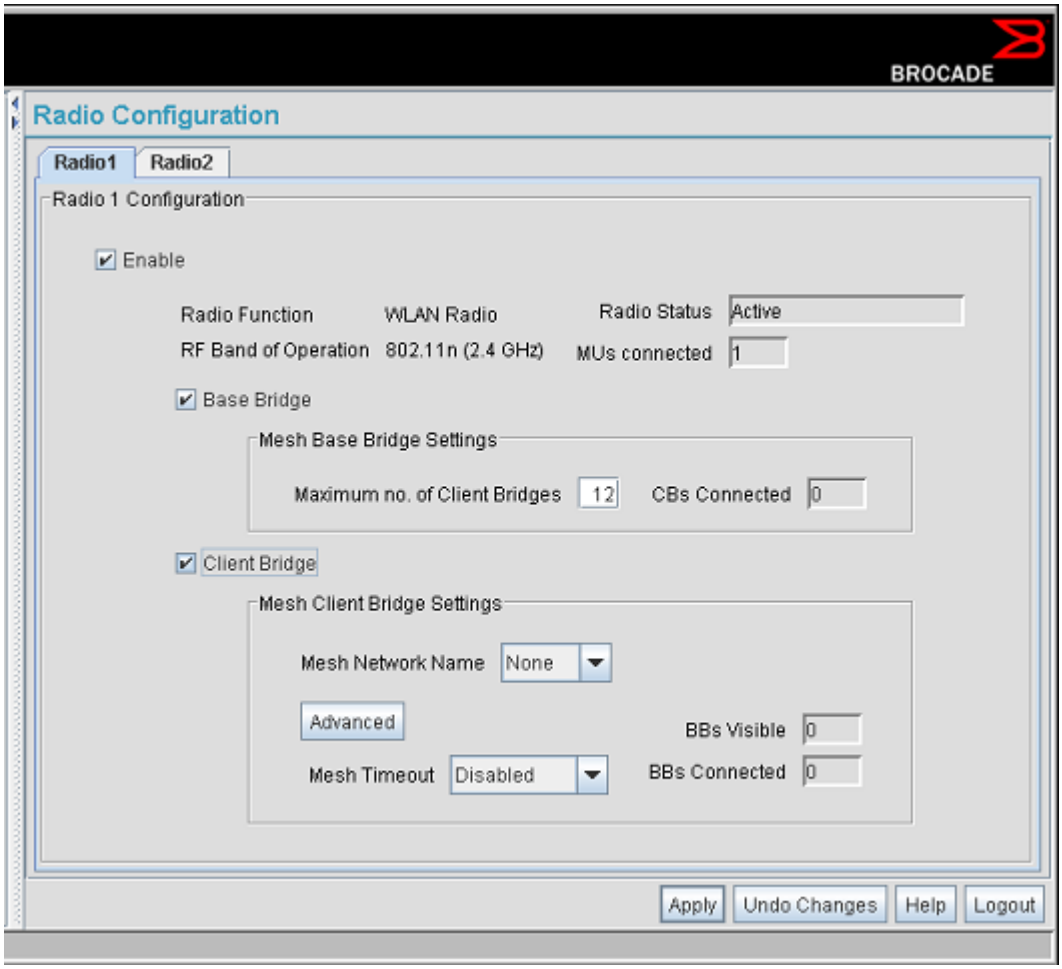
For radios 1 and 2, WIPS and WLAN modes are mutually exclusive. In WLAN mode, a radio functions as a traditional access point, providing wireless bridging. In WIPS mode a radio provides no wireless bridging. Instead, the radio performs the following functionality:

- *Wireless Termination* - The access point attempts to force an unwanted (or unauthorized) connection to disconnect.
- *Wireless Sniffing* - All received frames are reported to the WIPS server. This feature provides the WIPS server with visibility into the activity on the wireless network. The WIPS server processes the received traffic and provides the IT administrator with useful information about the 802.11 RF activities in the enterprise.
- *Spectrum Analysis* - The data needed to provide the current RF Spectrum is provided to the WIPS server. The access point does not display the data, but it is available to the WIPS server. Spectrum analysis can operate only when there are no WLAN radios configured. The WIPS daemon and server are responsible for limiting operation only when there is no radio in WLAN mode. When a configuration change is made at the AP, the Spectrum Analysis operation stops.
- *Live View*- The WIPS application (commonly referred to as AirDefense Enterprise) provides a live view of the sensors, APs and clients operating in a WLAN. Live view support exists throughout the WIPS application, wherever a device icon appears in an information panel or navigation tree. Access Live View by right-clicking on the device, which automatically limits the data to the specific device your choose.

The Radio Configuration screen displays with tabs. One tab for each access point radio. Verify tabs are selected and configured separately to enable the radio(s), and optionally set their mesh network definitions.

To set the Brocade Mobility 7131 Series Access Point radio configuration (this example is for a dual-radio access point):

1. Select *Network Configuration -> Wireless -> Radio Configuration* from the Brocade Mobility 7131 Series Access Point menu tree.



Review the *Radio Function* to assess if this radio is currently functioning as a WLAN radio or has been dedicated as a sensor.

Refer to *RF Band of Operation* parameter to ensure you are enabling the correct 802.11a/n or 802.11b/g/n radio. After the settings are applied within this Radio Configuration screen, the *Radio Status* and *Clients Connected* values update. If this is an existing radio within a mesh network, these values update in real-time.

NOTE
This section describes mesh networking (setting the radio's base and client bridge configuration) at a high level. For a detailed overview on the theory of mesh networking, see "Mesh networking overview" on page 583. For detailed information on the implications of setting the mesh configuration, see "Configuring mesh networking support" on page 587. To review mesh network deployment scenarios, see "Mesh network deployment - quick setup" on page 597.

Refer to the *Sensor-only mode* parameter to discern whether this access point radio has been set to function as WLAN radio (normal operation) or as a dedicated sensor (no WLAN support available). The access point is set as a sensor radio using either the access point's *Quick Setup* screen or using a CLI command. Sensor mode support is disabled by default. For more information on using the Quick Setup screen to define the radio mode, see "Basic device configuration" on page 51.

2. Set the *Maximum Clients* between 0 - 127.

   The maximum number of clients that can associate to a single AP is 127. Therefore, the possible number of clients that can associate to each radio is between 0 and 127. This implies the maximum number of associations for a single-radio AP is the same as the limit of 127 clients for the entire AP.

NOTE
The Maximum clients feature is not supported on single radio model access points, since client load balancing distributes client associations evenly among deployed APs. A single-radio AP's primary concern is how clients are distributed internally, and that depends on the maximum number of clients per WLAN, not per radio. Thus, the feature best supports multiple-radio APs. However, with a multiple-radio AP, a radio can be configured as either a Rogue AP or WIPS detector, not for just WLAN client support.

NOTE
The access point does not support client radio associations if its Maximum clients value is set to 0. Alternatively, if you set the value to 127 for one radio, you risk shutting out client associations for the other radio(s), as the AP does not validate the logic of a user's client association distribution.

3. Select the *Base Bridge* checkbox to allow the radio to accept client bridge connections from other access points in client bridge mode. The base bridge is the acceptor of mesh network data from those client bridges within the mesh network and never the initiator.
4. If the Base Bridge checkbox has been selected, use the *Max# Client Bridges* parameter to define the client bridge load on a particular base bridge.

   The maximum number of client bridge connections per radio is 12, with 24 representing the maximum for dual-radio models.

CAUTION
An access point is Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the access point's WAN connection. If this situation is experienced, log-in to the access point again.

Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of client bridge connections for this specific radio displays within the *CBs Connected* field. If this is an existing radio within a mesh network, this value updates in real-time.

CAUTION

A problem could arise if a Base Bridge's Indoor channel is not available on an Outdoor Client Bridge's list of available channels. As long as an Outdoor Client Bridge has the Indoor Base Bridge channel in its available list of channels, it can associate to the Base Bridge.

5. Select the *Client Bridge* checkbox to enable the access point radio to initiate client bridge connections with other mesh network supported access point's using the same WLAN.

   If the Client Bridge checkbox has been selected, use the *Mesh Network Name* drop-down menu to select the WLAN (ESS) the client bridge uses to establish a wireless link. The default setting, is (WLAN1). Brocade recommends creating (and naming) a WLAN specifically for mesh networking support to differentiate the Mesh supported WLAN from non-Mesh supported WLANs.

CAUTION

An access point in client bridge mode cannot use a WLAN configured with a Kerberos or EAP 802.1x based security scheme, as these authentication types secure user credentials not the mesh network itself.

NOTE
Ensure you have verified the radio configuration for both Radio 1 and Radio 2 before saving the existing settings and exiting the Radio Configuration screen.

Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of base bridges visible to the radio displays within the *BBs Visible* field, and the number of base bridges currently connected to the radio displays within the *BBs Connected* field. If this is an existing radio within a mesh network, these values update in real-time.

6. Click the *Advanced* button to define a prioritized list of access points to define Mesh Connection links. For a detailed overview on mesh networking and how to configure the radio for mesh networking support, see "Configuring mesh networking support" on page 587.
7. If using a dual-radio model access point, refer to the *Mesh Timeout* drop-down menu to define whether one of the radio's beacons on an existing WLAN or if a client bridge radio uses an uplink connection. The Mesh Timeout value is not available on a single-radio access point, since the radio would have to stop beaconing and go into scan mode to determine if a base bridge uplink is lost. The following drop-down menu options are available:

Disabled	When disabled, both radios are up at boot time and beaconing. If one radio (radio 1) does not have a mesh connection, the other radio (radio 2) is not affected. Radio 2 continues to beacon and associate clients, but Client's can only communicate amongst themselves using the access point. Disabled is the default value.

Uplink Detect	When Uplink Detect is selected, the access point only boots up the radio configured as a client bridge. The access point boots up the second radio as soon as the first mesh connection is established. However, if the client bridge radio loses its uplink connection, the second radio shuts down immediately. Uplink detect is the recommended setting within a multi-hop mesh network.
Enabled	If the mesh connection is down on one radio (radio 1), the other radio (radio 2) is brought down and stops beaconing after the timeout period (45 - 65535 seconds). This allows the client bridge (radio 1) to roam without dropping the Client's associated to radio 2. The disadvantage is that radio 2 may beacon for the timeout period and have to drop associated Client's because radio 1 could not establish its uplink. The default timeout period is 45 seconds.

NOTE
The Mesh Time Out variable overrides the *Ethernet Port Time Out* (EPTO) setting on the LAN page when the access point is in bridge mode. As long as the mesh is down, the access point acts in accordance to the Mesh Time Out setting regardless of the state of the Ethernet. However, if the Ethernet goes down and the mesh link is still up, the EPTO takes effect.

For a detailed overview on mesh networking and how to configure the radio for mesh networking support, see “Configuring mesh networking support” on page 587.

8. 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.

CAUTION

When defining a Mesh configuration and changes are saved, the mesh network temporarily goes down. The Mesh network is unavailable because the access point radio is reconfigured when applying changes. This can be problematic for users making changes within a deployed mesh network. If updating the mesh network using a LAN connection, the access point applet loses connection and the connection must be re-instated. If updating the mesh network using a WAN connection, the access point applet does not lose connection, but the mesh network is unavailable until the changes have been applied.

9. 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.
10. Click *Logout* to securely exit the 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 Brocade Mobility 7131 Series Access Point menu tree.

    For more information, see “Configuring the 802.11a/n or 802.11b/g/n radio” on page 167.

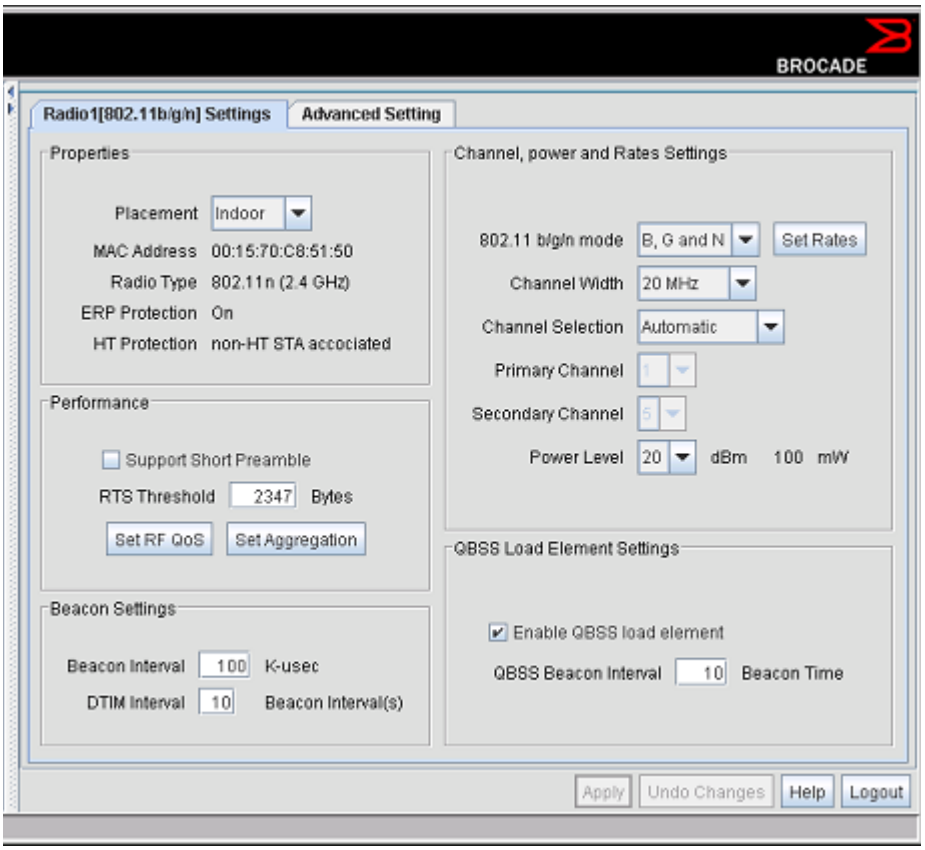
Configuring the 802.11a/n or 802.11b/g/n radio

Configure an 802.11a/n or 802.11b/g/n radio by selecting the radio's name (as defined using the 802.11a/n or 802.11b/g/n 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 and set the broadcast/multicast transmission control.

To configure the Brocade Mobility 7131 Series Access Point's 802.11a/n or 802.11b/g/n radio:

1. Select *Network Configuration -> Wireless -> Radio Configuration -> Radio1* (default name) from the Brocade Mobility 7131 Series Access Point menu tree.

   On a single-radio model, Radio1 could either be an 802.11a/n or 802.11b/g/n 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 Brocade Mobility 7131 Series Access Point.
MAC Address	The Brocade Mobility 7131 Series Access Point, 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.For additional information on access point MAC address assignments, see "Brocade Mobility 7131 Series Access Point MAC address assignment" on page 29.
Radio Type	The *Radio Type* parameter simply displays the radio type as 802.11a/n or 802.11b/g/n. This field is read only and always displays the radio type selected from the Brocade Mobility 7131 Series Access Point menu tree under the Radio Configuration item.
ERP Protection	*Extended Rate PHY* (ERP) allows 802.11g clients to interoperate with 802.11b only clients. ERP Protection is managed automatically by the access point and informs users when 802.11b clients are present within the access point's coverage area. The presence of 802.11b clients within the 802.11g coverage area negatively impacts network performance, so this feature should looked to as an indicator of why network performance has been degraded.
HT Protection	Displays the HT Protection state, and whether a non HT protected Client is currently associated with the Brocade Mobility 7131 Series Access Point.

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

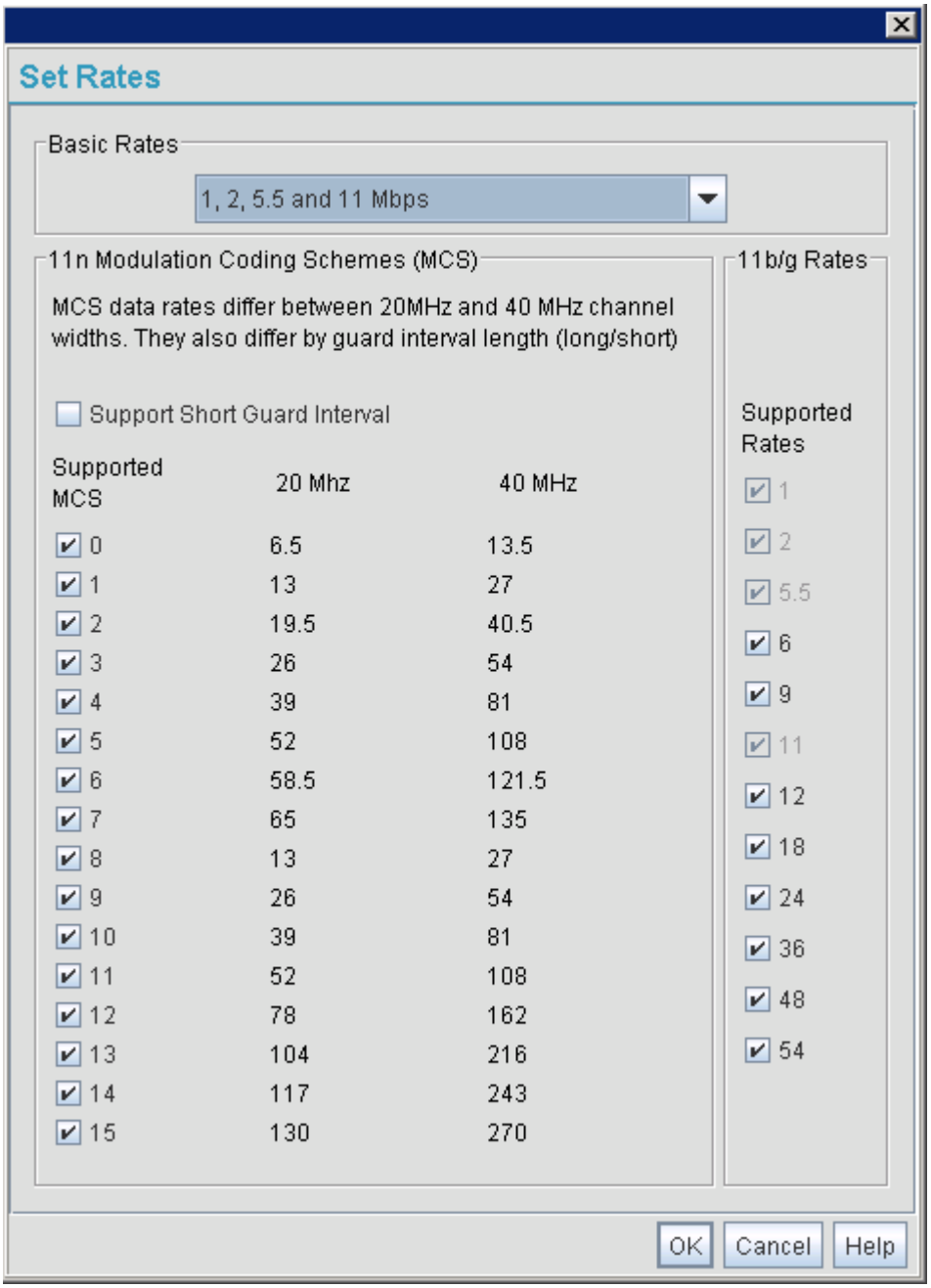
CAUTION

Indoor channels for a Brocade Mobility 7131 Access Point are different then a Brocade Mobility 7131N Access Point's indoor channels due to FCC regulatory restrictions. When deploying a mesh network, Brocade recommends manually configuring channels and not using the *Automatic* or *Uniform* options.

802.11 b/g/n Mode	For radio1, specify *B, G and N*, *B and G*, *G Only*, *B only* or *N Only* to define whether the 802.11b/g/n 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/n clients. Selecting b and g enables the Brocade Mobility 7131 Series Access Point to transmit to both b and g clients if legacy clients (802.11b) partially comprise the network. Select accordingly based on the Client requirements of the network. The rates for the access point's 2.4 GHz radio are as follows: *B, G and N* - Allows only basic rates (default setting). *B and G* - Allows 11b basic rates. Does not allow MCS rates. *G and N* - Requires basic rates (either 6, 12, 24 or 1, 2, 5.5, 11, 6, 12, 24). *G Only* - Requires one 11g basic rate. Does not allow MCS rates. *B Only* - Allows for 11b rates only. Does not allow G or N rates. *N Only* - Requires basic MCS rates. Note: If the mode is B and G, the Channel Width option is not available, and a Secondary Channel cannot be defined. For the 5 GHz radio, specify *A and N*, *A Only* or *N Only* to define whether the 802.11a/n radio transmits in the 5 Ghz band exclusively for 802.11a clients, 802.11n clients or transmits in the 5 Ghz band for both 802.11a/n clients. *A Only* - Allows 11a rates. *N Only* - Requires basic MCS rates. *A and N* - Allows only 11a basic rates (default setting).
Channel Width	Select the Channel Width (MHz) from the drop-down menu. The AP radio can support 20 and 40 MHz channel widths. 20 MHz is the default setting for the 2.4 GHz radio. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the Brocade Mobility 7131 Series Access Point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of "wider channels." 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Define a value as needed depending on the channel used. This field is not available when B and G is selected as the 802.11 b/g/n mode.

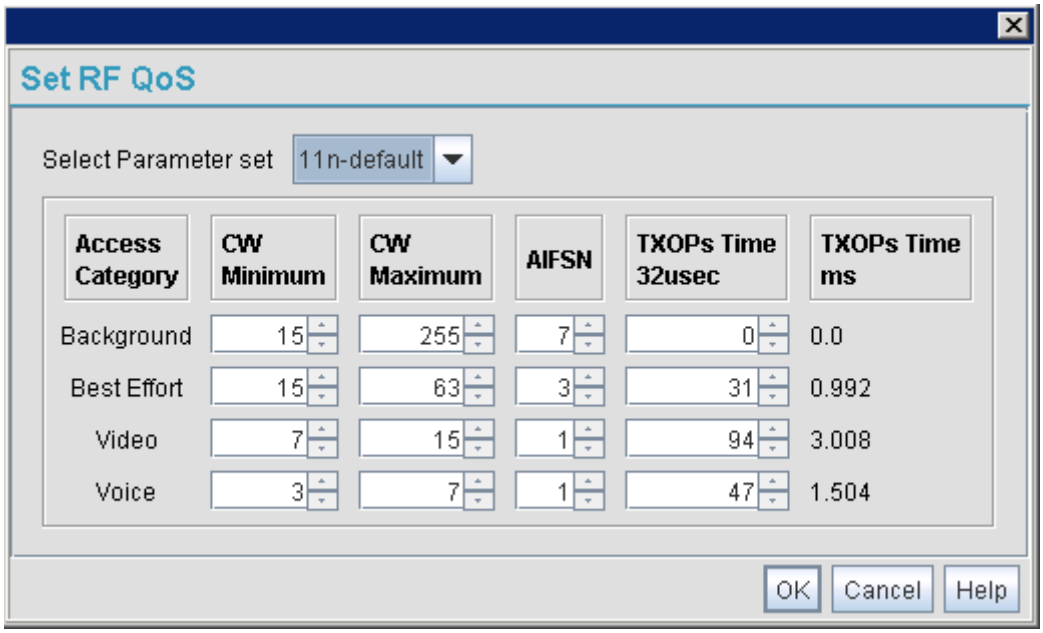
Channel Selection	The following channel selection options exist: *User Selected* - This is the default setting. If 20/40 MHz is selected as the Channel Width (supporting 11n), the *Secondary Channel* drop-down menu becomes enabled. The user must define the primary channel first. Then, depending on the primary channel defined, the secondary channel list is filled with channels making the combination of primary and secondary channels valid. The actual channels available depend on regulatory domain requirements. *Automatic* - When the access point is booted, the access point scans non-overlapping channels listening for beacons from other access points. After the channels are scanned, it will select the channel with the fewest access points. In the case of multiple access points on the same channel, it will select the channel with the lowest average power level. The *Random* option is available for use with the 802.11a/n radio. To comply with *Dynamic Frequency Selection* (DFS) requirements in the European Union, the 802.11a/n radio uses a randomly selected channel each time the access point is powered on.
Power Level	Use the drop-down menu to defines the transmit power of the 802.11a/n or 802.11b/g/n antenna(s). The values are expressed in dBm and mW.

Antenna Gain	Set the antenna gain used with the selected antenna type between 0.00 - 15.00 dBm. The access point's *Power Management Antenna Configuration File* (PMACF) automatically configures the access point's radio transmit power based on the antenna type (provided in the CLI), its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once the antenna type and gain are provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Brocade recommends that only a professional installer set the antenna gain and the antenna type.
Set Rates	Click the *Set Rates* button to define minimum and maximum data transmit rates for the radio. Use the *Basic Rates* drop-down menu to select the rates available for either the 2.4 GHz or 5 GHz radio band. The menu options differ, based on the radio band. For 2.4 GHz, the following options are available: 1 and 2 Mbps 1, 2, 5.5 and 11 Mbps (default setting) 1, 2, 5.5, 11 and 6, 12, 24 Mbps 1, 2, 5.5, 11 and 6, 12, 24 Mbps and MCS 0-7 6, 12 and 24 Mbps 6, 12 and 24 Mbps and MCS 0-7 MCS 0-7 For 5 Ghz, the following options are available: 6, 12 and 24 Mbps 6, 12 and 24 Mbps and MCS 0-7 MCS 0-7 When a basic rate option is selected (from the drop-down menu), the rates are automatically selected and grayed out in the *Supported Rates* radio boxes. Select remaining rates as needed for additional supported rates. Enable the *Support Short Guard Interval* checkbox to set a guard interval (for interference protection) for 20 MHz and 40 MHz channel widths. When enabled, the AP's radio defines values to enable a packet to be transmitted with guard interval based on the configuration and capabilities of associated clients. Clients can associate to a Brocade Mobility 7131 Series Access Point regardless of whether they support a short guard interval. If supporting 802.11n, select a *Supported MCS* index (0-15). Set a MCS *(modulation and coding scheme)* in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). Click *OK* to implement the selected rates and return to the radio configuration screen. Clicking *Cancel* reverts the Set Rates screen to the last saved configuration.

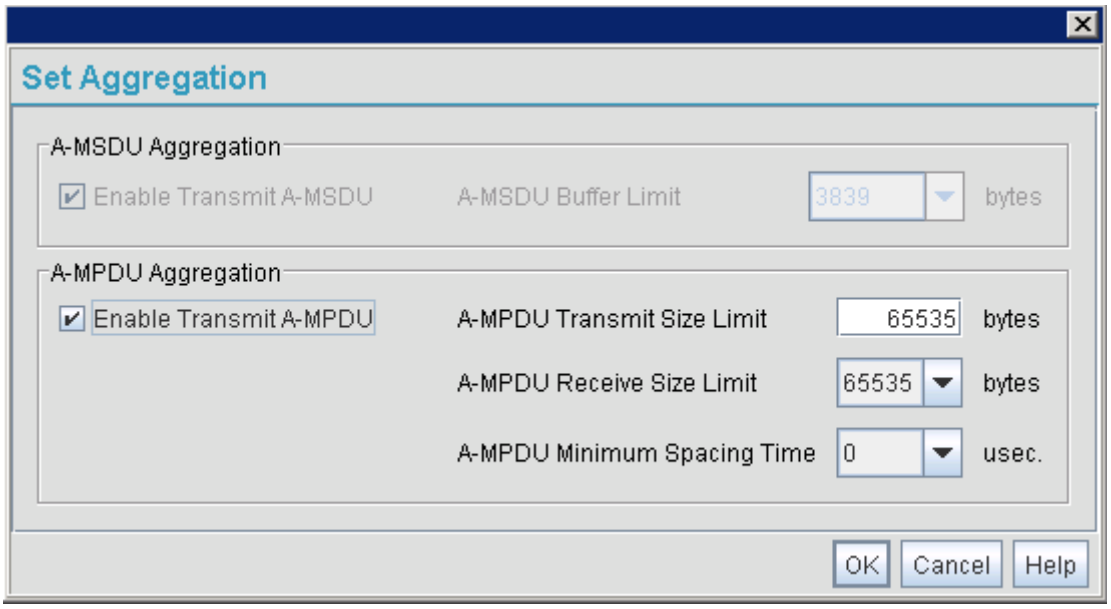


4. Configure the *Performance* field to set the preamble, thresholds values and QoS values for the radio.

Support Short Preamble Interval	The preamble is approximately 8 bytes of packet header generated by the access point and attached to a packet prior to transmission from the 802.11b radio. The preamble length for 802.11b transmissions is rate dependant. A short preamble is 50% shorter than a long preamble. Leave the checkbox unselected if in a mixed Client/AP environment, as clients and the access point 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 Brocade Mobility 7131 Series Access Point to use RTS (Request To Send) on frames longer than the specified length. The default is 2341bytes.
Set RF QoS	Click the *Set RF QoS* button to display the *Set RF QOS* screen to set QoS parameters for the radio. Do not confuse with the QoS configuration screen used for a WLAN. The Set RF QoS screen initially appears with default values displayed. Select *manual* from the *Select Parameter set* drop-down menu to edit 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/n or 802.11b/g/n radio, not the QoS policies configured for the WLAN (as created or edited from the *Quality of Service Configuration* screen). Brocade recommends only advanced users manually set these values. If the type of data-traffic is known, use the drop-down menu to select an option representative of the intended radio band support. Wifi represents multimedia traffic, default is typical data traffic and voice is for “Voice-Over-IP” supported wireless devices. Click *OK* to implement the selected QoS values and return to the 802.11a/n or 802.11b/g/n radio configuration screen. Clicking *Cancel* reverts the screen to the last saved configuration.



Set Aggregation	Select the *Enable Transmit A-MSDU* checkbox (within the A-MSDU Aggregation field) to allow the aggregation of MAC Service frames. When enabled, long frames can be both sent and received (up to 4 KB). Set the A-MSDU buffer limit to either 3839 bytes (default) or 7935 bytes. Select the *Enable Transmit A-MPDU* checkbox (within the A-MPDU Aggregation field) to allow the aggregation of MAC Protocol frames. When enabled, long frames can be both sent and received (up to 64 KB). When enabled, define an A-MPDU Transmit Size Limit (default is 2 bytes), A-MPDU Receive Size Limit (default is 65535 bytes) and an A-MPDU Minimum Spacing Time (default is 0 usec). Set these values as appropriate to broadcast the maximum length A-MPDU transmit and receive intervals that can be used.



5. Refer to the *Beacon Settings* field to set the radio beacon and DTIM intervals.

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 for each of the four access point BSSIDs. If a system has an abundance of broadcast traffic and it needs to be delivered quickly, Brocade recommends decreasing the DTIM interval for that specific BSSID. However, decreasing the DTIM interval decreases the battery life on power save stations. The default is 10 for each BSSID. Brocade recommends using the default value unless qualified to understand the performance risks of changing it.

6. Refer to the *QBSS Load Element Setting*s field to determine whether channel usage data is transmitted to associated devices.

Enable QBSS Load Element	When enabled, the access point communicates channel usage data to associated devices using an interval you define. The QBSS load represents the percentage of time the channel is in use by the access point and the access point's Client count. This information is helpful in assessing the access point's overall load on a channel, its availability for additional device associations and multi media traffic support. This setting is enabled by default.
QBSS Beacon Interval	Set the QBSS beacon (transmission) interval the access point uses for sending QBSS data to associated devices.

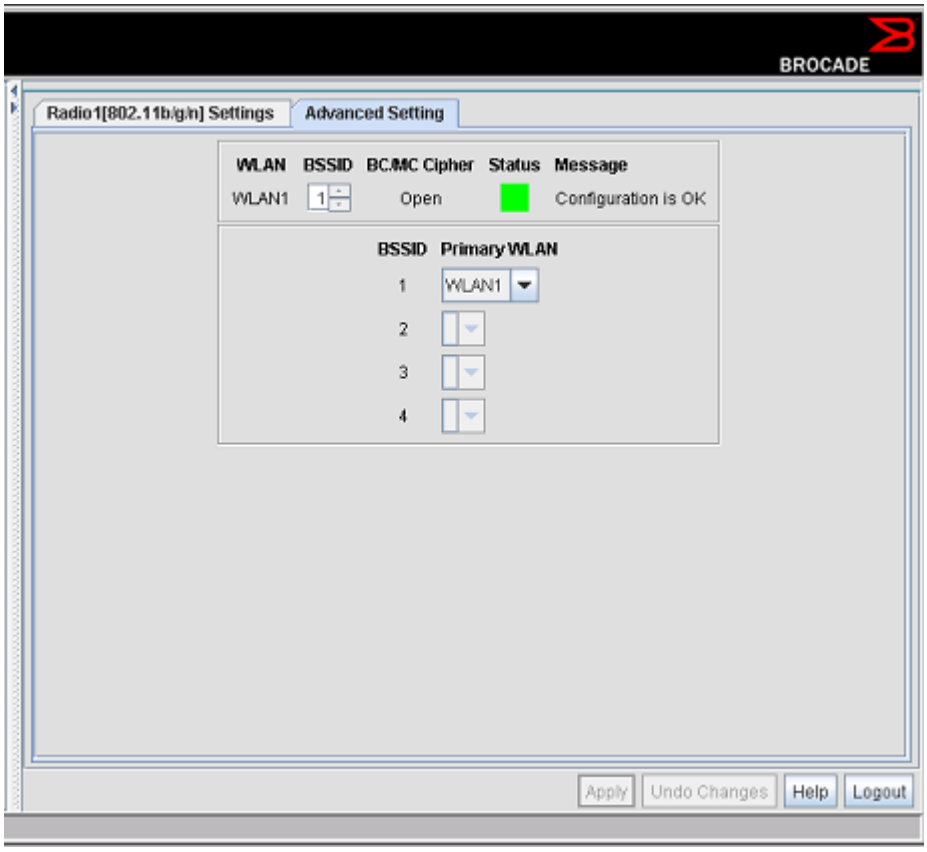
7. Refer to the *Broadcast/Multicast Transmit Control* field to define the broadcast/multicast transmission configuration.

   The *Optimized for Range* radio button is selected by default. This default option is ideal when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates selected from this radio's Set Rates screen.

   Select the *Optimized for Throughput* radio button to transmit group packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.

   NOTE
   Broadcast/multicast rate control is supported in both standalone and adaptive AP configurations and can be imported/exported as part of the access point's existing configuration import and export capability.

8. Select the *Advanced Setting*s tab to strategically map BSSIDs to WLANs in order to define them as primary WLANs.



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 access point, there are 4 BSSIDs available. If using a dual-radio access point, 4 BSSIDs for the 802.11b/g/n radio and 4 BSSIDs for the 802.11a/n radio are available.

WLAN	Lists the WLAN names available to the 802.11a/n or 802.11b/g/n radio that can be assigned to a BSSID.
BSSID	Assign a BSSID value of 1 through 4 to a WLAN in order to map the WLAN to a specific BSSID.
BC/MC Cipher	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.

Status	Displays the following color coded status: Red - Error (Invalid Configuration) Yellow - Warning (Broadcast Downgrade) Green - Good (Configuration is OK)
Message	Displays the verbal status of the WLAN and BSSID assignments. If the Status column displays green, the Message will typically be *Configuration is OK*. If yellow, a description of invalid configuration displays.

9. 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.
10. 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.
11. 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.
12. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring client rate limiting

Use the *Rate Limiting* screen to control the client rate limit allotted to individual WLANs. client rate limiting enables an administrator to determine how much radio bandwidth is allowed to each client within any one of the 16 supported AP WLANs. Rate limiting is on per a client basis for the WLAN.

To define client rate limits for specific WLANs on an access point radio:

1. Select *Network Configuration -> Wireless -> Rate Limiting* from the access point menu tree.

2. Select the *Enable Rate Limiting* option to globally enable client rate limiting for each of the access point's 16 WLANs.

   Once enabled, client rate limiting still needs to be enabled for a specific WLAN, then the rate limit allocation needs to be defined for client traffic within that specific WLAN. To modify a WLAN-to-radio assignment, see "Creating/editing individual WLANs" on page 139.
3. Refer to the *Per WLAN Rate Limits* field to review the rate limits defined thus far for any of the access point's 16 WLANs.

The rates are displayed in Kbps for both wired to wireless and wireless to wired traffic flows from the WLAN and its radio configuration.

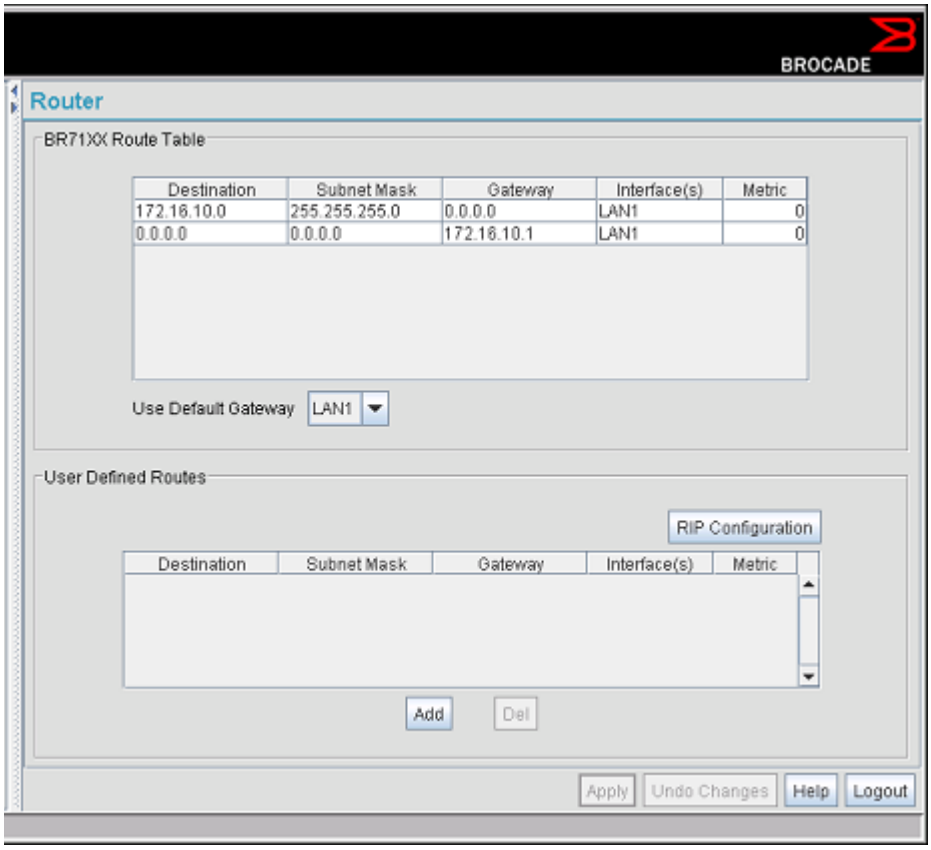
4. Click *Apply* to save any changes to the Bandwidth Management screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
5. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Bandwidth Management screen to the last saved configuration.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

NOTE
Though the Rogue AP and Firewall features appear after the Bandwidth Management features within the access point menu tree, they are described in "Configuring Access Point Security" on page 191, as both items are data protection functions. More specifically, see, "Configuring firewall settings" on page 213 and "Configuring rogue AP detection" on page 238.

Configuring router settings

The Brocade Mobility 7131 Series Access Point router uses routing tables and protocols to forward data packets from one network to another. The Brocade Mobility 7131 Series Access Point router manages traffic within the network, and directs traffic from the WAN to destinations on the Brocade Mobility 7131 Series Access Point managed LAN. Use the Brocade Mobility 7131 Series Access Point *Router* screen to view the router's connected routes. To access the Router screen.

1. Select *Network Configuration -> Router* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the Brocade Mobility 7131 Series Access Point *Router Table* field to view existing routes.

   The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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 125.

3. From the *Use Default Gateway* drop-down menu, select the WAN or either of the two LANs (if enabled) to server as the default gateway to forward data packets from one network to another.

4. To set or view the RIP configuration, click the *RIP Configuration* button.

   Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing-table information. The Router screen also allows the administrator to select the type of RIP and the type of RIP authentication used by the controller. For more information on configuring RIP, see "Setting the RIP configuration" on page 180.

5. 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.

   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.

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

7. Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

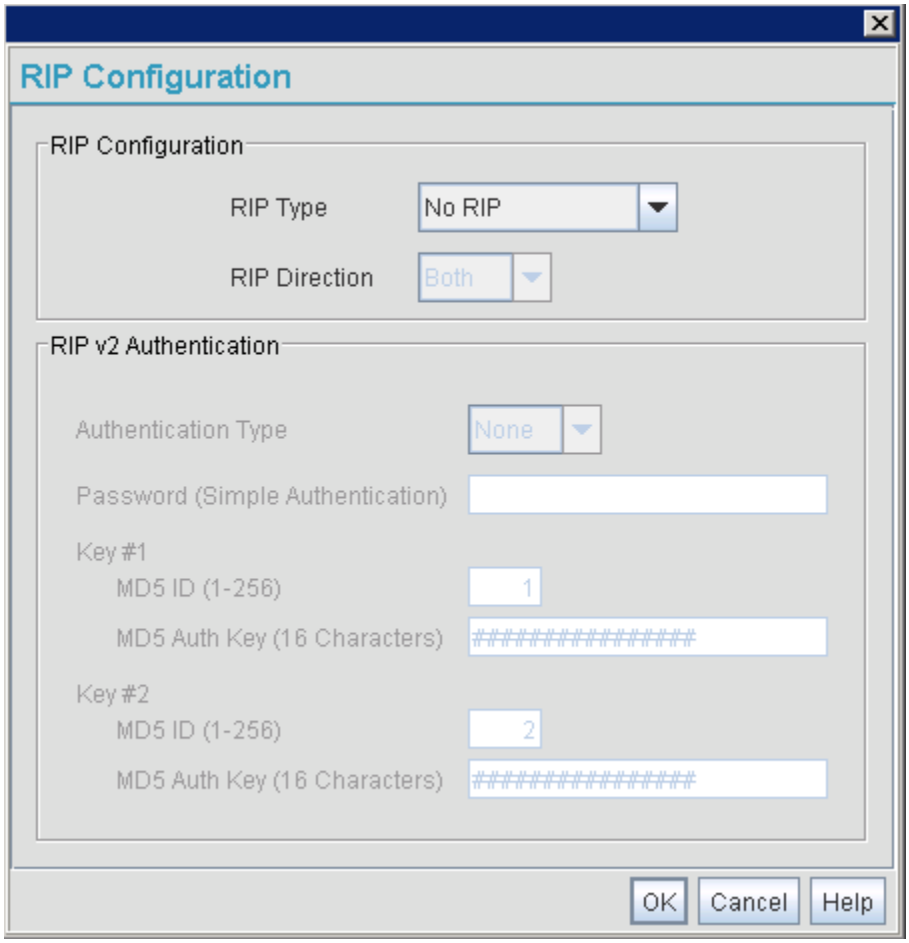
Setting the RIP configuration

To set the RIP configuration:

1. From within the RIP Configuration field, select the RIP Type from the drop-down menu. The following options are available:

No RIP	The *No RIP* option prevents the access point's router from exchanging routing information with other routers. Routing information may not be appropriate to share, for example, if the access point manages a private LAN.
RIP v1	RIP version 1 is a mature, stable, and widely supported protocol. It is well suited for use in stub networks and in small autonomous systems that do not have enough redundant paths to warrant the overhead of a more sophisticated protocol.
RIP v2 (v1 compat)	RIP version 2 (compatible with version 1) is an extension of RIP v1's capabilities, but it is still compatible with RIP version 1. RIP version 2 increases the amount of packet information to provide the a simple authentication mechanism to secure table updates.
RIP v2	RIP version 2 enables the use of a simple authentication mechanism to secure table updates. More importantly, RIP version 2 supports subnet masks, a critical feature not available in RIP version 1. This selection is not compatible with RIP version 1 support.

2. Select a routing direction from the *RIP Direction* drop-down menu. *Both* (for both directions), *Rx only* (receive only), and *TX only* (transmit only) are available options.



3. If RIP v2 or RIP v2 (v1 compat) is the selected RIP type, the *RIP v2 Authentication* field becomes active. Select the type of authentication to use from the *Authentication Type* drop-down menu. Available options include:

None	This option disables the RIP authentication.
Simple	This option enable RIP version 2's simple authentication mechanism. This setting activates the Password (Simple Authentication) field.
MD5	This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128-bit fingerprint. The MD5 setting activates the RIP v2 Authentication settings for keys (below).

4. If the Simple authentication method is selected, specify a password of up to 15 alphanumeric characters in the *Password (Simple Authentication)* area.
5. If the MD5 authentication method is selected, fill in the *Key #1* field (Key #2 is optional). Enter any numeric value between 0 and 256 into the *MD5 ID* area. Enter a string consisting of up to 16 alphanumeric characters in the *MD5 Auth Key* area.
6. Click the *OK* button to return to the Router screen. From there, click *Apply* to save the changes.

Configuring IP filtering

Use the access point's IP filtering functionality to determine which IP packets are processed normally by the access point and which are discarded. If discarded, a packet is deleted and ignored (as if never received). The allow/deny mechanism used by IP filtering makes it similar to an *access control list* (ACL).

IP filtering supports the creation of up to 20 filter rules enforced at layer 3. Once defined (using the access point's SNMP, GUI or CLI), filtering rules can be enforced on the access point's LAN1 or LAN2 interfaces and within any of the 16 access point WLANs. An additional default action is also available denying traffic when filter rules fail. Lastly, imported and exported configurations retain their defined IP filtering configurations.

IP filtering is a network layer facility. The IP filtering mechanism does not know anything about the application using the network connections, only the connections themselves. For example, you can deny user access to an internal network on the default telnet port, but if you rely on IP filtering alone, you cannot stop people from using the telnet program with a port you allow to pass through your firewall.

There are a couple of important rules a packet adheres to when its compared with the filter policy list:

- Packets are always filtered in sequential order (filtering always begins with the first filter policy displayed in the IP Filtering screen, then the second, third, and so on). The *IP Filtering* screen is invoked for LANs within the LAN1 or LAN2 screen and for WLANs within the New WLAN or Edit WLAN screen. It's from this screen that allow or deny designations are set for IP filtering.
- Packets are compared with lines of the filter policy list until a match is made. Once a packet matches a line of the list, it's acted upon, and no further comparisons take place. If inspected packets are determined to not be IP packets, it permitted by the access point for its inbound or outbound destination.

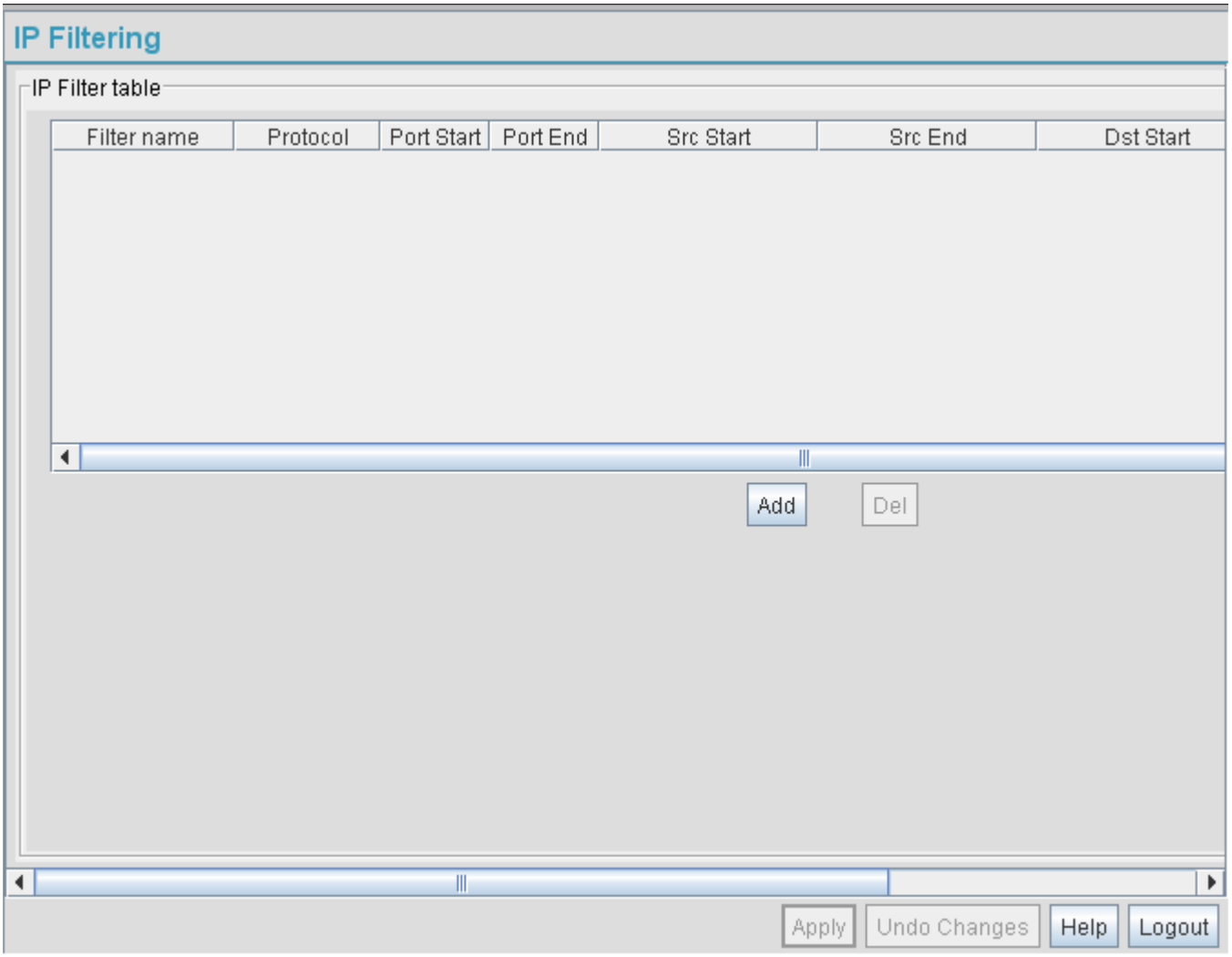
Once you create a filter policy, apply it to an interface in either an incoming or outgoing direction.

- Traffic entering the access point's LAN1, LAN2 or WLAN (1-16) from a client is classified as *Incoming* traffic.
- Traffic leaving the access point's LAN1, LAN2 or WLAN (1-16) in route to a client is classified as *Outgoing* traffic.

For additional examples of how to configure IP Filter policies for both an access point WLAN and LAN, see "IP filter configuration - example" on page 185.

To filter packets against undesired data traffic:

1. Select *Network Configuration -> IP Filtering* from the access point menu tree.



When the IP Filtering screen is initially displayed, there are no default filtering policies, and they must be created.

NOTE
With IP Filtering, users can only define a destination port, not a source port.

2. Click the *Add* button to define the attributes of a new IP Filtering policy. The following policy (or filtering rule) attributes require definition.

Filter name	Create a name for the filter policy unique to its function in order to differentiate it from others that may have somewhat similar configurations.
Protocol	Specify the protocol used for the filter policy. The options are *ALL, TCP, UDP, ICMP, PIM, GRE, RSVP, IDP, PUP, EGP, IPIP, ESP, AH, IGMP, IPVG, COMPR_H and RAW_IP.* The protocol number can also be used as the protocol name. This allows the use or protocols that are not within the drop-down menu.

Port Start	Defines the socket number (or port) number representing the beginning protocol port range either allowed or denied permission to the target LAN1, LAN2 or WLAN.
Port End	Defines the socket number (or port) number representing the ending protocol port range either allowed or denied permission to the target LAN1, LAN2 or WLAN.
Src Start	Creates a range beginning source IP address to be either allowed or denied IP packet forwarding. The source address is where the packet originated. Setting the Src End value the same as the Src Start allows or denies just this address without defining a range.
Src End	Providing this address completes a range of source (data origination) addresses than can either be allowed or denied access to the LAN1, LAN2 or WLAN.
Dst Start	Creates a range beginning destination IP address to be either allowed or denied IP packet forwarding. Setting the Dst End value the same as the Dst Start allows or denies just this address without defining a range.
Dst End	Providing this address completes a range of destination addresses than can either be allowed or denied access to the LAN1, LAN2 or WLAN.
In Use	Displays YES if the listed filter policy is currently being utilized by LAN1, LAN2 or a WLAN. NO is displayed if the listed policy is currently not be utilized by either of the LAN ports or any of the access point's 16 WLANs.

NOTE
Once filter policies have been defined, they can then be applied to traffic on either of the two access point LAN ports or any of the 16 access point WLANs. The procedure for applying a filtering policy is the same, as both the LAN1/LAN2 and WLAN screens display the same IP Filtering sub screen for this operation. For more information, see "Applying a filter to LAN1, LAN2 or a WLAN (1-16)" on page 184.

3. If necessary, select an existing policy and select the *Del* button to permanently remove the filtering policy from those available.
4. Click *Apply* to save any changes to the IP Filtering screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
5. Click *Undo Changes* to securely exit the IP Filtering screen without saving your changes.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Applying a filter to LAN1, LAN2 or a WLAN (1-16)

Once filter polices are defined, they must be applied to a LAN or WLAN within the LAN1 or LAN2 screens, or within the WLAN's New/Edit screens, not from within the main IP Filtering menu.

To apply an existing IP filter policy to LAN1, LAN2 or a WLAN:

1. Display the IP Filtering menu.

   From the LAN1 or LAN2 screen:

a. Select *Network Configuration -> LAN -> LAN1 (or LAN2)* from the access point menu tree.

b. Select the *Enable IP Filtering* button in the lower, right-hand side of the screen.

c. Select the *IP Filtering* button.

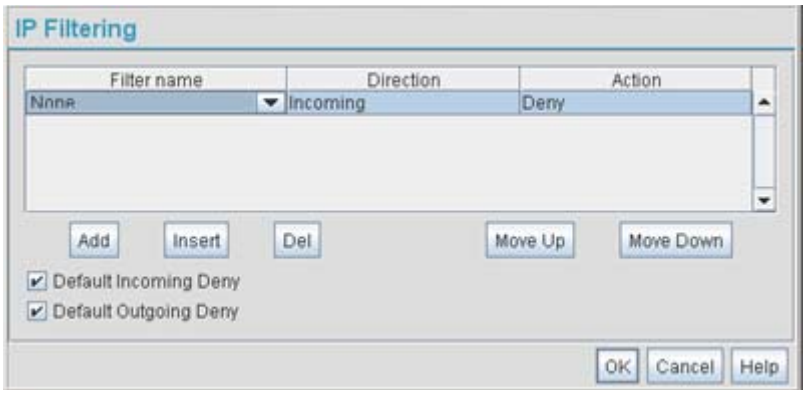
From the Wireless screen:

a. Select *Network Configuration -> Wireless* from the access point menu tree.

b. Click the *Create* button to apply the filter to a new WLAN, or highlight an existing WLAN and click the *Edit* button. Either the *New WLAN* or *Edit WLAN* screen displays.

c. Select the *Enable IP Filtering* button in the lower portion of the screen.

d. Select the *IP Filtering* button.



The screen displays with both the *Default Incoming Deny* and *Default Outgoing Deny* checkboxes selected by default. Consequently, if you enable IP filtering but do not apply any filters that allow IP traffic, then no IP traffic will be forwarded, as the default deny settings have precedence.

2. Use the *Filter name* drop menu to select an existing filter.
3. Set the *Direction* as Incoming or Outgoing as required.
4. Apply an *Action* of Allow or Deny to permit or restrict the rules of this filter in the direction selected.
5. Select *Add* to apply the filter(s) (and their rules and permissions) to the LAN or WLAN.
6. Click *OK* add the IP filter to the LAN or WLAN. Navigating away from the screen without clicking OK results in all changes to the screens being lost.
7. Click *Cancel* to securely exit the IP Filtering screen without saving your changes.

   For additional examples of how to configure IP Filter policies for both an access point WLAN and LAN, see "IP filter configuration - example" on page 185.

IP filter configuration - example

The following describes how to setup a global filter, apply it to a WLAN or LAN and review statistics to assess the filter's configuration.

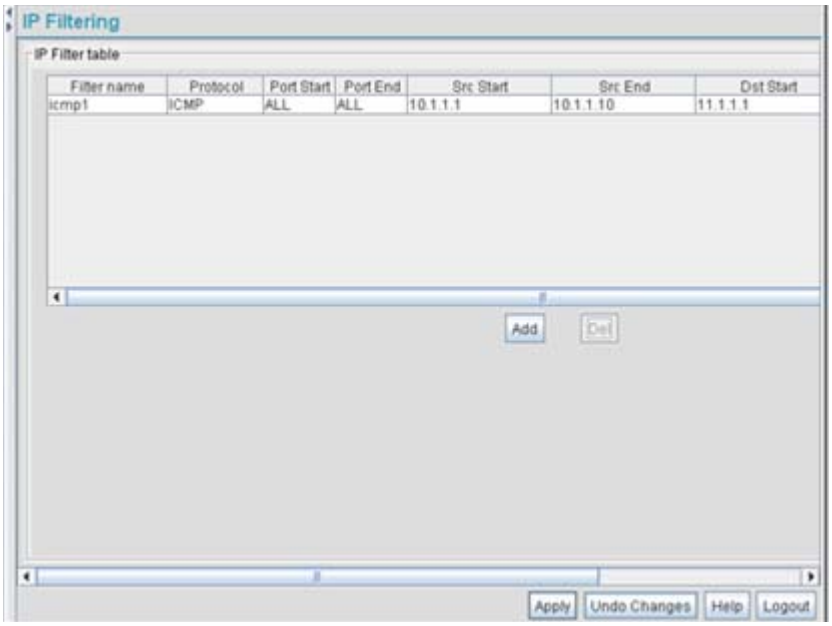
Creating a global filter

A global filter contains IP packet parameters that need to be matched where the filter is applied. These parameters include protocol number (TCP, ICMP etc.), port range, source IP range and destination IP range. Though an IP filter can be created using either the access point applet or CLI, the following example uses the CLI:

```
admin(network.ipfilter)>add icmp1 ICMP ALL ALL 10.1.1.1 10.1.1.10 11.1.1.1
11.1.1.10

admin(network.ipfilter)>show
-------------------------------------------------------------------------------
Idx Name        Protocol Port-Start-End SrcIP-Start-End DstIP-Start-End In-Use
-------------------------------------------------------------------------------
1   icmp1       ICMP     ALL            10.1.1.1        11.1.1.1        NO
                                        10.1.1.10       11.1.1.10
admin(network.ipfilter)>
```

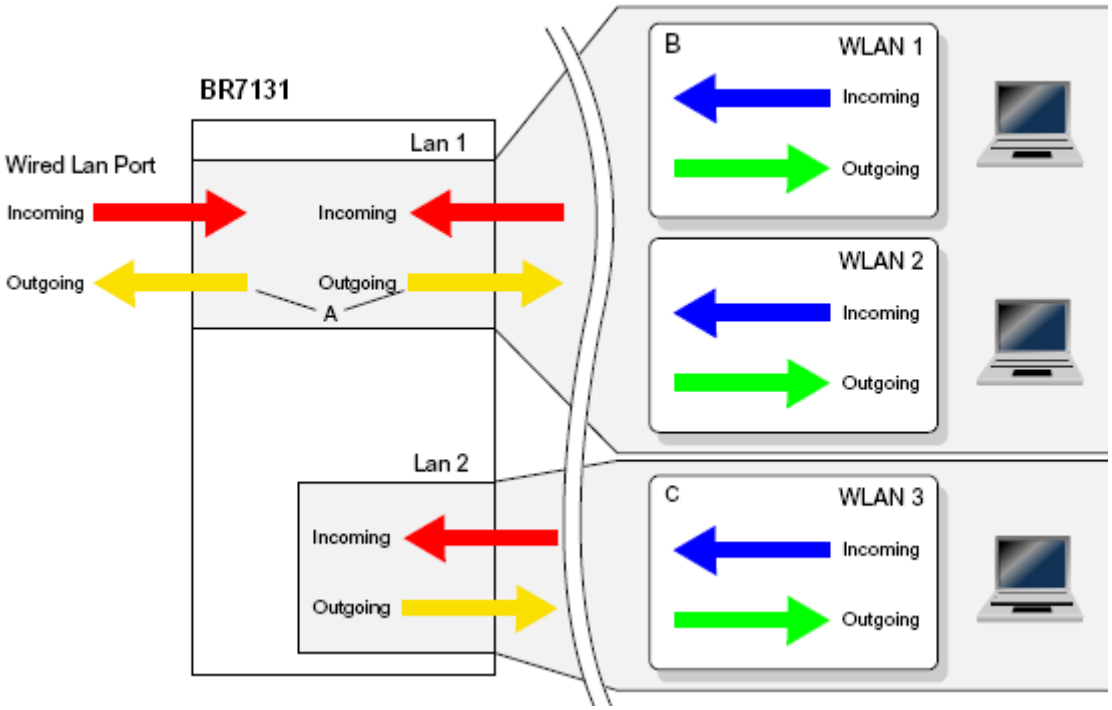
Once created, the filter displays within the *Network Configuration -> IP Filtering* screen.



Applying the filter to a WLAN or LAN

Once created, filters in the IP Filter Table can be applied to a WLAN or LAN. Refer to the following diagram to illustrate this point

NOTE
When both LAN IP filtering and WLAN IP filtering are enabled, a packet must pass the criteria of both LAN *and* WLAN filter policies.



Adding a filter to LAN 1 for outbound traffic results in the inspection of packets at point A. Both packets out the physical port and wireless transmissions are checked. Adding a filter to WLAN 1 for inbound traffic results in the inspection of packets at point B. Even though WLAN 2 is on LAN 1, its packets are unaffected. Adding a filter to WLAN 3 for inbound traffic results in the inspection of packets at point C.

Default rules must also be set upon enabling IP filtering on a LAN or WLAN. By default, when IP filtering is enabled, all inbound and outbound traffic is disabled. Default filters are applied when no other applied filter is matched.

When applying multiple filters, the filter which matches first is applied. In this sense the filter priority is the order of the list from top to bottom.

Creating a WLAN IP filter policy

The following example uses the access point CLI:

```
admin(network.wireless.wlan.ipfpolicy)>set mode 1 enable
admin(network.wireless.wlan.ipfpolicy)>add 1 icmp1 incoming deny
admin(network.wireless.wlan.ipfpolicy)>show 1

-------------------------------------------------------------------------
Idx Filter-Name          Direction      Action
-------------------------------------------------------------------------
1   icmp1                 incoming      deny

IP Filter Mode                      : enable
Default Incoming Action             : allow
Default Outgoing Action             : allow
admin(network.wireless.wlan.ipfpolicy)>
```

Creating a LAN IP Filter Policy

The following example uses the access point CLI:

```
admin(network.lan.ipfpolicy)>add 1 icmp1 incoming deny
admin(network.lan.ipfpolicy)>show 1
-----------------------------------------------------------------
Idx Filter-Name          Direction      Action
-----------------------------------------------------------------
1   icmp1                 incoming      deny

IP Filter Mode                    : enable
Default Incoming Action           : deny
Default Outgoing Action           : deny
admin(network.lan.ipfpolicy)>
```

NOTE
For information on applying a filter to a WLAN or LAN using the access point GUI applet, see, "Applying a filter to LAN1, LAN2 or a WLAN (1-16)" on page 184.

Assessing IP filter stats

Detailed IP filter statistics can be displayed as follows from the access point CLI:

```
admin(stats)>show s-wlan 1

Name                            : joe
ESSID                           : joe
Authentication                  : No Authentication
Encryption                      : No Encryption
Radio/s                         : 802.11a, 802.11b/g
Number of Associated Clients    : 1

Traffic Information:

Packets per second:
Rx                 : 0 pps
Tx                              : 0 pps
Total                           : 0 pps

<Hit any key to continue>
Throughput:
Rx                              : 0.00 Mbps
Tx                              : 0.00 Mbps
Total                           : 0.00 Mbps
Average Bit Speed               : 0.00 Mbps
%Non-Unicast Packets            : 0.00 %

RF Status:
Avg MU Signal                   : 0.0 dBm
Avg MU Noise                    : 0.0 dBm
Avg MU Signal-to-Noise          : 0.0 dB


Error Information:
Average Number of Retries       : 0.00 Retries
Dropped Packets                 : 0.00 %
%Undecryptable Packets          : 0.00 %

IP Filtering:
Incoming:
icmp1                           : 0 denied
Default Action                  : 64 allowed
```

```
Outgoing:
Default Action                : 75 allowed

admin(stats)>show lan 1

LAN Interface Information
LAN Interface 1                   : enable
IP Address 1                      : 192.168.0.1
Network Mask                      : 255.255.255.0
Ethernet Address                  : 0015700078C5
Speed                             : 100 Mbps
Duplex                            : full

LAN Rx Information
rx packets                        : 12520
rx bytes                          : 2663360
rx errors                         : 0
rx dropped                        : 0
Rx Overruns                       : 0
Rx Frame Errors                   : 0

LAN Tx Information
tx packets                        : 7105
tx bytes                          : 3236256
tx errors                         : 0
tx dropped                        : 0
Tx Overruns                       : 0
Tx Carrier Errors                 : 0

WLANs on this LAN :

IP Filtering:
Incoming:
icmp1                         : 0 denied
Default Action                : 0 denied
Outgoing:
Default Action                : 0 denied
```

Chapter

Configuring Access Point Security

6

In this chapter

- Configuring security options 192
- Setting passwords 192
- Enabling authentication and encryption schemes 194
- Configuring Kerberos authentication 196
- Configuring 802.1x EAP authentication 198
- Configuring WEP encryption 202
- Configuring KeyGuard encryption 204
- Configuring WPA/WPA2 using TKIP 206
- Configuring WPA2-CCMP (802.11i) 208
- Configuring firewall settings 213
- Configuring VPN tunnels 220
- Configuring content filtering settings 235
- Configuring rogue AP detection 238
- Configuring user authentication 245

Security measures for the Brocade Mobility 7131 Series Access Point and its WLANs are critical. Use the available Brocade Mobility 7131 Series Access Point security options to protect the Brocade Mobility 7131 Series Access Point LAN from wireless vulnerabilities, and safeguard the transmission of RF packets between the Brocade Mobility 7131 Series Access Point and its associated clients.

WLAN security can be configured on an ESS by ESS basis on the Brocade Mobility 7131 Series Access Point. Sixteen separate ESSIDs (WLANs) can be supported on a Brocade Mobility 7131 Series Access Point, and must be managed (if necessary) between the 802.11a/n and 802.11b/g/n 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 Brocade Mobility 7131 Series Access Point can also create VPN tunnels to securely route traffic through a IPSEC tunnel and block transmissions with devices interpreted as Rogue APs.

NOTE
Security for the Brocade Mobility 7131 Series Access Point can be configured in various locations throughout the Brocade Mobility 7131 Series Access Point menu structure. This chapter outlines the security options available to the Brocade Mobility 7131 Series Access Point, and the menu locations and steps required to configure specific security measures.

Configuring security options

To configure the data protection options available on the Brocade Mobility 7131 Series Access Point, refer to the following:

- To set an administrative password for secure Brocade Mobility 7131 Series Access Point logins, see "Setting passwords" on page 192.
- To display security policy screens used to configure the authetication and encryption schemes available to the Brocade Mobility 7131 Series Access Point, see "Enabling authentication and encryption schemes" on page 194. 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 198.
- To define a security policy supporting Kerberos, see, "Configuring Kerberos authentication" on page 196.
- To create a security policy supporting WEP, see "Configuring WEP encryption" on page 202.
- To configure a security policy supporting KeyGuard, see, "Configuring KeyGuard encryption" on page 204.
- To define a security policy supporting WPA-TKIP, see "Configuring WPA/WPA2 using TKIP" on page 206.
- To create a security policy supporting WPA2-CCMP, see "Configuring WPA2-CCMP (802.11i)" on page 208.
- To create WLANs with same SSID but different BSSIDs and security schemes, see "Configuring multi cipher support" on page 211.
- To configure the Brocade Mobility 7131 Series Access Point to block specific kinds of HTTP, SMTP and FTP data traffic, see "Configuring firewall settings" on page 213.
- To create VPN tunnels allowing traffic to route securely through a IPSEC tunnel to a private network, see "Configuring VPN tunnels" on page 220.
- To configure the Brocade Mobility 7131 Series Access Point to block transmissions with devices detected as Rogue AP's (hostile devices), see "Configuring rogue AP detection" on page 238.

Setting passwords

Before setting the Brocade Mobility 7131 Series Access Point security parameters, verify an administrative password for the Brocade Mobility 7131 Series Access Point has been created to restrict access to the device before advanced device security is configured.

To password protect and restrict Brocade Mobility 7131 Series Access Point device access:

1. Connect a wired computer to the Brocade Mobility 7131 Series Access Point 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 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.

To connect to the access point, the IP address is required. If connected to the access point using the WAN port, the default static IP address is 10.1.1.1. The default password is "*admin123*." If connected to the access point using the LAN port, the default setting is DHCP client. The user is required to know the IP address to connect to the access point using a Web browser.

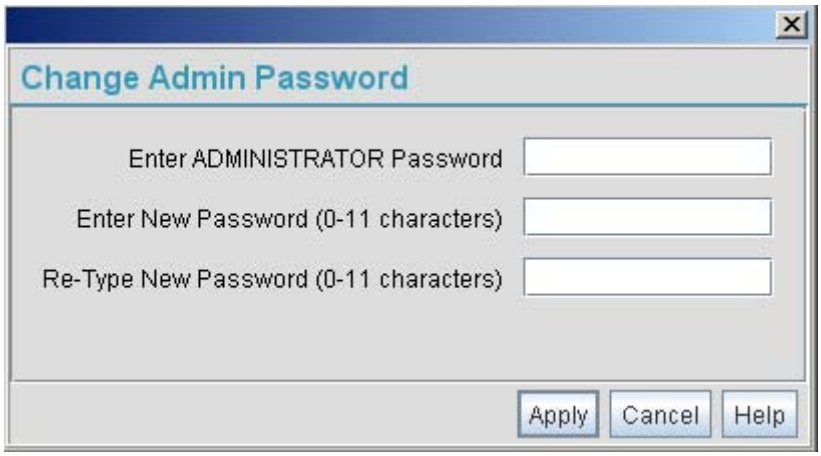
The Brocade Mobility 7131 Series Access Point Login screen displays.

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 Brocade Mobility 7131 Series Access Point. The user is required to enter a numerical IP address.

4. Log in using the "*admin*" as the default Username and "*admin123*" 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.



CAUTION

Restoring the access point's configuration back to default settings changes the administrative password back to "admin123." If restoring the configuration back to default settings, be sure you change the administrative password accordingly.

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 Brocade Mobility 7131 Series Access Point has not had its System Settings (device name, location etc.) configured, see "Configuring system settings" on page 63.

   Once the password has been set, refer back to "Configuring security options" on page 192 to determine which Brocade Mobility 7131 Series Access Point security feature to configure next.

Resetting the access point password

The access point has a means of restoring its password to its default value. Doing so also reverts the access point's security, radio and power management configuration to their default settings. Only an installation professional should reset the access point's password and promptly define a new restrictive password.

To contact Brocade Support in the event of a password reset requirement, go to *www.brocade.com/support*.

CAUTION

Only a qualified installation professional should set or restore the access point's radio and power management configuration in the event of a password reset.

Enabling authentication and encryption schemes

To complement the built-in firewall filters on the WAN side of the Brocade Mobility 7131 Series Access Point, the WLAN side of the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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 a Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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 authetnication or encryption checkbox displays a configuration field for the selected security scheme within the *New Security Policy* screen.

NOTE
An existing security policy can be edited from the Security Configuration screen by selecting an existing policy and clicking the *Edit* button. Use the *Edit Security Policy* screen to edit the policy. For more information on editing an existing security policy, refer to security configuration sections described in steps 4 and 5.

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. Brocade 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.
802.1x EAP	Select the *802.1x EAP* button to display the *802.1x EAP Settings* field within the New Security Policy screen.

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 Brocade Mobility 7131 Series Access Point. 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 202.
WEP 128 (104-bit key)	Select the *WEP 128 (104 bit key)* button to display the *WEP 128 Settings* field within the New Security Policy screen.
KeyGuard	Select the *KeyGuard* button to display the *KeyGuard Settings* field within the New Security Policy screen.
WPA/WPA2 TKIP	Select the *WPA/WPA2 TKIP* button to display the *WPA/TKIP Settings* field within the New Security Policy screen.
WPA2/CCMP (802.11i)	Select the *WPA2/CCMP (802.11)* button to display the *WPA2/CCMP Settings* field within the New Security Policy screen.

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:

Brocade Mobility 7131 Series Access Point authentication:

- To create a security policy supporting Kerberos, see, "Configuring Kerberos authentication" on page 196.

- To define a security policy supporting 802.1x EAP, see "Configuring 802.1x EAP authentication" on page 198.

Brocade Mobility 7131 Series Access Point encryption:

- To create a security policy supporting WEP, see "Configuring WEP encryption" on page 202.
- To define a security policy supporting KeyGuard, see, "Configuring KeyGuard encryption" on page 204.
- To configure a security policy supporting WPA/TKIP, see "Configuring WPA/WPA2 using TKIP" on page 206.
- To create a security policy supporting WPA2/CCMP, see "Configuring WPA2-CCMP (802.11i)" on page 208.

7. Click *Cancel* to return to the target WLAN screen without keeping any of the changes made within the New Security Policy screen.

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 access point with Brocade 802.11b 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* checkbox be selected for authentication to function properly. See "Configuring network time protocol (NTP)" on page 99 to configure the NTP server.

NOTE

If 802.11a/n is selected as the radio used for a specific WLAN, the WLAN cannot use a Kerberos supported security policy, as no Brocade 802.11a/n clients can support Kerberos.

To configure Kerberos on the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point 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.

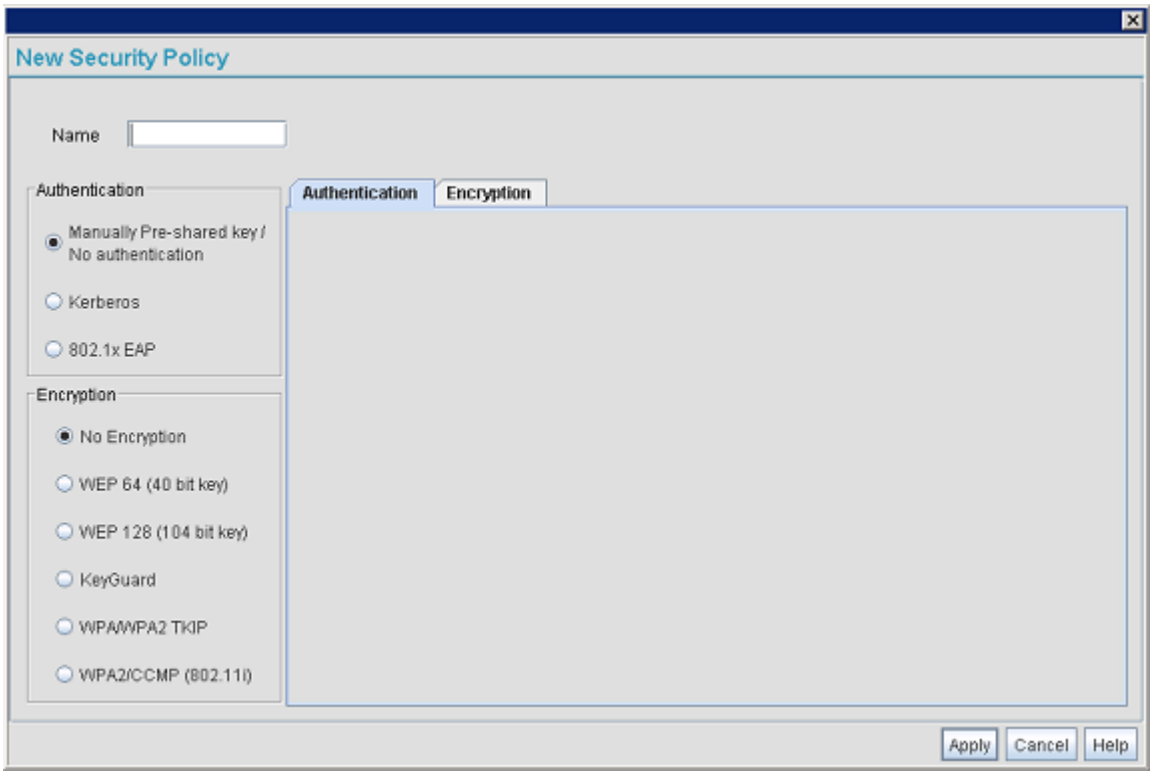
2. Click the *Create* button to configure a new policy supporting Kerberos.

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 Brocade Mobility 7131 Series Access Point.

Realm Name	Specify a realm name that is case-sensitive, for example, BROCADE.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.
Primary KDC	Specify a numerical (non-DNS) IP address and port for the primary *Key Distribution Center (KDC).* The KDC implements an Authentication Service and a Ticket Granting Service, whereby an authorized user is granted a ticket encrypted with the user's password. The KDC has a copy of every user password.
Backup KDC	Optionally, specify a numerical (non-DNS) IP address and port for a backup KDC. Backup KDCs are referred to as slave servers. The slave server periodically synchronizes its database with the primary (or master) KDC.

Remote KDC	Optionally, specify a numerical (non-DNS) IP address and port for a remote KDC. Kerberos implementations can use an administration server allowing remote manipulation of the Kerberos database. This administration server usually runs on the KDC.
Port	Specify the ports on which the Primary, Backup and Remote KDCs reside. The default port number for Kerberos Key Distribution Centers is Port 88.

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.

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 Brocade Mobility 7131 Series Access Point passes EAP packets from the client to an authentication server on the wired side of the Brocade Mobility 7131 Series Access Point. All other packet types are blocked until the authentication server (typically, a Radius server) verifies the Client's identity.

To configure 802.1x EAP authentication on the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point menu tree.

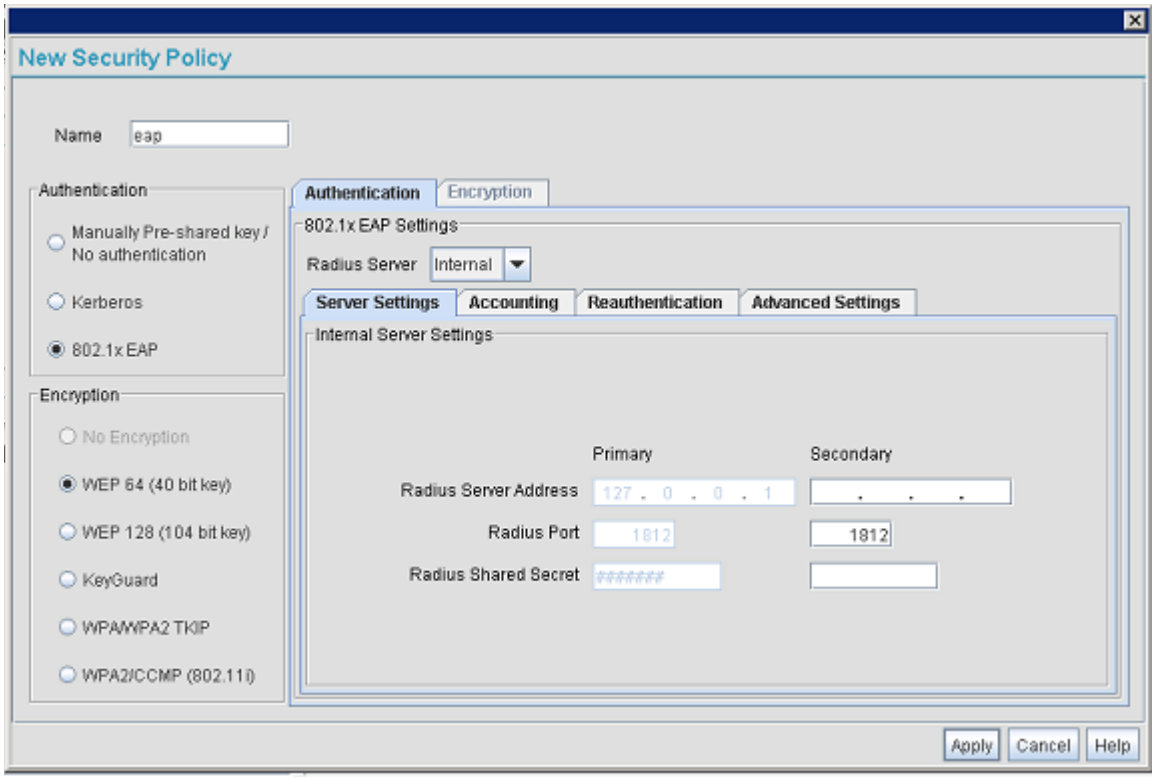
   If security policies supporting 802.1x EAP exist, they appear within the *Security Configuration* screen. These existing policies can be used as is, or their properties edited by clicking the *Edit* button. To configure a new security policy supporting 802.1x EAP, continue to step 2.
2. Click the *Create* 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 Setting*s 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. If using the access point's Internal Radius server, leave the *Radius Server* drop-down menu in the default setting of *Internal*. If an external Radius server is used, select *External* from the drop-down menu.

CAUTION

If using external radius authentication with admin users, and the connectivity to the Radius server is lost, the values will revert to local authentication.



6. Configure the *Server Setting*s field as required to define address information for the authentication server. The appearance of the Server Settings field varies depending on whether Internal or External has been selected from the Radius Server drop-down menu.

Radius Server Address	If using an External Radius Server, 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. This setting is not available if Internal has been selected from the Radius Server drop-down menu.

RADIUS Port	If using an External Radius Server, 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. This setting is not available if Internal has been selected from the Radius Server drop-down menu.
RADIUS Shared Secret	Specify a shared secret for authentication on the Internal or Primary Radius server (External Radius Server only). 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 and numbers. 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.

7. Select the *Accounting* tab as required to define a timeout period and retry interval Syslog for clients interoperating with the Brocade Mobility 7131 Series Access Point and EAP authentication server. The items within this tab could be enabled or disabled depending on whether Internal or External has been selected from the Radius Server drop-down menu.

External Radius Server Address	Specify the IP address of the external Radius server used to provide Radius accounting.
External Radius Port	Specify the port on which the Radius server is listening. The default port is 1813.
External Radius Shared Secret	Specify a shared secret for authentication. The shared secret is required to match the shared secret on the Radius server.
Client Timeout	Specify the time (in seconds) for the access point's retransmission of EAP-Request packets. The default is 10 seconds. If this time is exceeded, the authentication session is terminated.
Retries	Specify the number of retries for the Client to retransmit a missed frame to the Radius server before it times out of the authentication session. The default is 2 retries.
Enable Syslog	Select the *Enable Syslog* checkbox to enable Radius accounting syslog messages relating to EAP events to be written to the specified syslog server.
Syslog Server IP Address	Enter the IP address of the destination syslog server to be used to log EAP events.

8. Select the *Reauthentication* tab as required to define authentication connection policies, intervals and maximum retries. The items within this tab are identical regardless of whether Internal or External is selected from the Radius Server drop-down menu.

Enable Reauthentication	Select the *Enable Reauthentication* checkbox to configure a wireless connection policy so clients 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 interval 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 default interval of 3600 seconds is recommended.
Max. Retries (1-99) retries	Define the maximum number of Client 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.

NOTE
The default values described are the recommended values. Do not change these values unless consulted otherwise by an administrator.

9. Select the *Advanced Setting*s tab as required to specify a Client quiet period, timeout interval, transmit period, and retry period for clients and the authentication server. The items within this tab are identical regardless of whether Internal or External is selected from the Radius Server drop-down menu.

Client Quiet Period (1-65535) secs	Specify an idle time (in seconds) between Client authentication attempts, as required by the authentication server. The default is 10 seconds.
Client Timeout (1-255) secs	Define the time (in seconds) for the access point's retransmission of EAP-Request packets. The default is 10 seconds.
Client Tx Period (1-65635) secs	Specify the time period (in seconds) for the access point's retransmission of the EAP Identity Request frame. The default is 5 seconds.
Client Max Retries (1-10) retries	Specify the maximum number of times the access point retransmits an EAP-Request frame to the client before it times out the authentication session. The default is 2 retries.
Server Timeout (1-255) secs	Specify the time (in seconds) for the access point's retransmission of EAP-Request packets to the server. The default is 5 seconds. If this time is exceeded, the authetnication session is terminated.
Server Max Retries (1-255 retries)	Specify the maximum number of times for the access point to retransmit an EAP-Request frame to the server before it times out the authentication session. The default is 2 retries.

10. 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.
11. 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.

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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point 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.

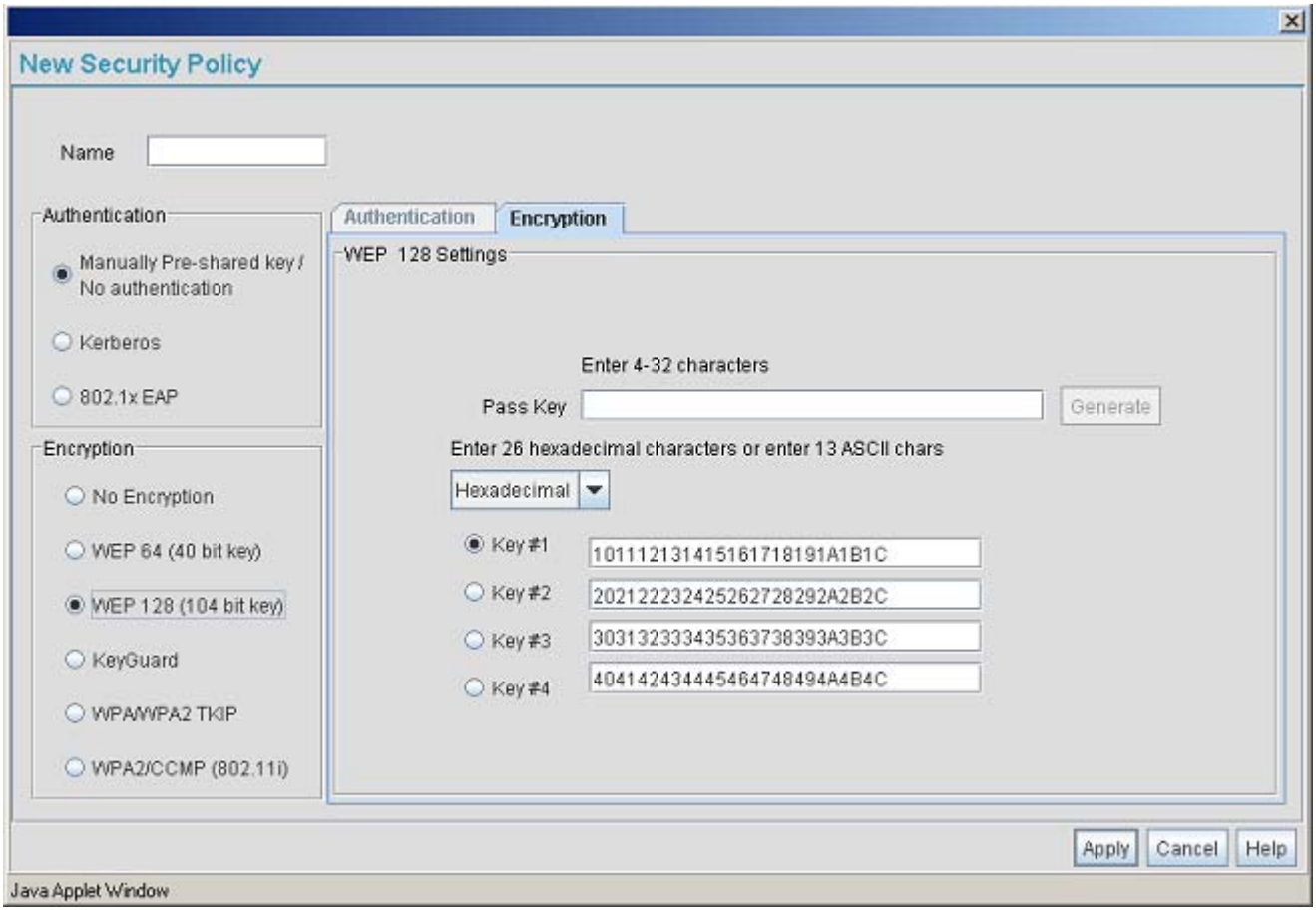
2. Click the *Create* button to configure a new policy supporting WEP.

   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 Setting*s or *WEP 128 Setting*s 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 Setting*s or *WEP 128 Setting*s field as required to define the Pass Key used to generate the WEP keys. These keys must be the same between the access point and its Client 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 Brocade Mobility 7131 Series Access Point, other proprietary routers and Motorola clients use the algorithm to convert a string to the same hexadecimal number. Clients without Brocade adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys #1-4	Use the *Key #1-4* areas to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for activation by clicking its radio button.

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.

Configuring KeyGuard encryption

KeyGuard is a proprietary encryption method. KeyGuard is an 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.

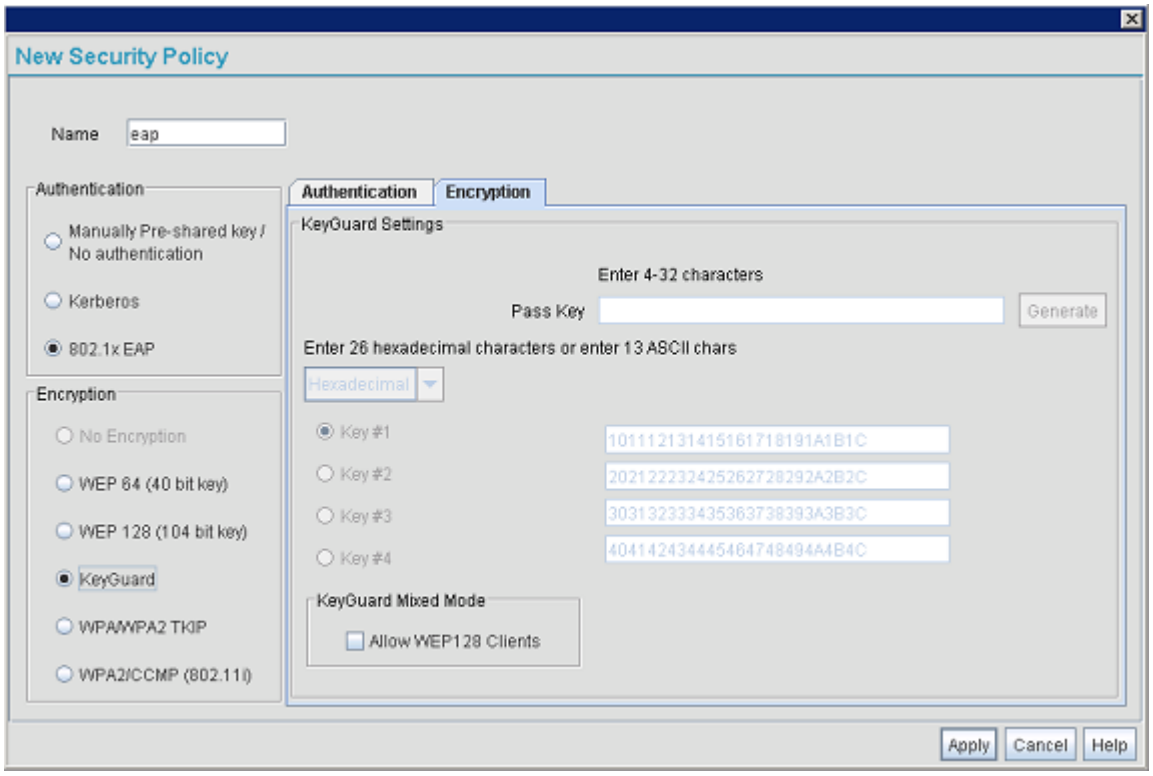
WPA2-CCMP (not KeyGuard) offers the highest level of security among the encryption methods available with the Brocade Mobility 7131 Series Access Point.

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point menu tree.

   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 Setting*s 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 access point and its Client 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 Brocade Mobility 7131 Series Access Point, other proprietary routers, and Motorola clients use the algorithm to convert a string to the same hexadecimal number. Clients without Brocade adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys #1-4	Use the *Key #1-4* areas to specify key numbers. The keys are 26 hexadecimal characters in length. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for KeyGuard include:

Key 1	101112131415161718191A1B1C
Key 2	20212223242526272829 2A2B2C
Key 3	303132333435363738393A3B3C
Key 4	404142434445464748494A4B4C

6. Select the *Allow WEP128 Clients* checkbox (from within the *KeyGuard Mixed Mode* field) to enable WEP128 clients to associate with an access point's KeyGuard supported WLAN. The WEP128 clients must use the same keys as the KeyGuard clients to interoperate within the access point's KeyGuard supported WLAN.

7. Click the *Apply* button to save any changes made within the KeyGuard Setting field of the New Security Policy screen.
8. 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.

Configuring WPA/WPA2 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.

The 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.

Wi-Fi Protected Access 2 (WPA2) is an enhanced version of WPA. WPA2 uses the *Advanced Encryption Standard* (AES) instead of TKIP. AES supports 128-bit, 192-bit and 256-bit keys.

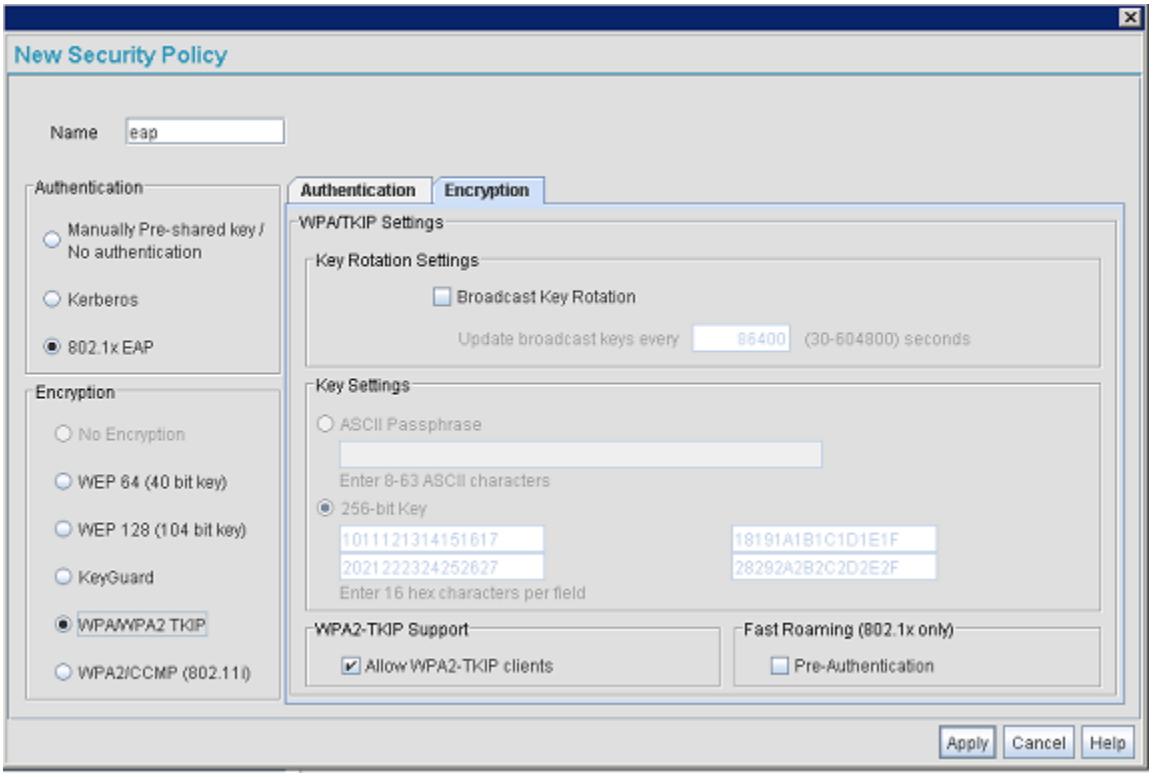
WPA/WPA2 also provide strong user authentication based on 802.1x EAP. To configure WPA/WPA2 encryption on the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point 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/WPA2 TKIP* radio button.

   The *WPA/TKIP Setting*s 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 Setting*s area as needed to broadcast encryption key changes to clients and define the broadcast interval.

Broadcast Key Rotation	Select the *Broadcast Key Rotation* checkbox to enable or disable broadcast key rotation. When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated on every interval specified in the Broadcast Key Rotation Interval. Enabling broadcast key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.
Update broadcast keys every (300-604800 seconds)	Specify a time period in seconds to rotate the key index used for the broadcast key. Set the interval to a shorter duration like 3600 seconds for tighter broadcast traffic security on the wireless LAN. Set the interval to a longer duration like 86400 seconds for less broadcast traffic security requirements. Default value is 86400 secs.

6. Configure the *Key Setting*s area as needed to set an ASCII Passphrase and key values.

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 Brocade Mobility 7131 Series Access Point 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 WPA/TKIP include:

1011121314151617

18191A1B1C1D1E1F

2021222324252627

28292A2B2C2D2E2F

7. Enable *WPA2-TKIP Support* as needed to allow WPA2 and TKIP client interoperation.

Allow WPA2-TKIP clients	WPA2-TKIP support enables WPA2 and TKIP clients to operate together on the network.

8. Configure the *Fast Roaming (802.1x only)* field as required to enable additional Brocade Mobility 7131 Series Access Point roaming and key caching options. This feature is applicable only when using 802.1x EAP authentication with WPA2-TKIP.

Pre-Authentication	Selecting this option enables an associated Client to carry out an 802.1x authentication with another Brocade Mobility 7131 Series Access Point before it roams to it. The Brocade Mobility 7131 Series Access Point caches the keying information of the client until it roams to the other Brocade Mobility 7131 Series Access Point. 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 and WPA2-TKIP is enabled.
Opportunistic PMK Caching	Select the *Opportunistic Pairwise Master Key* (PMK) Caching option to reduce handoff latency by pre-establishing security associations between a client and the Mobility 7131 series access points in a wireless network.

NOTE
PMK key caching is enabled internally by default for WPA2-TKIP when 802.1x EAP authentication is enabled.

9. Click the *Apply* button to save any changes made within this New Security Policy screen.
10. 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.

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 Brocade Mobility 7131 Series Access Point provides.

To configure WPA2-CCMP on the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless -> Security* from the Brocade Mobility 7131 Series Access Point 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.

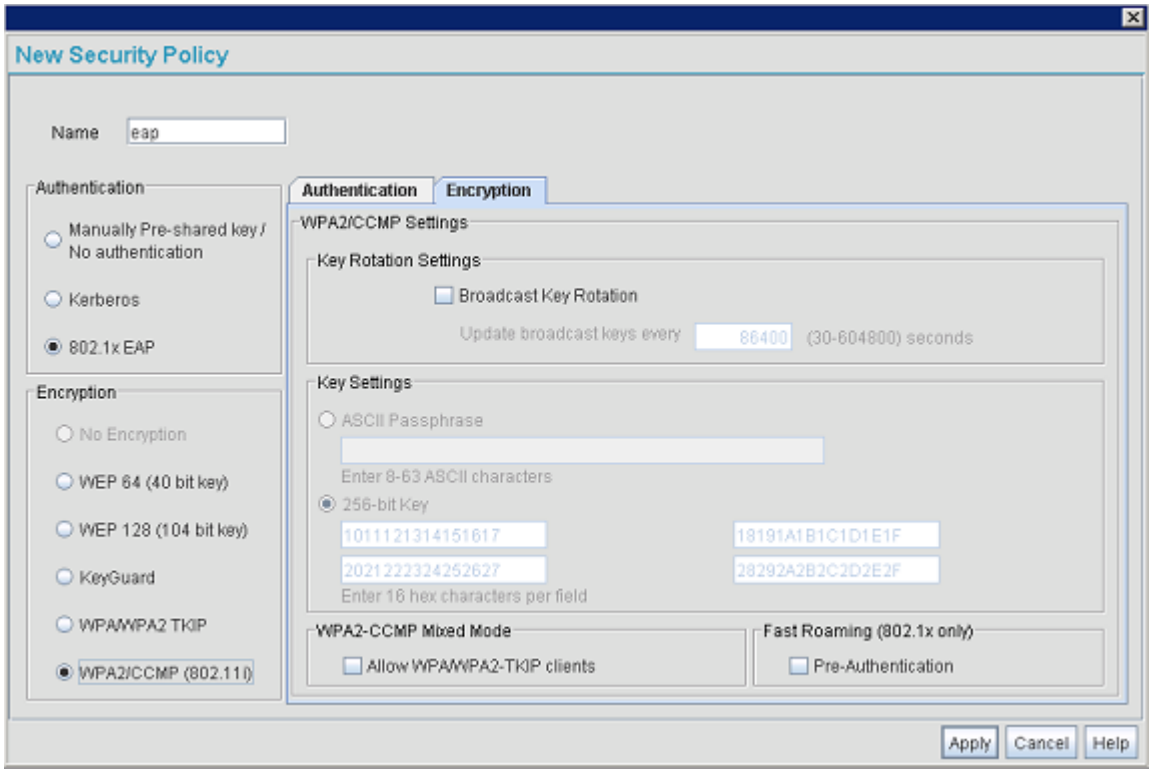
2. Click the *Create* button to configure a new policy supporting WPA2-CCMP.

   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 broadcast key rotation. When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated on every interval specified in the Broadcast Key Rotation Interval. Enabling broadcast key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.
Update broadcast keys every (300-604800 seconds)	Specify a time period in seconds to rotate the key index used for the broadcast key. Set the interval to a shorter duration like 3600 seconds for tighter broadcast traffic security on the wireless LAN. Set the interval to a longer duration like 86400 seconds for less broadcast traffic security requirements. Default value is 86400 secs.

6. Configure the *Key Setting*s 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 Brocade Mobility 7131 Series Access Point 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 WPA and WPA2 TKIP client interoperation.

Allow WPA/WPA2-TKIP clients	WPA2-CCMP Mixed Mode enables WPA2-CCMP, WPA-TKIP and WPA2-TKIP clients to operate together on the network. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. Brocade recommends enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate within a WLAN populated by WPA2-CCMP enabled clients.

8. Configure the *Fast Roaming (802.1x only)* field as required to enable additional Brocade Mobility 7131 Series Access Point roaming and key caching options.

Pre-Authentication	Selecting this option enables an associated Client to carry out an 802.1x authentication with another Brocade Mobility 7131 Series Access Point before it roams to it. The Brocade Mobility 7131 Series Access Point caches the keying information of the client until it roams to the other Brocade Mobility 7131 Series Access Point. 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.
Opportunistic PMK Caching	Select the *Opportunistic Pairwise Master Key* (PMK) Caching option to reduce handoff latency by pre-establishing security associations between a client and the Mobility 7131 access points in the wireless network.

NOTE
PMK key caching is enabled internally by default when 802.1x EAP authentication is enabled.

9. Click the *Apply* button to save any changes made within this 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.

Configuring multi cipher support

The access point's Multi Cipher allows legacy and new clients (Wi-Fi handheld devices) within the same WLAN. Multi cipher extends the access point's existing WLAN security options by allowing dynamic WEP and 802.11i configurations to co-exist, and allowing multiple security policies to be associated with the same ESSID on different WLANs. Within such an environment, legacy clients are capable of WEP, while new clients are capable of WPA/2-TKIP and WPA2-CCMP encryption. This particular form of multi cipher (security) support helps maintain the co-existence of Dynamic WEP and 802.11i based environments.

To support this feature, certain security policy combinations need to be available on a per-WLAN basis. The following combinations are supported:

- WEP 64 and WPA/WPA2-TKIP
- WEP 64 and WPA2-CCMP
- WEP 128 and WPA/WPA2-TKIP
- WEP 128 and WPA2-CCMP
- WPA2-CCMP and WPA/WPA2-TKIP

To configure multi cipher support, WLANs should be created with the same ESSID, but different BSSIDs and security schemes. This results in the AP announcing different beacons for the same ESSID. Clients can then select a corresponding BSSID to associate, depending on their individual configurations.

From the client's point of view, the scenario is as if there are two APs available with same ESSID, but different security policies. The client can choose an appropriate AP based on its configuration.

NOTE
Multi Cipher is supported in adaptive mode (AAP), provided the required configuration is allowed on switch.

Configuring multi cipher support requires:

- Creating WLANs with the same ESSID, but different BSSIDs and security schemes. This results in the AP beaconing the same ESSID, but a different BSSID.
- Each WLAN having a unique WLAN name. If a WLAN's name is same as the ESSID, it's difficult to distinguish them when doing WLAN-BSSID grouping.
- Not using WLANs with same ESSID and security scheme. If this were to be deployed, beacons will contain the same ESSID and security scheme data, but different BSSIDs would be generated, potentially confusing clients.
- Ensuring WLANs with the same ESSID use the same authentication method(s) in their security policies.
- WLANs with the same ESSID not use both WEP64 and WEP128 as security schemes. If both are defined for the same ESSID, clients configured with WEP could be associated with the wrong WLAN and fail to get an IP address.

NOTE
Since the AP supports a maximum of 4 different BSSID groups, Brocade recommends grouping WLANs with common security schemes under the same BSSID group to support a greater number of WLANs.

To configure multiple cipher support:

1. Create a WLAN supporting WEP64 as its security scheme.

   For information on how to create or edit a WLAN and assign it a security scheme, see "Creating/editing individual WLANs" on page 139.

   For information on how to assign a WLAN a security policy supporting WEP, see "Configuring WEP encryption" on page 202.

2. Create a second WLAN with the same ESSID as the WLAN created in step 1. However, assign the second WLAN a security policy supporting WPA2-CCMP.

   For information on how to assign a WLAN a security policy supporting WEP, see "Configuring WPA2-CCMP (802.11i)" on page 208.

   NOTE
   Ensure the WLANs created in steps 1 and 2 have unique names assigned.

3. Map the WLANs created in steps 1 and 2 to different BSSID groups.

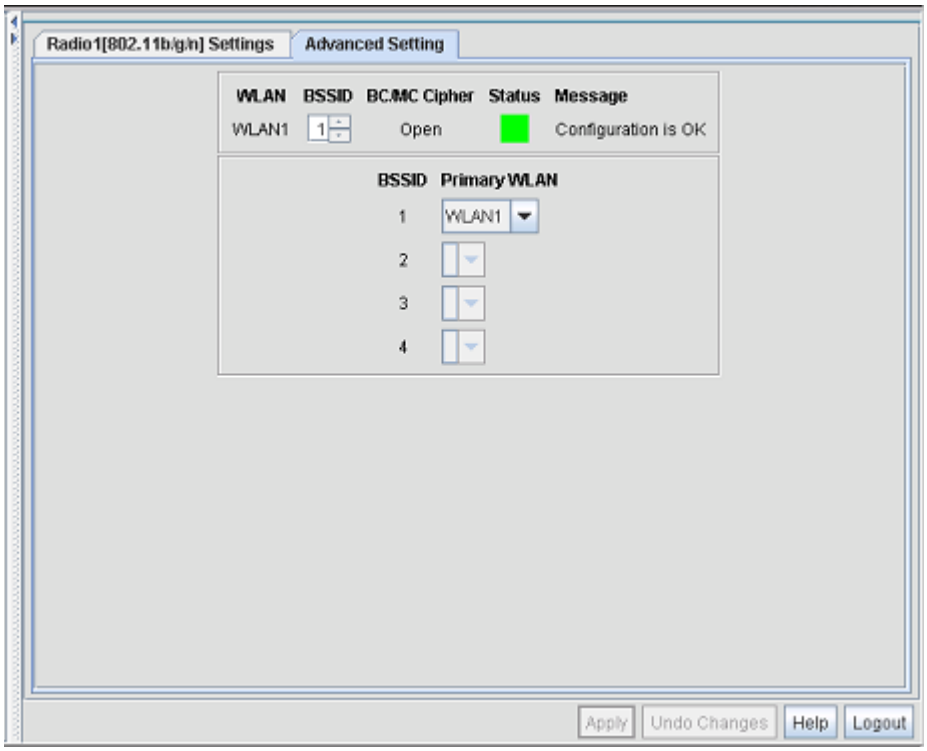
   a. Select *Network Configuration -> Wireless -> Radio Configuration -> Radio1 or Radio 2* from the access point's menu tree.

   b. Select the *Advanced Setting*s tab.

   c. MAP BSSIDs (4 BSSIDs are available for mapping) to WLANs. For additional information on how to MAP BSSIDs to WLANs, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

CAUTION

When WLANs with WEP64/WEP128/TKIP/CCMP cipher suites are in the same BSSID group, a common cipher for the group encryption key cannot be set. Brocade recommends grouping WLANs strategically into different BSSID groups. The status field in the WLAN-BSSID group mapping displays whether the WLANs in a particular BSSID group are up or not.



This results in the AP beaconing the same ESSID but different WLAN BSSIDs and security schemes.

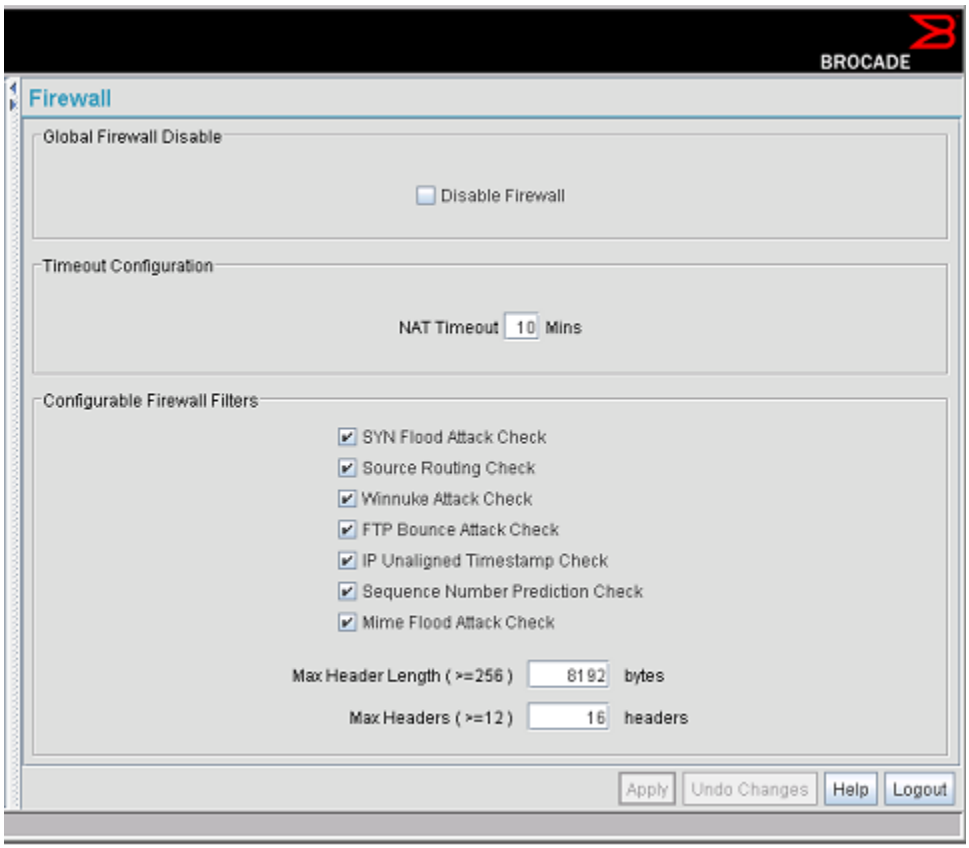
Configuring firewall settings

The Brocade Mobility 7131 Series Access Point's firewall is a set of related programs located in the gateway on the WAN side of the Brocade Mobility 7131 Series Access Point. The firewall uses a collection of filters to screen information packets for known types of system attacks. Some of the Brocade Mobility 7131 Series Access Point's filters are continuously enabled, others are configurable.

Use the Brocade Mobility 7131 Series Access Point'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 Brocade Mobility 7131 Series Access Point firewall settings:

1. Select *Network Configuration -> Firewall* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Global Firewall Disable* field to enable or disable the Brocade Mobility 7131 Series Access Point firewall.

Disable Firewall	Select the *Disable Firewall* checkbox to disable all firewall functions on the Brocade Mobility 7131 Series Access Point. This includes firewall filters, NAT, VP, content filtering, and subnet access. Disabling the Brocade Mobility 7131 Series Access Point firewall makes the Brocade Mobility 7131 Series Access Point vulnerable to data attacks and is not recommended during normal operation if using the WAN port.

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 Brocade Mobility 7131 Series Access Point 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:

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.
Max Header Length (>=256)	Use the *Max Header Length* field to set the maximum allowable header length (at least 256 bytes).
Max Headers (>=12)	Use the *Max Headers* field to set the maximum number of headers allowed (at least 12 headers).

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 Access Point applet. A prompt displays confirming the logout before the applet is closed.

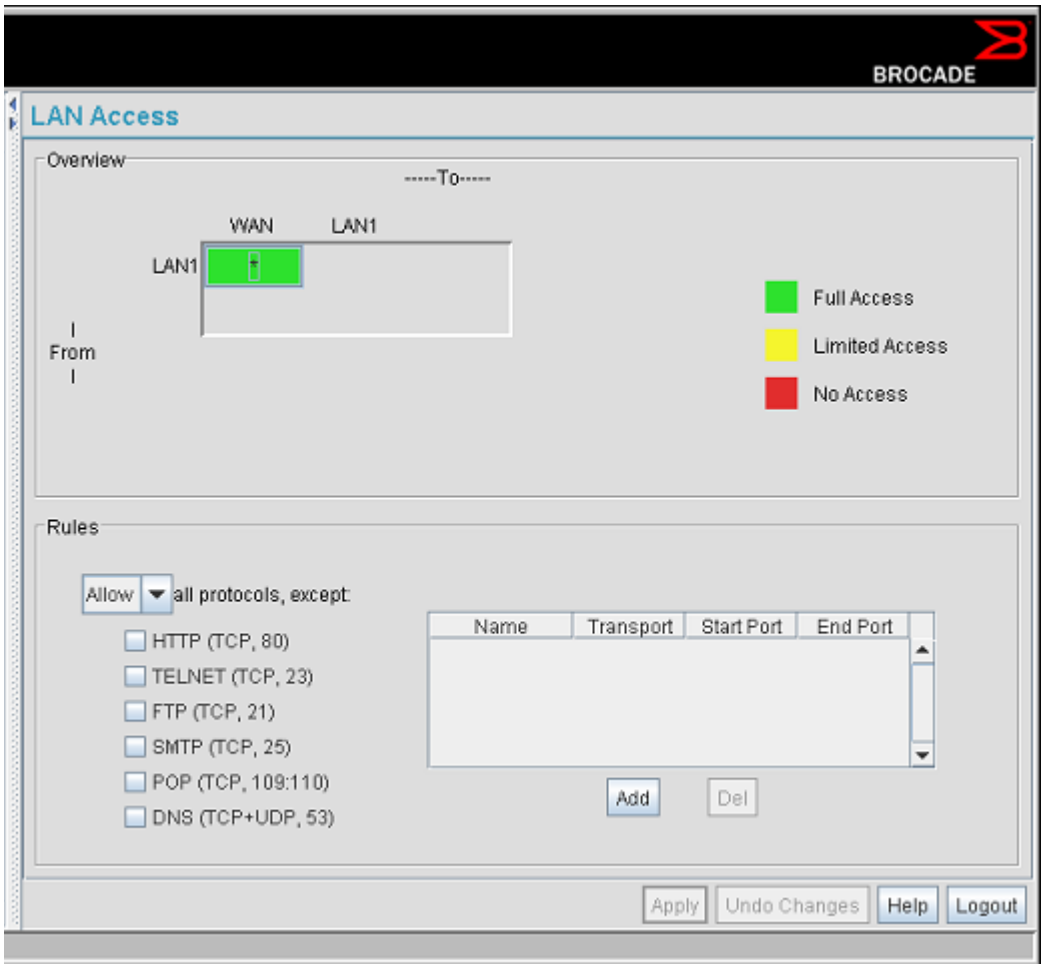
Configuring LAN to WAN access

The Brocade Mobility 7131 Series Access Point LAN can be configured to communicate with the WAN side of the Brocade Mobility 7131 Series Access Point. Use the *Subnet Access* screen to control access from the LAN1 (or LAN2) interfaces to the WAN interface. This access level will function as an ACL in a router to allow/deny certain IP addresses or subnets to access certain interfaces (or subnets belonging to those interfaces) by creating access policies. It also functions as a filter to allow/deny access for certain protocols such as HTTP, Telnet, FTP etc.

To configure Brocade Mobility 7131 Series Access Point subnet access:

1. Select *Network Configuration -> Firewall -> Subnet Access* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Refer to the *Overview* field to view rectangles representing subnet associations. The three possible colors indicate the current access level, as defined, for each subnet association.

Color	Access Type	Description
Green	Full Access	No protocol exceptions (rules) are specified. All traffic may pass between these two areas.
Yellow	Limited Access	One or more protocol rules are specified. Specific protocols are either enabled or disabled between these two areas. Click the table cell of interest and look at the exceptions area in the lower half of the screen to determine the protocols that are either allowed or denied.
Red	No Access	All protocols are denied, without exception. No traffic will pass between these two areas.



3. Configure the *Rules* field 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.
Pre configured Rules	The following protocols are preconfigured with the Brocade Mobility 7131 Series Access Point. 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.
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..
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.

4. Click *Apply* to save any changes to the Subnet Access screen. 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 Subnet Access screen to the last saved configuration.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Available protocols

Protocols that are not pre-configured can be specified using the drop down list within the *Transport* column within the Subnet 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)*.

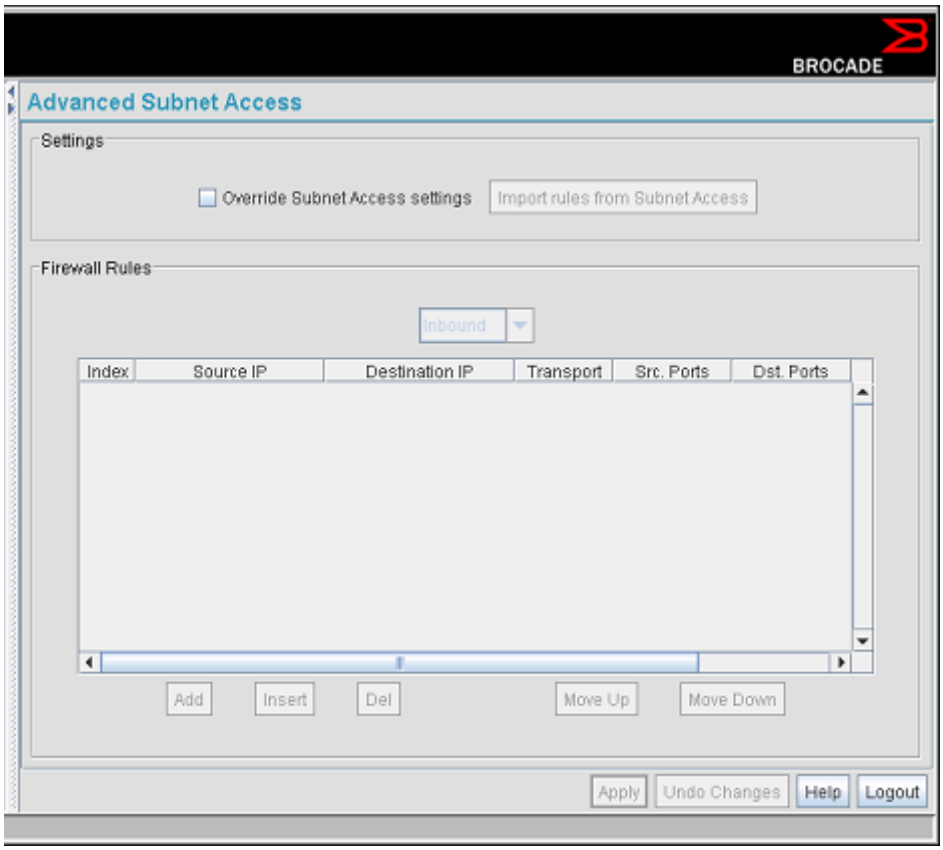
  AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
- *ESP - 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.

Configuring Advanced Subnet Access

Use the *Advanced Subnet 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 Subnet Access* screen allows you to import existing subnet access rules into the advanced subnet access rules.

To configure Brocade Mobility 7131 Series Access Point Advanced Subnet Access:

1. Select *Network Configuration -> Firewall -> Advanced Subnet Access* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Configure the *Setting*s field as needed to override the settings in the Subnet Access screen and import firewall rules into the Advanced Subnet Access screen.

Override Subnet 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 *Subnet Access* screen.
Import rules from Subnet 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.
Src. Ports (Source Ports)	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.
Dst. Ports (Destination Ports	The destination port range determines which ports the firewall rule applies to on the destination IP address. Click on the field to configure the destination 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.

4. Click *Apply* to save any changes to the Advanced Subnet 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 Subnet Access screen to the last saved configuration.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring VPN tunnels

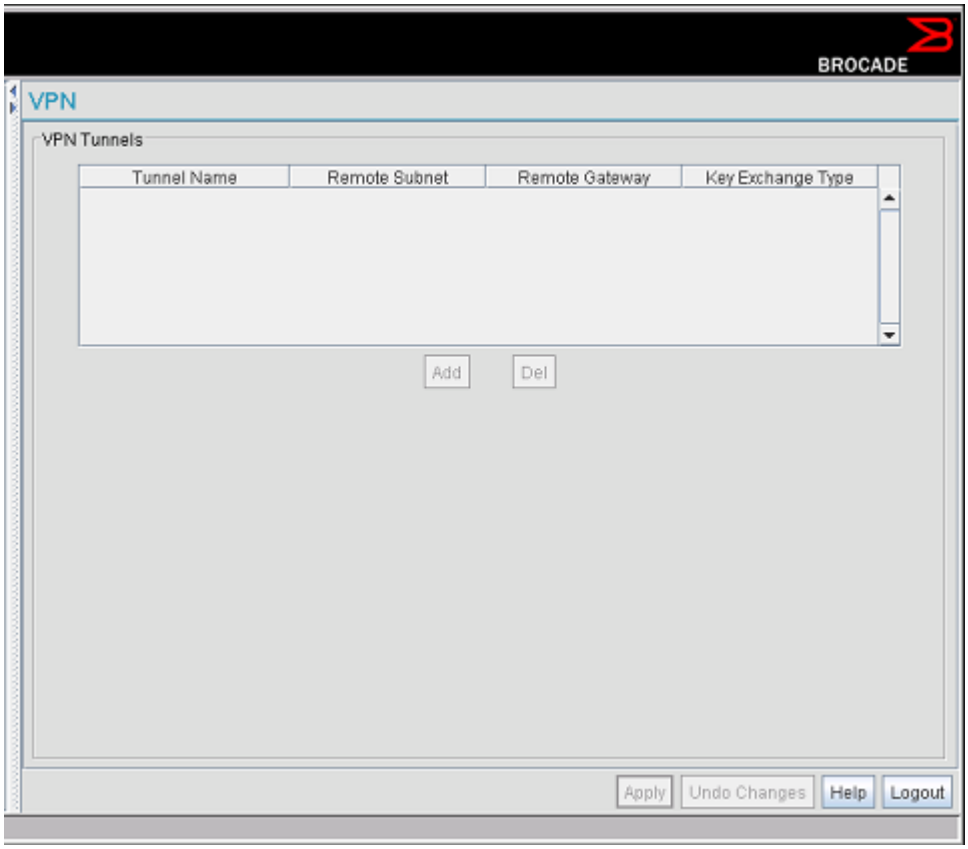
The Brocade Mobility 7131 Series Access Point allows up to 25 VPN tunnels to either a VPN endpoint or to another Brocade Mobility 7131 Series Access Point. VPN tunnels allow all traffic on a local subnet to route securely through a IPSEC tunnel to a private network. A VPN port is a virtual port which 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 decrypted.

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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> VPN* from the Brocade Mobility 7131 Series Access Point menu tree.



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 Brocade Mobility 7131 Series Access Point.
Remote Subnet	The *Remote Subnet* column lists the remote subnet for each tunnel. The remote subnet is the subnet the remote network uses for connection.

Remote Gateway	The *Remote Gateway* 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 controller.
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*.

NOTE
When creating a tunnel, the remote subnet and remote subnet mask must be that of the target device's LAN settings. The remote gateway must be that of the target device's WAN IP address.

If access point #1 has the following values:

- *WAN IP address*: 20.1.1.2
- *LAN IP address:* 10.1.1.1
- *Subnet Mask:* 255.0.0.0

Then, the VPN values for access point #2 should be:

- *Remote subnet*: 10.1.1.0 or 10.0.0.0
- *Remote subnet mask:* 255.0.0.0
- *Remote gateway*: 20.1.1.2

3. If a VPN tunnel has been added to the list of available Brocade Mobility 7131 Series Access Point tunnels, use the *VPN Tunnel Config* field to optionally modify the tunnel's properties.

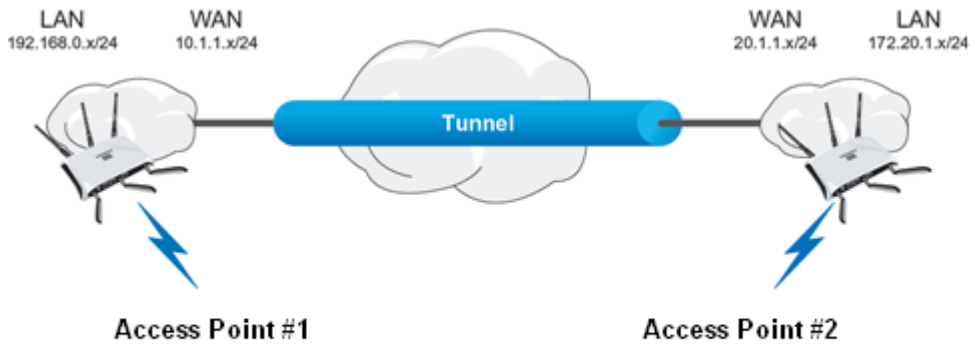
Tunnel Name	Enter a name to define the VPN tunnel. The tunnel name is used to uniquely identify each tunnel. Select a name best suited to that tunnel's function so it can be selected again in the future if required in a similar application.
Interface name	Use the drop-down menu to specify the LAN1, LAN2 or WAN connection used for routing VPN traffic. Remember, only one LAN connection can be active on the access point Ethernet port at a time. The LAN connection specified from the LAN screen to receive priority for Ethernet port connectivity may be the better subnet to select for VPN traffic.
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.
Default Gateway	Displays the WAN interface's default gateway IP address.

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.
Auto (IKE) Key Exchange	Select the Auto (IKE) Key Exchange checkbox to configure AH and/or ESP without having to manually enter keys. The keys automatically generate and rotate for the authentication and encryption type selected.
Auto Key Settings	Select the Auto (IKE) Key Exchange checkbox, and click the *Auto Key Settings* button to open a screen where AH authentication and ESP encryption/authentication can be configured.
IKE Settings	After selecting Auto (IKE) Key Exchange, click the *IKE Settings* button to open a screen where IKE specific settings can be configured.

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 Access Point applet. A prompt displays confirming the logout before the applet is closed.

Creating a VPN tunnel between two access points

This section describes how to define a simple configuration using two access points to create an IPSec tunnel.



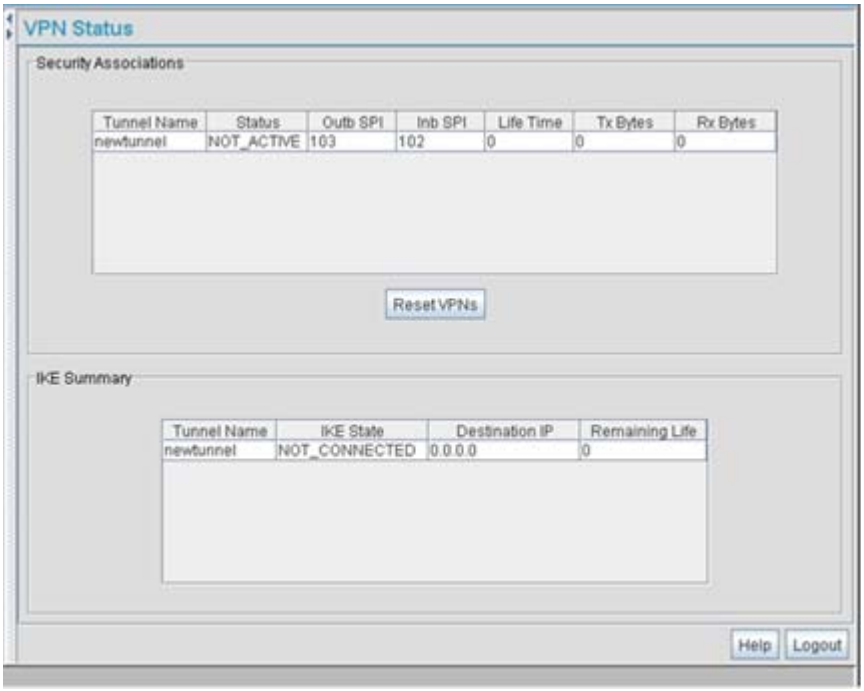
To create a IPSec VPN tunnel between two access points:

1. Ensure the WAN ports are connected via the internet
2. Select *Network Configuration -> WAN -> VPN* from the access point menu tree.
3. Enter any tunnel name (tunnel names do not need to match).

4. Enter the WAN port IP address of AP #1 in the *Local WAN IP* field
5. Enter the LAN IP subnet and mask of AP #2 in the *Remote Subnet* and *Remote Subnet Mask* fields,
6. Enter the WAN port IP address of AP #2 in the *Remote Gateway* field
7. Click *Add* to add the tunnel to the list.
8. Select the *Auto (IKE) Key Exchange* button.
9. Select *Auto Key Settings*.
10. Select *ESP with Authentication* and *AES 128-bit*. Click *OK*.
11. Select the *IKE Settings* button.
12. Select *Pre Shared Key (PSK)*.
13. Enter the Passphrase.

    Passphrases must match on both VPN devices.
14. Select *AES 128-bit*.
15. Select *Group 2*.
16. Click *OK*.

    This will take you back to the main VPN configuration screen.
17. Click *Apply* to save the updates
18. Select *Network Configuration -> WAN -> VPN -> VPN Status* from the access point menu tree. Check the VPN status on the access point.



Notice the status displays "NOT_ACTIVE". This screen automatically refreshes to get the current status of the VPN tunnel. Once the tunnel is active, the IKE_STATE changes from NOT_CONNECTED to SA_MATURE.

19. On AP #2, repeat the same steps as above. However, replace AP #2 information with AP #1 information.
20. Once both tunnels are established, ping each side to ensure connectivity.

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.

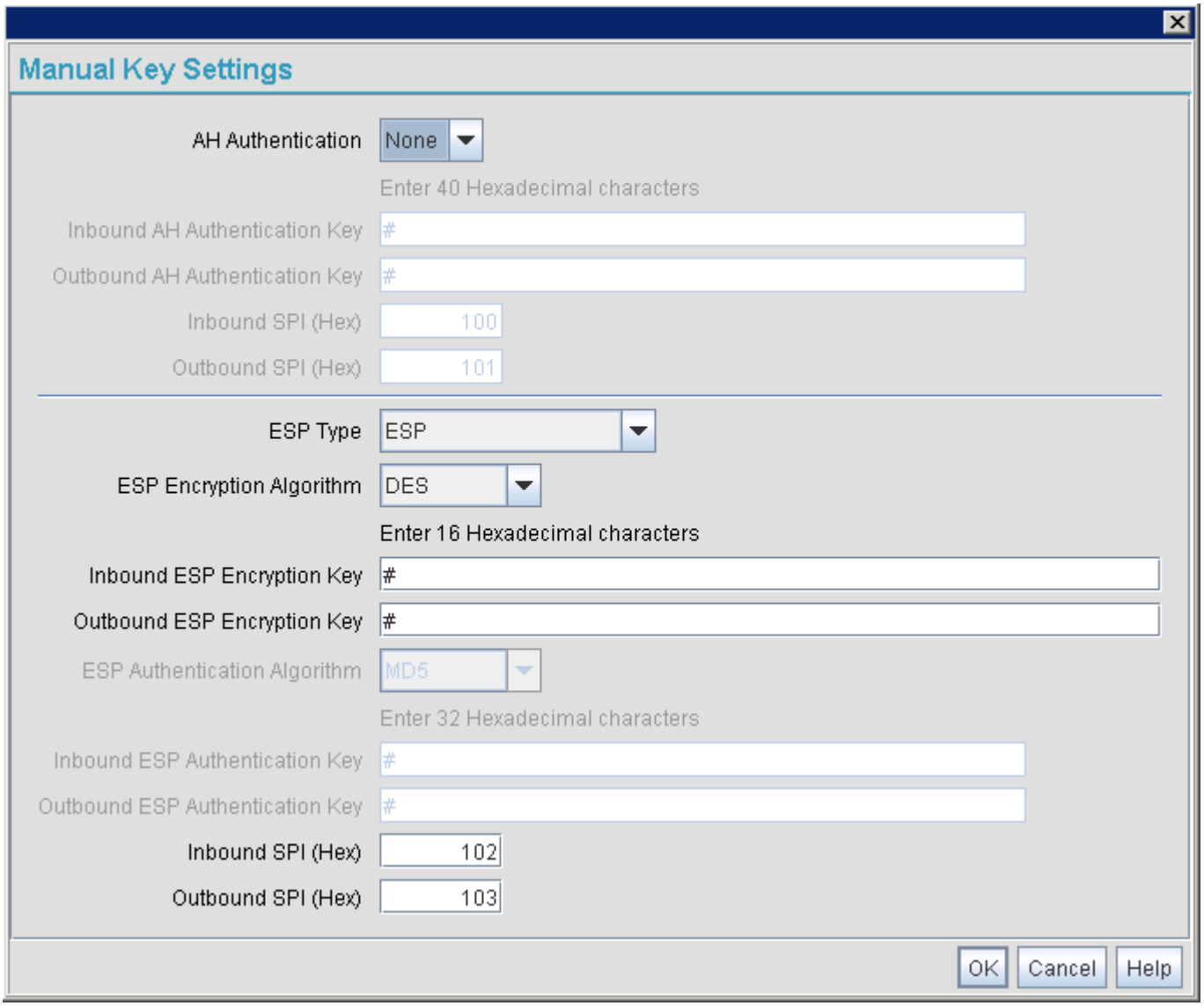
A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies the algorithms to use for the selected security protocol. If you specify an ESP protocol in a transform set, specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication 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 Setting*s screen to specify the transform sets used for VPN access.

To configure manual key settings for the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> VPN* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Refer to the *VPN Tunnel Config* field, select the *Manual Key Exchange* radio button and click the *Manual Key Setting*s button.



3. Configure the *Manual Key Setting*s screen to modify the following:

NOTE
When entering Inbound or Outbound encryption or authentication keys, an error message could display stating the keys provided are “weak”. Some WEP attack tools invoke a dictionary to hack WEP keys based on commonly used words. To avoid entering a weak key, try to not to produce a WEP key using commonly used terms and attempt to mix alphabetic and numerical key attributes when possible.

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 (for MD5/SHA1) hexadecimal (0-9, A-F) 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 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key value must match the corresponding inbound key on the remote security gateway.
Inbound SPI (Hex)	Enter an up to six-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 up to six-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.
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 (48-character hexadecimal) keys. • *AES 128-bit* - Uses the Advanced Encryption Standard algorithm with 128-bit (32-character hexadecimal) keys. • *AES 192-bit* - Uses the Advanced Encryption Standard algorithm with 192-bit (48-character hexadecimal) keys. • *AES 256-bit* - Uses the Advanced Encryption Standard algorithm with 256-bit (64-character hexadecimal) keys.
Inbound ESP Encryption Key	Enter a key for inbound traffic. The length of the key is determined by the selected encryption algorithm. The key must match the outbound key at the remote gateway.
Outbound ESP Encryption Key	Define a key for outbound traffic. The length of the key is determined by the selected encryption algorithm. The key must match the inbound key at the remote gateway.

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 (for MD5/SHA1) hexadecimal (0-9, A-F) 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 (for MD5/SHA1) hexadecimal (0-9, A-F) characters in length. The key must match the corresponding inbound key on the remote security gateway.
Inbound SPI (Hex)	Define an (up to) six-character (maximum) hexadecimal value to identify the inbound security association created by the encryption algorithm. The value must match the corresponding outbound SPI value configured on the remote security gateway.
Outbound SPI (Hex)	Enter an (up to) six-character (maximum) hexadecimal value to identify the outbound security association created by the encryption algorithm. The value must match the corresponding inbound SPI value configured 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

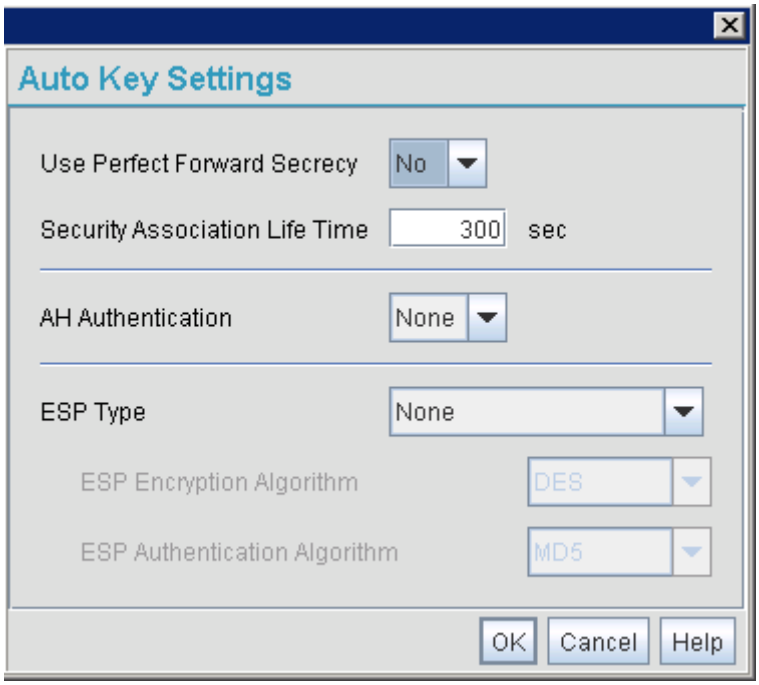
4. Click *Ok* to return to the VPN screen. Click *Apply* to retain the settings made on the *Manual Key Settings* screen.
5. Click *Cancel* to return to the VPN screen without retaining the changes made to the *Manual Key Settings* screen.

Configuring auto key settings

The Brocade Mobility 7131 Series Access Point'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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> VPN* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Refer to the *VPN Tunnel Config* field, select the *Auto (IKE) Key Exchange* radio button 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.
Security Association Life Time	The Security Association Life Time is the configurable interval used to timeout association requests that exceed the defined interval. The available range is from 300 to 65535 seconds. The default is 300 seconds.
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. No keys are required to be manually provided. *MD5* - Enables the Message Digest 5 algorithm. No keys are required to be manually provided. *SHA1* - Enables Secure Hash Algorithm 1. No keys are required to be manually provided.

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. *None* - Disables ESP. The rest of the fields are not active. *ESP* - Enables ESP for this tunnel. *ESP with Authentication* - Enables ESP with authentication.
ESP Encryption Algorithm	Use this menu to select the encryption and authentication algorithms for this VPN tunnel. *DES* - Selects the DES algorithm.No keys are required to be manually provided. *3DES* - Selects the 3DES algorithm. No keys are required to be manually provided. *AES 128-bit* - Selects the Advanced Encryption Standard algorithm with 128-bit. No keys are required to be manually provided. *AES 192-bit* - Selects the Advanced Encryption Standard algorithm with 192-bit. No keys are required to be manually provided. *AES 256-bit* - Selects the Advanced Encryption Standard algorithm with 256-bit. No keys are required to be manually provided.
ESP Authentication Algorithm	Use this menu to select the authentication algorithm to be used with ESP. This menu is only active when ESP with Authentication was selected for the ESP type. *MD5* - Enables the Message Digest 5 algorithm requiring 128-bit. No keys are required to be manually provided. *SHA1* - Enables Secure Hash Algorithm. No keys are required to be manually provided.

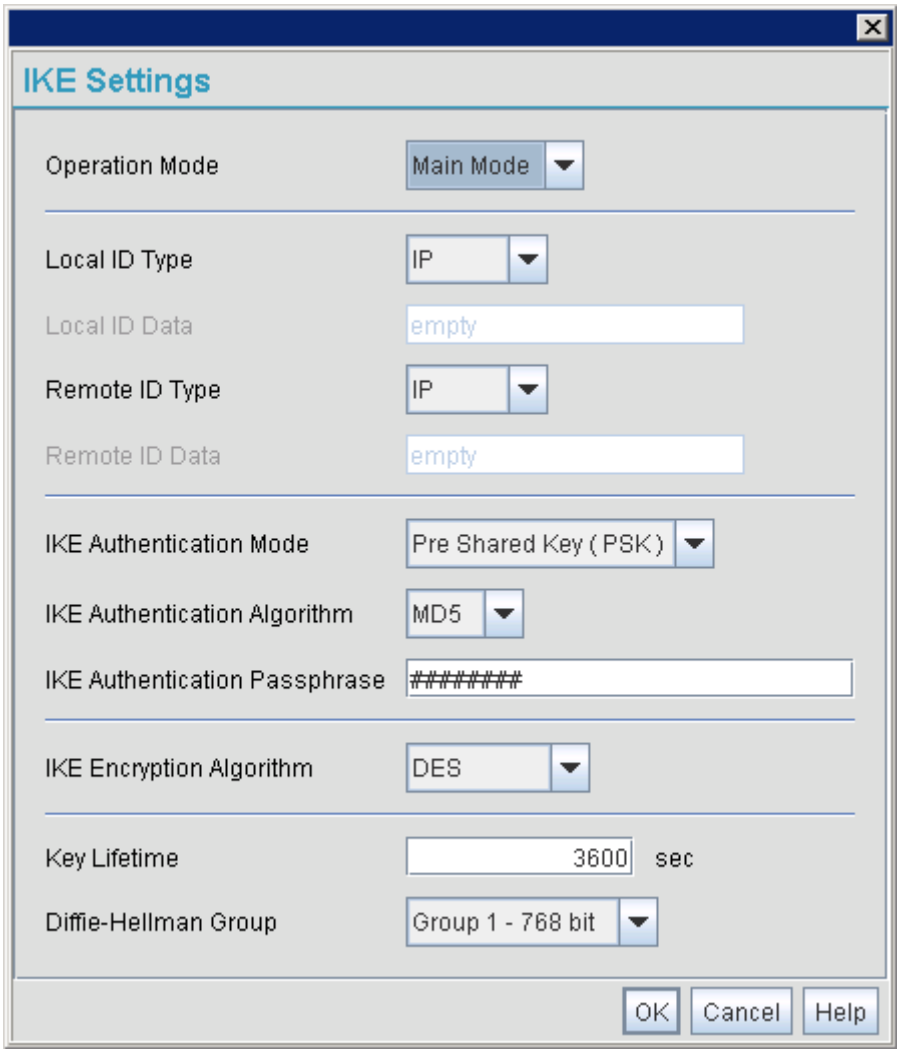
4. Click *Ok* to return to the VPN screen. Click Apply to retain the settings made on the *Auto Key Settings* screen.
5. Click *Cancel* to return to the VPN screen without retaining the changes made to this screen.

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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> VPN* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Refer to the *VPN Tunnel Config* field, select the *Auto (IKE) Key Exchange* radio button 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
Local ID Type	Select the type of ID to be used for the Brocade Mobility 7131 Series Access Point end of the SA. *IP* - Select IP if the local ID type is the IP address specified as part of the tunnel. *FQDN* - Use FQDN if the local ID is a fully qualified domain name (such as brocade.com). *UFQDN* - Select UFQDN if the local ID is a user fully-qualified email (such as johndoe@brocade.com).

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 Brocade Mobility 7131 Series Access Point end of the tunnel from the *Remote ID Type* drop-down menu. *IP* - Select the IP option if the remote ID type is the IP address specified as part of the tunnel. *FQDN* - Select FQDN if the remote ID type is a fully qualified domain name (such as brocade.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 remote ID type is a user unqualified email address (such as johndoe@brocade.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.
IKE Authentication Algorithm	IKE provides data authentication and anti-replay services for the VPN tunnel. Select an authentication methods from the drop-down menu. *MD5* - Enables the Message Digest 5 algorithm. No keys are required to be manually provided. *SHA1* - Enables Secure Hash Algorithm. No keys are required to be manually provided.
IKE Authentication Passphrase	If you selected *Pre-Shared Key* as the authentication mode, you must provide a passphrase.
IKE Encryption Algorithm	Select the encryption and authentication algorithms for the VPN tunnel from the drop-down menu. *DES* - Uses the DES encryption algorithm. No keys are required to be manually provided. *3DES* - Enables the 3DES encryption algorithm. No keys are required to be manually provided. *AES 128-bit* - Uses the Advanced Encryption Standard algorithm with 128-bit. No keys are required to be manually provided. *AES 192-bit* - Enables the Advanced Encryption Standard algorithm with 192-bit. No keys are required to be manually provided. *AES 256-bit* - Uses the Advanced Encryption Standard algorithm with 256-bit. No keys are required to be manually provided.

Key Lifetime	The number of seconds the key is valid. At the end of the lifetime, the key is renegotiated. The Brocade Mobility 7131 Series Access Point 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, 768-bit and 1024-bit. 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.

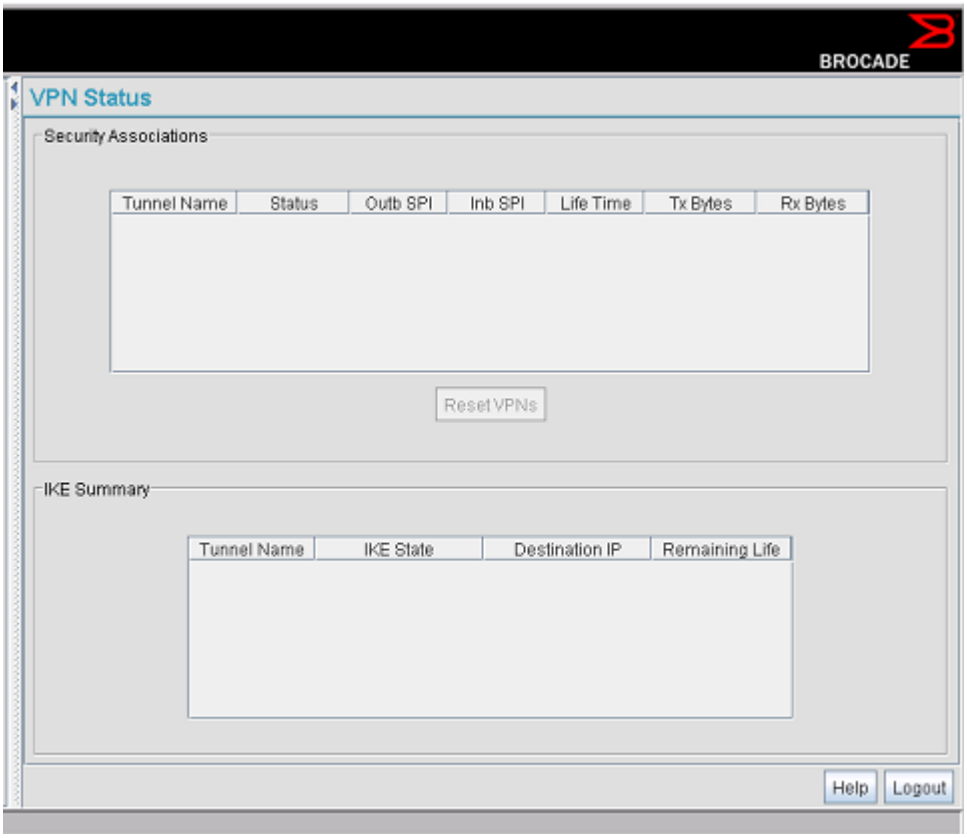
4. Click *Ok* to return to the VPN screen. Click Apply to retain the settings made on the *IKE Settings* screen.
5. Click *Cancel* to return to the VPN screen without retaining the changes made to the *IKE Settings* screen.

Viewing VPN status

Use the *VPN Status* screen to display the status of the tunnels configured on the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point menu tree.

To view VPN status:

1. Select *Network Configuration -> WAN -> VPN -> VPN Status* from the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point.
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 Brocade Mobility 7131 Series Access Point to identify a security association. There are unique outbound and inbound SPIs.
Inb SPI	The *Inb SPI* column displays the inbound *Security Parameter Index* (SPI) for each of the tunnels. The SPI is used locally by the Brocade Mobility 7131 Series Access Point to identify a security association. There are unique outbound and inbound SPIs.
Life Time	Use the *Life Time* column to view the lifetime associated with a particular Security Association (SA). Each SA has a finite lifetime defined. When the lifetime expires, the SA can no longer be used to protect data traffic. The maximum SA lifetime is 65535 seconds.

Tx Bytes	The *Tx Bytes* column lists the amount of data (in bytes) transmitted through each configured tunnel.
Rx Bytes	The *Rx Bytes* column lists the amount of data (in bytes) received through each configured tunnel.

3. Click the *Reset VPNs* button to reset active VPNs. Selecting *Reset VPNs* forces renegotiation of all the Security Associations and keys. Users could notice a slight pause in network performance.
4. Reference the *IKE Summary* field to view the following:

Tunnel Name	Displays the name of each of the tunnels configured to use IKE for automatic key exchange.
IKE State	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 *NOT_CONNECTED.* When the tunnel is active, the *IKE State* field displays *CONNECTED.*
Destination IP	Displays the destination IP address for each tunnel configured to use IKE for automatic key exchange.
Remaining Life	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.

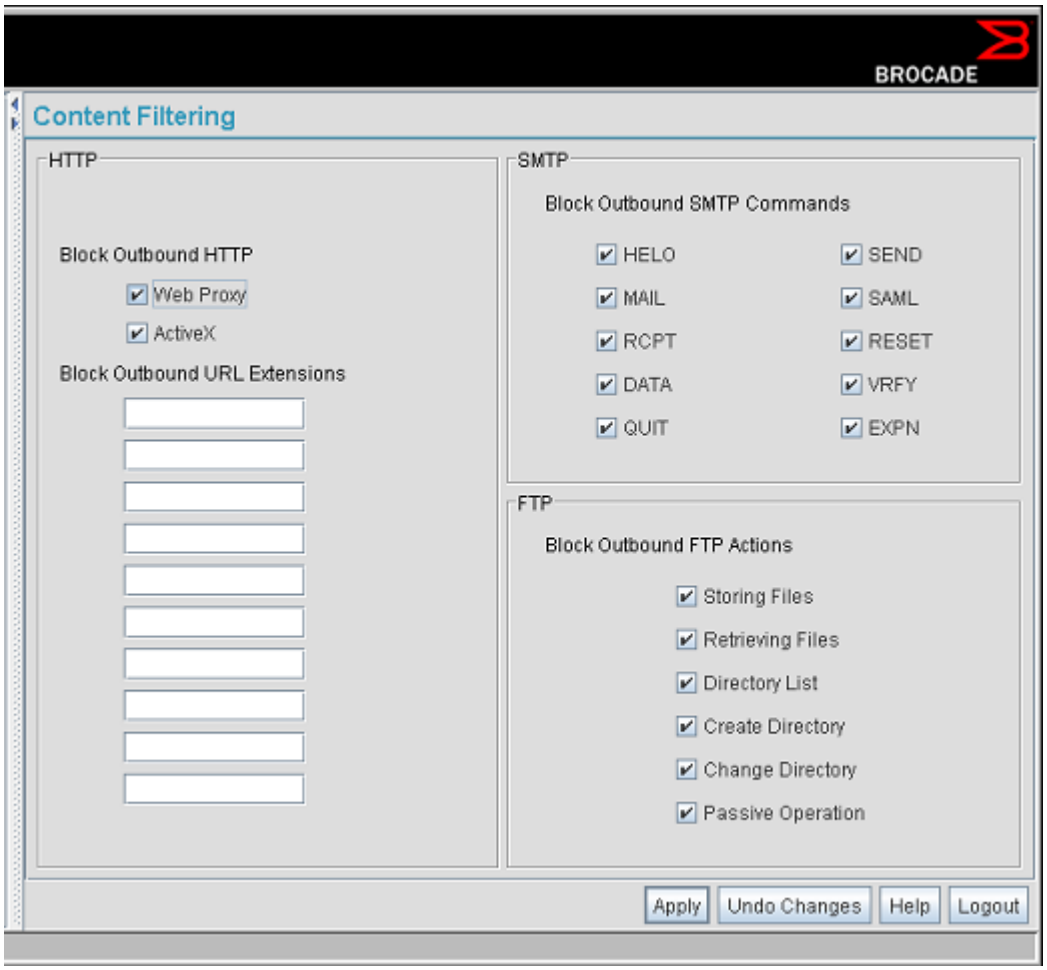
5. Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

Configuring content filtering settings

Content filtering allows system administrators to block specific commands and URL extensions from going out through the access point's 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 Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> WAN -> Content Filtering* from the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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.
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.

3. Configure the *SMTP* field to disable or restrict specific kinds of network mail traffic.

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 Brocade Mobility 7131 Series Access Point'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.

Block Outbound FTP Actions	*File Transfer Protocol (FTP)* is the Internet standard for host-to-host mail transport. FTP generally operates over TCP port 20 and 21. FTP filtering allows the blocking of any or all outgoing FTP functions. Check the box next to the command to disable the command when using FTP across the Brocade Mobility 7131 Series Access Point's WAN port. • *Storing Files* - Blocks the request to transfer files sent from the client across the AP's WAN port to the FTP server. • *Retrieving Files* - Blocks the request to retrieve files sent from the FTP server across the AP's WAN port to the client. • *Directory List* - Blocks requests to retrieve a directory listing sent from the client across the AP's WAN port to the FTP server. • *Create Directory* - Blocks requests to create directories sent from the client across the AP's WAN port to the FTP server. • *Change Directory* - Blocks requests to change directories sent from the client across the AP's WAN port to the FTP server. • *Passive Operation* - Blocks passive mode FTP requests sent from the client across the AP's WAN port to the FTP server.

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 Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring rogue AP detection

It is possible that not all of the devices identified by the Brocade Mobility 7131 Series Access Point are operating legitimately within the Brocade Mobility 7131 Series Access Point's radio coverage area. A rogue AP is a device located nearby an authorized Brocade Brocade Mobility 7131 Series Access Point but recognized as having properties rendering its operation illegal and threatening to the Brocade Mobility 7131 Series Access Point and the LAN. Rogue AP detection can be configured independently for both Brocade Mobility 7131 Series Access Point 802.11a/n and 802.11b/g/n radios (if using a dual radio sku Brocade Mobility 7131 Series Access Point). A rogue detection interval is the user-defined interval the Brocade Mobility 7131 Series Access Point waits to search for rogue APs. Additionally, the access point does not detect rogue APs on illegal channels (channels not allowed by the regulatory requirements of the country the access point is operating in).

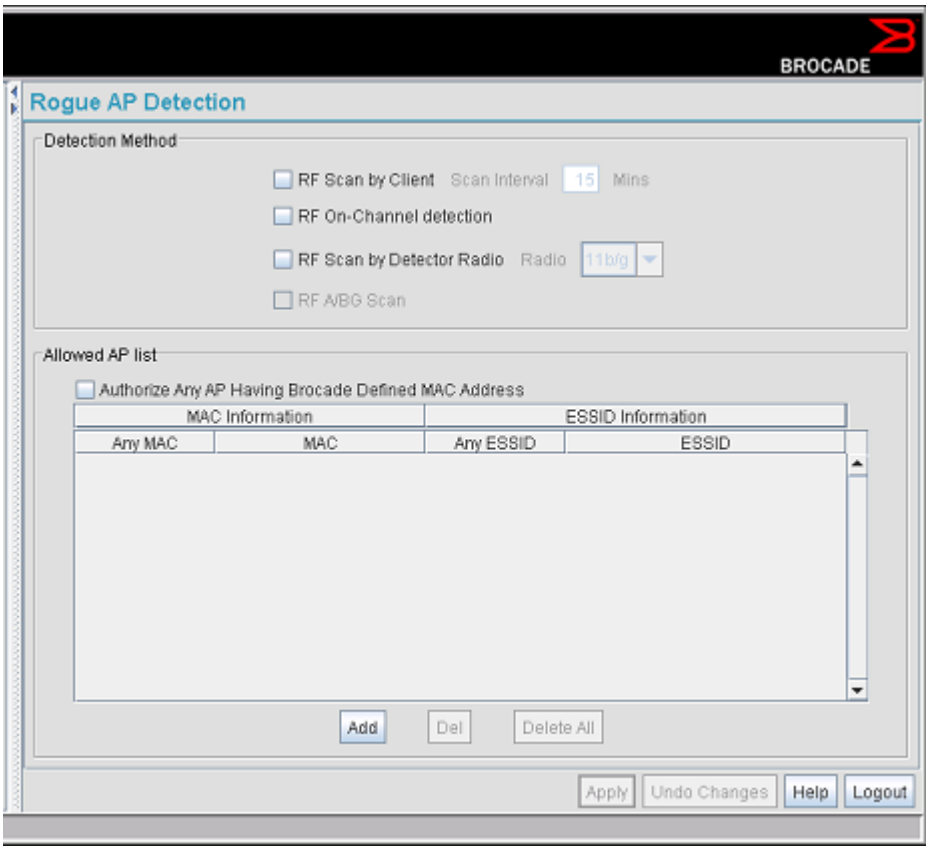
The rogue detection interval is used in conjunction with Motorola clients that identify themselves as rogue detection capable to the access point. The detection interval defines how often the access point requests these clients to scan for a rogue AP. A shorter interval can affect the performance of the Client, but it will also decrease the time it takes for the access point to scan for a rogue AP. A longer interval will have less of an impact to the clients, 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 Client performance.

CAUTION

Using an antenna other than the Dual-Band Antenna (Part No. ML-2452-APA2-01) could render the Brocade Mobility 7131 Series Access Point's Rogue AP Detector Mode feature inoperable. Contact your Brocade sales associate for specific information.

To configure Rogue AP detection for the Brocade Mobility 7131 Series Access Point:

1. Select *Network Configuration -> Wireless -> Rogue AP Detection* from the Brocade Mobility 7131 Series Access Point menu tree.



CAUTION

Users cannot define a rogue detection method when one of the access point radios is functioning as a WIPS sensor. To use one of the radios as a detector, you must disable WIPS sensor mode first, then set a radio for the desired detection method.

2. Configure the *Detection Method* field to set the detection method (Client or Brocade Mobility 7131 Series Access Point) and define the 802.11a/n or 802.11b/g/n radio to conduct the rogue AP search.

RF Scan by Client	Select the *RF Scan by Client* checkbox to enable clients to scan for potential rogue APs within the network. Define an interval in the *Scan Interval* field for associated clients to beacon in an attempt to locate a rogue AP. Set the interval to a value sooner than the default if a large volume of device network traffic is anticipated within the coverage area of the target Brocade Mobility 7131 Series Access Point. The *Scan Interval* field is not available unless the RF Scan by Client checkbox is selected. Motorola clients must be associated and have rogue AP detection enabled.
RF On-Channel Detection	Select the *RF On-Channel Detection* checkbox to enable the access point to detect rogue APs on its current (legal) channel setting.
RF Scan by Detector Radio	If the access point is a dual-radio model, select the *RF Scan by Detector Radio* checkbox to enable the selected 11a or 11b/g radio to scan for rogue APs. For example, if *11b/g* is selected, the existing 11a radio would act as the “detector radio,” scanning on all 11b/g channels while the existing 11b/g radio continues to service clients. The assumption is, when planning to do an all channel scan on one band, the clients would also be on that band. The radio on the other band is used as the “detector radio.”
RF A/BG Scan	Select this checkbox to scan for rouges over all channels on both of the access point’s 11a and 11bg radio bands. The switching of radio bands is based on a timer with no user intervention required. This option provides a good opportunity to detect rogues, as rogues often roam from one association to a stronger one regardless of the current operating channel.

3. Use the *Allowed AP List* field to restrict Brocade AP’s from Rogue AP detection and create a list of device MAC addresses and ESSID’s approved for interoperability with the Brocade Mobility 7131 Series Access Point.

Authorize Any AP Having Brocade Defined MAC Address	Select this checkbox to enable all access points with a Brocade MAC address to interoperate with the Brocade Mobility 7131 Series Access Point conducting a scan for rogue devices.
Add	Click *Add* to display a single set of editable MAC address and ESS address values.
Del (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. Do not use < > | " & \ ? as characters for the ESSID name.

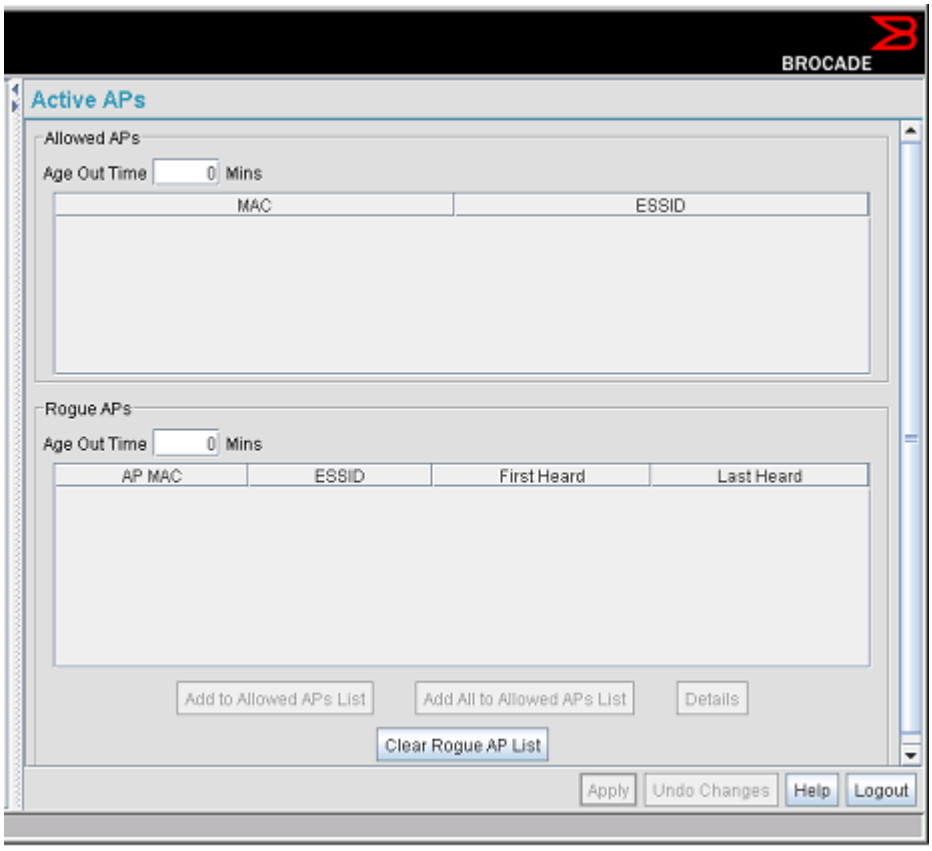
4. Click *Apply* to save any changes to the Rogue AP Detection screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.
5. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Rogue AP Detection screen to the last saved configuration.
6. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Moving rogue APs to the allowed AP list

The *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 Brocade Mobility 7131 Series Access Point menu tree.



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 242.
7. To remove the Rogue AP entries displayed within the e Rogue APs field, click the *Clear Rogue AP List* button.

   Brocade only recommends clearing the list of Rogue APs when the devices displaying within the list do not represent a threat to the access point managed network.
8. 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.
9. 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.
10. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

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 Brocade Mobility 7131 Series Access Point 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 Brocade 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 access point'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 access point detecting the rogue AP.
Detection Method	Displays the *RF Scan by Client*, *RF On-Channel Detection* or *RF Scan by Detector Radio* method selected from the Rogue AP screen to detect rogue devices.
First Heard (days:hrs:min)	Defines the time in (days:hrs:min) that the rogue AP was initially heard by the detecting AP.
Last Heard (days:hrs:min)	Defines the time in (days:hrs:min) that the rogue AP was last heard by the detecting AP.
Channel	Displays the channel the rogue AP is using.

5. Click *OK* to securely exit the Detail screen and return to the Active APs screen.
6. Click *Cancel* (if necessary) to undo any changes made and return to the Active APs screen.

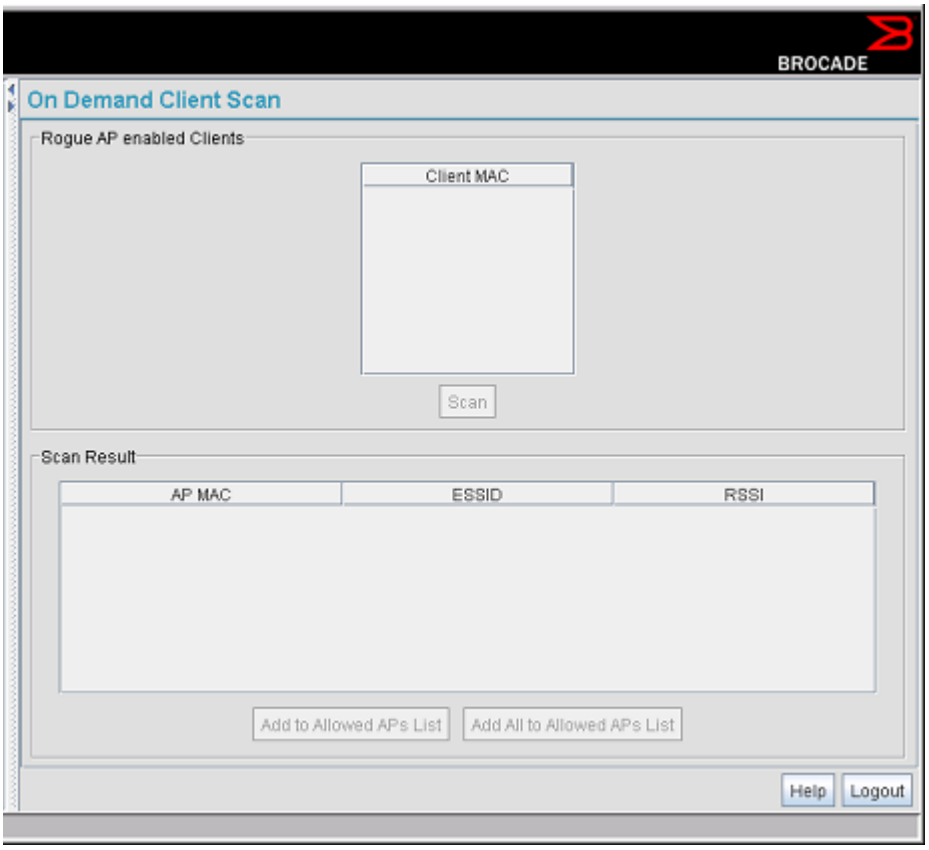
Using clients to detect rogue devices

The access point can use an associated Client 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 Client's detection capabilities with the access point's own rogue AP detection functionality, the rogue detection area can be significantly extended.

To use associated rogue AP enabled clients to scan for rogue APs:

1. Select *Network Configuration -> Wireless -> Rogue AP Detection -> Client Scan* from the Brocade Mobility 7131 Series Access Point menu tree.

   The *On Demand Client Scan* screen displays with associated clients with rogue AP detection enabled



2. Highlight a Client from within the *Rogue AP enabled clients* field and click the scan button.

   The target Client 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 238.

   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 Client 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 Client from the Rogue AP enabled clients field as needed to scan for additional rogue APs.
6. Click *Logout* to return to the Rogue AP Detection screen.

Configuring user authentication

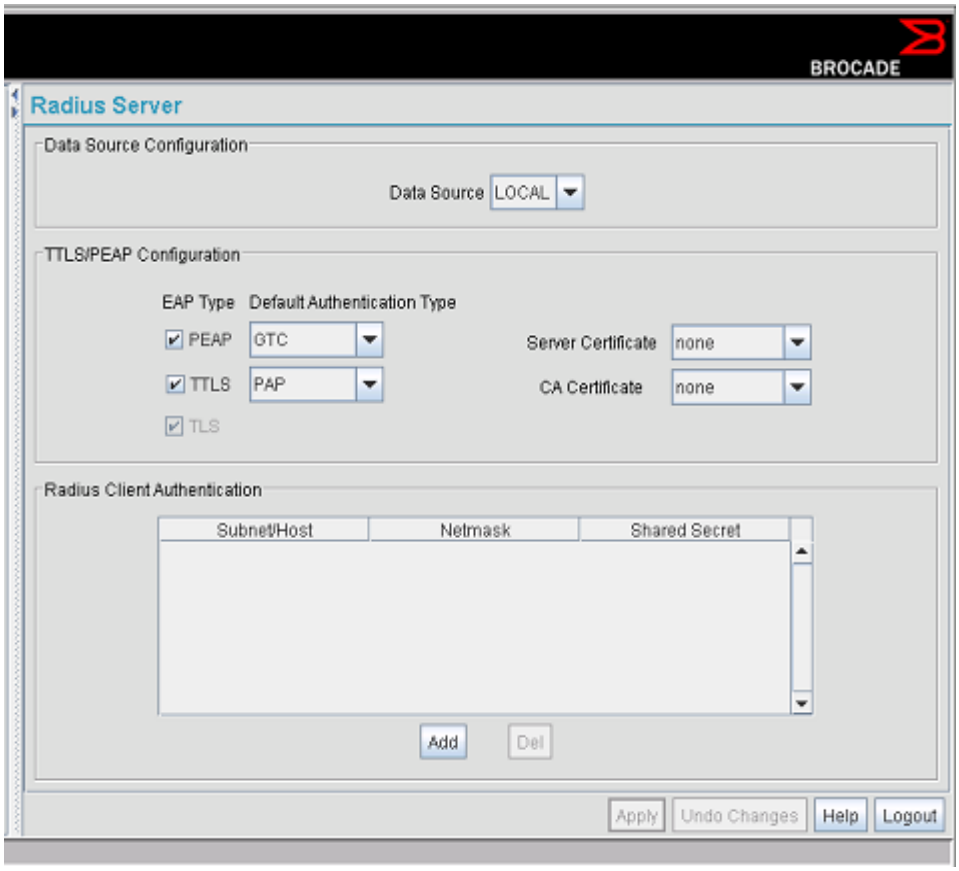
The access point can work with external Radius and LDAP Servers (AAA Servers) to provide user database information and user authentication.

Configuring the Radius Server

The *Radius Server* screen enables an administrator to define data sources and specify authentication information for the Radius Server.

To configure the Radius Server:

1. Select *System Configuration -> User Authentication -> Radius Server* from the menu tree.



2. From within the *Data Source Configuration* field, use the *Data Source* drop-down menu to select the data source for the Radius server.

Local	An internal user database serves as the data source. Use the *User Database* screen to enter the user data.
LDAP	If LDAP is selected, the controller will use the data in an LDAP server. Configure the LDAP server settings on the LDAP screen under Radius Server on the menu tree.

NOTE
When using LDAP, only PEAP-GTC and TTLS/PAP are supported.

3. Use the *TTLS/PEAP Configuration* field to specify the Radius Server default EAP type, EAP authentication type and a Server or CA certificate (if used).

EAP Type	Use the *EAP Type* checkboxes to enable the default EAP type(s) for the Radius server. Options include: • *PEAP* - Select the PEAP checkbox to enable both PEAP types (GTC and MSCHAP-V2) available to the access point. PEAP uses a TLS layer on top of EAP as a carrier for other EAP modules. PEAP is an ideal choice for networks using legacy EAP authentication methods. • *TTLS* - Select the TTLS checkbox to enable all three TTLS types (MD5, PAP and MSCHAP-V2) available to the access point.TTLS is similar to EAP-TLS, but the client authentication portion of the protocol is not performed until after a secure transport tunnel is established. This allows EAP-TTLS to protect legacy authentication methods used by some RADIUS servers. • *TLS* - The TLS checkbox is selected but disabled by default and resides in the background as it does not contain user configurable parameters.
Default Authentication Type	Specify a PEAP and/or TTLS Authentication Type for EAP to use from the drop-down menu to the right of each checkbox item. PEAP options include: • *GTC - EAP Generic Token Card* (GTC) is a challenge handshake authentication protocol using a hardware token card to provide the response string. • *MSCHAP-V2 - Microsoft CHAP* (MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol. • TTLS options include: • *PAP - Password Authentication Protocol* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized. WatchGuard products do not support the PAP protocol because the username and password are sent as clear text that a hacker can read. • *MD5* - This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128- bit fingerprint. The MD5 algorithm is intended for digital signature applications, in which a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptographic system. • *MSCHAP-V2 - Microsoft CHAP* (MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
Server Certificate	If you have a server certificate from a CA and wish to use it on the Radius server, select it from the drop-down menu. Only certificates imported to the access point are available in the menu.
CA Certificate	You can also choose an imported CA Certificate to use on the Radius server. If using a server certificate signed by a CA, import that CA's root certificate using the CA certificates screen. After a valid CA certificate has been imported, it is available from the CA Certificate drop-down menu.

CAUTION

If you have imported a Server or CA certificate, the certificate will not be saved when updating the access point's firmware. Export your certificates before upgrading the access point's firmware. From the access point CLI, use the *admin(system.cmgr)> expcert* command to export the certificate to a secure location.

4. Use the *Radius Client Authentication* table to configure multiple shared secrets based on the subnet or host attempting to authenticate with the Radius server. Use the *Add* button to add entries to the list. Modify the following information as needed within the table.

Subnet/Host	Defines the IP address of the subnet or host that will be authenticating with the Radius server. If a WLAN has been created to support mesh networking, then enter the IP address of mesh client bridge in order for the Client to authenticate with a base bridge.
Netmask	Defines the netmask (subnet mask) of the subnet or host authenticating with the Radius server.
Shared Secret	Click the Passwords button and set a shared secret used for each host or subnet authenticating against the RADIUS server. The shared secret can be up to 7 characters in length.

5. Click *Apply* to save any changes to the Radius Server screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
6. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Radius Server screen to the last saved configuration.
7. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring LDAP authentication

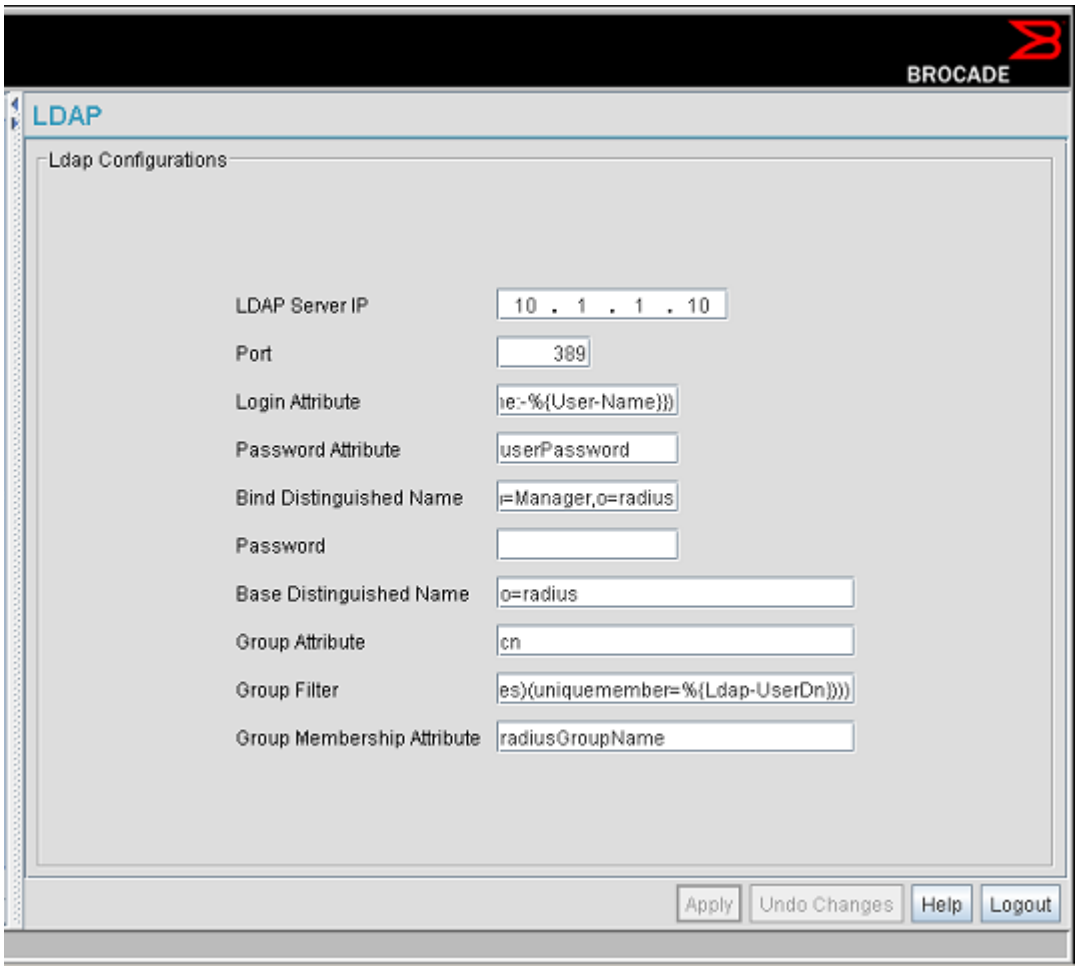
When the Radius Data Source is set to use an external LDAP server (see "Configuring the Radius Server" on page 245), the *LDAP* screen is used to configure the properties of the external LDAP server.

To configure the LDAP server:

1. Select *System Configuration -> User Authentication -> RADIUS Server -> LDAP* from the menu tree.

NOTE
For the onboard Radius server to work with Windows Active Directory or open LDAP as the database, the user has to be present in a group within the organizational unit. The same group must be present within the onboard Radius server's database. The group configured within the onboard Radius server is used for group policy configuration to support a new Time Based Rule restriction feature.

NOTE
The LDAP screen displays with unfamiliar alphanumeric characters (if new to LDAP configuration). Brocade recommends only qualified administrators change the default values within the LDAP screen.



2. Enter the appropriate information within the LDAP Configuration field to allow the access point to interoperate with the LDAP server. Consult with your LDAP server administrator for details on how to define the values in this screen.

LDAP Server IP	Enter the IP address of the external LDAP server acting as the data source for the Radius server. The LDAP server must be accessible from the WAN port or from the access point's active subnet.
Port	Enter the TCP/IP port number for the LDAP server acting as a data source for the Radius. The default port is 389.
Login Attribute	Specify the login attribute used by the LDAP server for authentication. In most cases, the default value should work. Windows Active Directory users must use "sAMAccountName" as their login attribute to successfully login to the LDAP server.
Password Attribute	Enter the password used by the LDAP server for authentication.

Bind Distinguished Name	Specify the distinguished name used to bind with the LDAP server.
Password	Enter a valid password for the LDAP server.
Base Distinguished Name	Enter a name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.
Group Attribute	Define the group attribute used by the LDAP server.
Group Filter	Specify the group filters used by the LDAP server.
Group Member Attribute	Enter the Group Member Attribute sent to the LDAP server when authenticating users.

CAUTION

Windows Active Directory users must set their Login Attribute to "sAMAccountName" in order to successfully login to the LDAP server.

3. Click *Apply* to save any changes to the LDAP screen. Navigating away from the screen without clicking Apply 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 LDAP screen to the last saved configuration.
5. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Configuring a proxy Radius server

The access point has the capability to proxy authentication requests to a remote Radius server based on the suffix of the user ID (such as myisp.com or company.com). The access point supports up to 10 proxy servers.

CAUTION

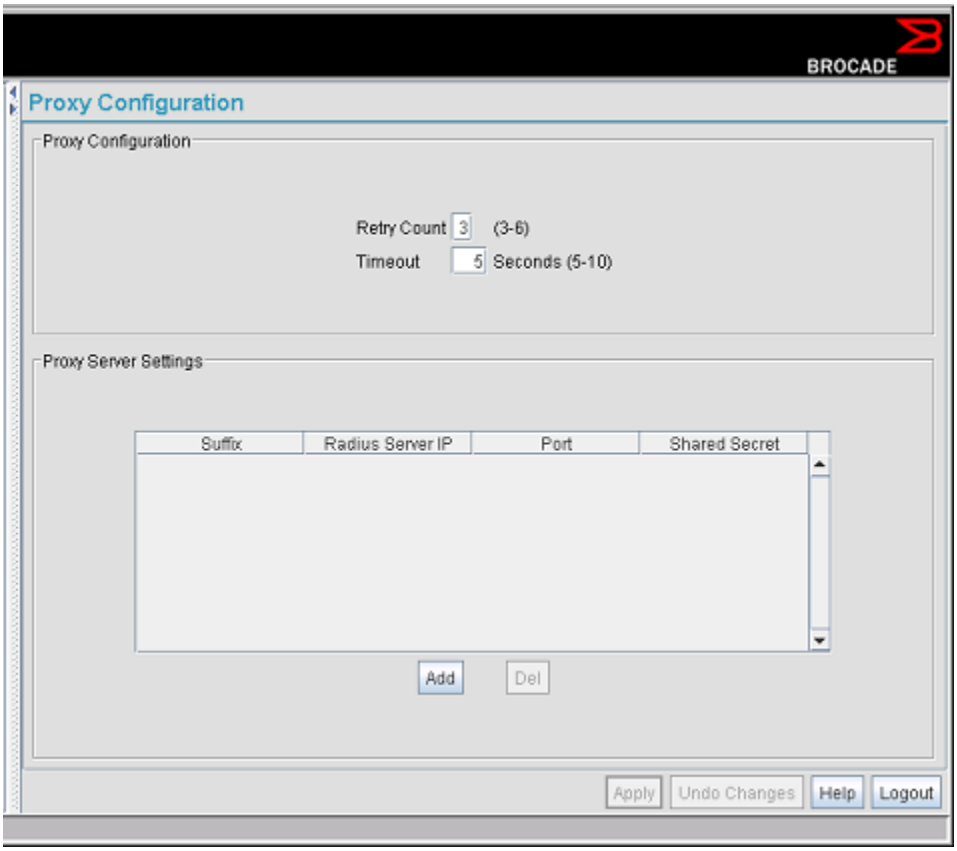
If using a proxy server for Radius authentication, the *Data Source* field within the Radius server screen must be set to *Local*. If set to LDAP, the proxy server will not be successful when performing the authentication. To verify the existing settings, see "Configuring the Radius Server" on page 245.

CAUTION

When configuring the credentials of an Client, ensure its login (or user) name is a *Fully Qualified Domain Name* (FQDN), or it cannot be authenticated by the access point's proxy server. For example; *br7131@2kserver.FUSCIA.com*.

To configure the proxy Radius server for the Brocade Mobility 7131 Series Access Point:

1. Select *System Configuration -> User Authentication -> RADIUS Server -> Proxy* from the menu tree.



2. Refer to the *Proxy Configuration* field to define the proxy server's retry count and timeout values.

Retry Count	Enter a value between 3 and 6 to indicate the number of times the access point attempts to reach a proxy server before giving up.
Timeout	Enter a value between 5 and 10 to indicate the number of elapsed seconds causing the access point to time out on a request to a proxy server.

3. Use the *Add* button to add a new proxy server. Define the following information for each entry:

Suffix	Enter the domain suffix (such as myisp.com or mycompany.com) of the users sent to the specified proxy server.
RADIUS Server IP	Specify the IP address of the Radius server acting as a proxy server.
Port	Enter the TCP/IP port number for the Radius server acting as a proxy server. The default port is 1812.
Shared Secret	Set a shared secret used for each suffix used for authentication with the Radius proxy server.

4. To remove a row, select the row and click the *Del* (Delete) button.

5. Click *Apply* to save any changes to the Proxy screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
6. Click *Undo Changes* (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Proxy screen to the last saved configuration.
7. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

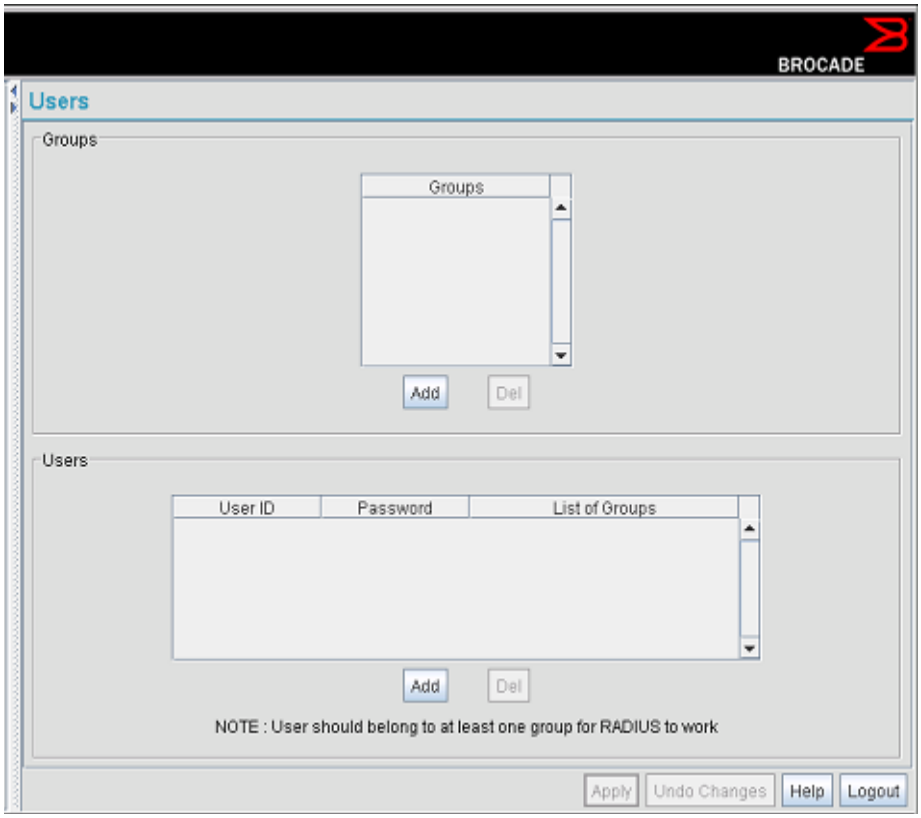
Managing the local User database

Use the *User Database* screen to create groups for use with the Radius server. The database of groups is employed if *Local* is selected as the Data Source from the Radius Server screen. For information on selecting Local as the Data Source, see "Configuring the Radius Server" on page 245.

To add groups to the User database:

NOTE
Each group can be configured to have its own access policy using the Access Policy screen. For more information, see "Defining user access permissions by group" on page 254.

1. Select *System Configuration -> User Authentication -> User Database* from the menu tree.



Refer to the *Groups* field for a list of all groups in the local Radius database. The groups are listed in the order added. Although groups can be added and deleted, there is no capability to edit a group name.

2. Click the *Add* button and enter the name of the group in the new blank field in the Groups table.
3. To remove a group, select the group from the table and click the *Del* (Delete) key.

   The *Users* table displays the entire list of users. Up to 100 users can be entered here. The users are listed in the order added. Users can be added and deleted, but there is no capability to edit the name of a group.
4. To add a new user, click the *Add* button at the bottom of the Users area.
5. In the new line, type a *User ID* (username).
6. Click the *Password* cell. A small window displays. Enter a password for the user and click *OK* to return to the Users screen.
7. Click the *List of Groups* cell. A new screen displays enabling you to associate groups with the user. For more information on mapping groups with a user, see "Mapping users to groups" on page 253.
8. Click *Apply* to save any changes to the Users screen. Navigating away from the screen without clicking Apply 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 Users screen to the last saved configuration.
10. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Mapping users to groups

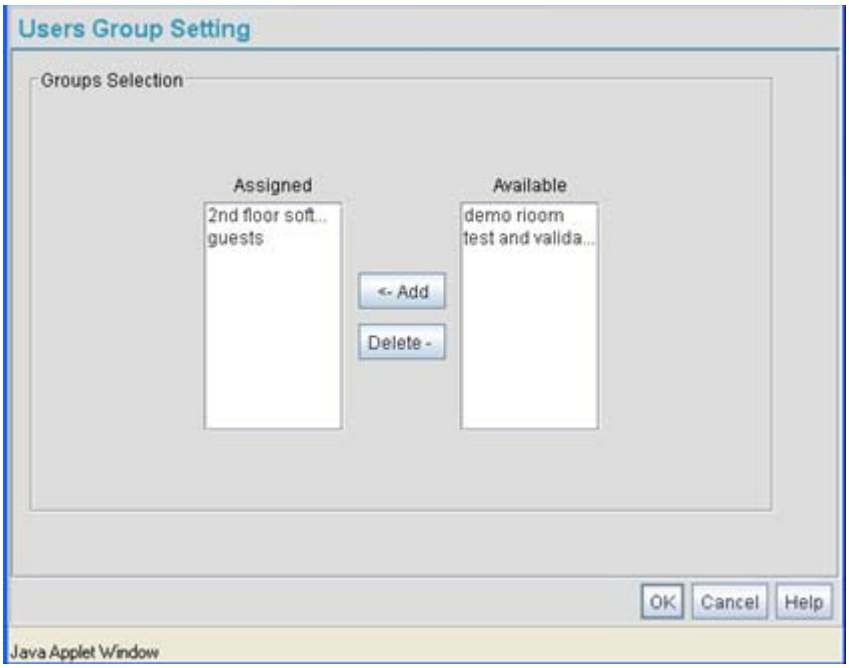
Once users have been created within the *Users* screen, their access privileges need to be configured for inclusion to one, some or all of the groups also created within the Users screen.

To map users to groups for group authentication privileges:

1. If you are not already in the Users screen, select *System Configuration -> User Authentication -> User Database* from the menu tree.

   Existing users and groups display within their respective fields. If user or group requires creation or modification, make your changes before you begin to map them.
2. Refer to the Users field and select the *List of Groups* column for the particular user you wish to map to one or more groups.

   The *Users Group Setting* screen displays with the groups available for user inclusion displayed within the *Available* column.



3. To add the user to a group, select the group in the *Available* list (on the right) and click the *<-Add* button.

   Assigned users will display within the *Assigned* table. Map one or more groups as needed for group authentication access for this particular user.

4. To remove the user from a group, select the group in the Assigned list (on the left) and click the *Delete->* button.

5. Click the *OK* button to save your user and group mapping assignments and return to the Users screen.

Defining user access permissions by group

An external AAA server maintains the users and groups database used by the access point for access permissions. Various kinds of access policies can be applied to each group. Individual groups can be associated with their own time-based access policy. Each group's policy has a user defined interval defining the days and hours access is permitted. Authentication requests for users belonging to the group are honored only during these defined hourly intervals.

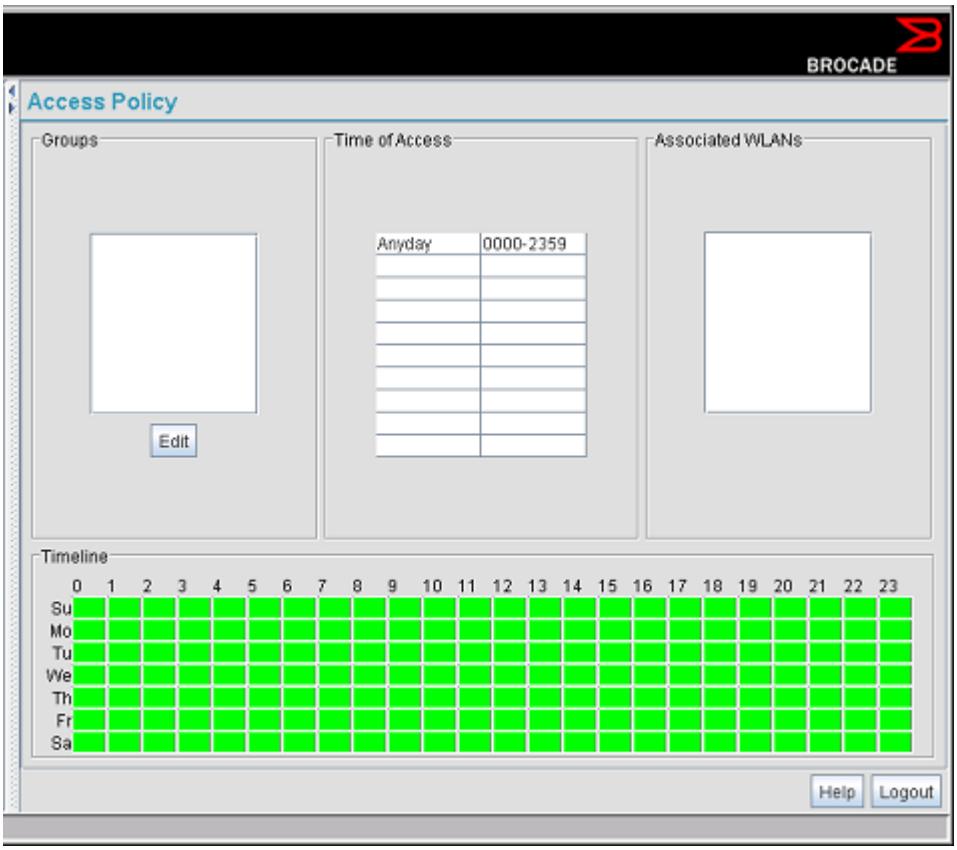
Defining the user access policy

Refer to the *Access Policy* screen to define WLAN access for the user group(s) defined within the Users screen. Each group created within the Users screen displays in the Access Policy screen within the groups column. Similarly, existing WLANs can be individually mapped to user groups by clicking the WLANs button to the right of each group name. For more information on creating groups and users, see "Managing the local User database" on page 252. For information on creating a new WLAN or editing the properties of an existing WLAN, see "Creating/editing individual WLANs" on page 139.

CAUTION

If using the Radius time-based authentication feature to authenticate access point user permissions, ensure *UTC* has been selected from the Date and Time Settings screen's *Time Zone* field. If UTC is not selected, time based authentication will not work properly. For information on setting the time zone for the access point, see "Configuring network time protocol (NTP)" on page 99.

1. Select *User Authentication -> Radius Server -> Access Policy* from the menu tree.



The Access Policy screen displays the following fields:

Groups	The *Groups* field displays the names of those existing groups that can have access intervals applied to them. Click the *Edit* button to display a screen designed to create access intervals for specific days and hours. A mechanism also exists for mapping specific WLANs to these intervals.
Time of Access	The *Time of Access* field displays the days of the week and the hours defined for group access to access point resources. This data is defined for the group by selecting the *Edit* button from within the *groups* field.

Associated WLANs	The *Associated WLANs* field displays the WLANs assigned the user group access permissions listed within the filters and grid fields. Add additional WLANs to a group by selecting the Edit button within the groups field.
grid	Refer to the *grid* field to review a bar graph of the selected group's access privileges. Revise the selected group's privileges as needed to

2. Review the existing access intervals assigned to each group by selecting the group from amongst those displayed. To modify a group's permissions, see "Editing group access permissions" on page 256.
3. Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

Editing group access permissions

The Access Policy screen provides a mechanism for modifying an existing group's access permissions. A group's permissions can be set for any day of the week and include any hour of the day. Ten unique access intervals can be defined for each existing group.

To update a group's access permissions:

1. Select *User Authentication -> Radius Server -> Access Policy* from the menu tree.
2. Select an existing group from within the groups field.
3. Select the *Edit* button.

   The Edit Access Policy screen displays.

4. Define up to 10 access policies for the selected group within the *Time Based Access Policy* field.

   Use the drop-down menus on the left-hand side of the screen to define the day of the week for which each policy applies. If continual access is required, select the *All Days* option. If continual access is required during Monday through Friday, but not Saturday or Sunday, select the *Weekdays* option.

   Use the *Start Time* and *End Time* values to define the access interval (in HHMM format) for each access policy. Each policy for a given group should have unique intervals. Policies can be created for different intervals on the same day of the week.

   NOTE
   Groups have a strict start and end time (as defined using the Edit Access Policy screen). Only during this period of time can authentication requests from users be honored (with no overlaps). Any authentication request outside of this defined interval is denied regardless of whether a user's credentials match or not.

5. Refer to the *WLANs* field to select existing WLANs to apply to the selected group's set of access permissions.

   The group's existing WLANs are already selected within the Edit screen. Select those additional WLANs requiring the access permissions specified in options 1-10 within the Time Based Access Policy field.

6. Click *Apply* to save any changes to the Edit Access Policy screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.

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

Chapter

7

Monitoring Statistics

In this chapter

- Viewing WAN statistics 259
- Viewing LAN statistics 263
- Viewing a LAN's IP filter statistics. 267
- Viewing radio statistics summary. 275
- Viewing client statistics summary 280
- Viewing the mesh statistics summary 284
- Viewing known access point statistics. 286

The Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point's 802.11a/n and 802.11b/g/n radios. An advanced radio statistics page is also available to display retry histograms for specific data packet retry information.

Associated Client stats can be displayed collectively for associated clients and individually for specific clients. An echo (ping) test is also available to ping specific clients to assess the strength of the AP association.

Finally, the Brocade Mobility 7131 Series Access Point can detect and display the properties of other APs detected within the Brocade Mobility 7131 Series Access Point radio coverage area. The type of AP detected can be displayed as well as the properties of individual APs.

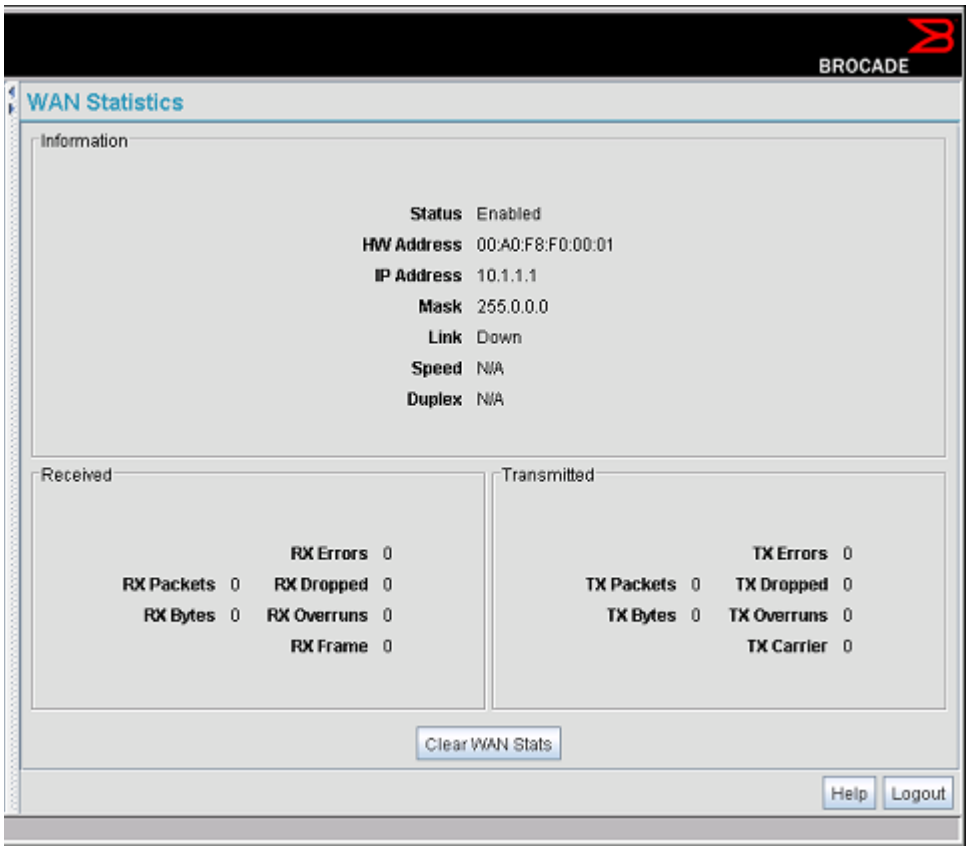
Viewing WAN statistics

Use the Brocade Mobility 7131 Series Access Point *WAN Stats* screen to view real-time statistics for monitoring the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point *WAN Stats* screen is view-only with no configurable data fields.

To view Brocade Mobility 7131 Series Access Point WAN Statistics:

1. Select *Status and Statistics -> WAN Stats* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Information* field to reference the following Brocade Mobility 7131 Series Access Point 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.
HW Address	The Media Access Control (MAC) address of the Brocade Mobility 7131 Series Access Point WAN port. The WAN port MAC address is hard coded at the factory and cannot be changed.For more information on how access point MAC addresses are assigned, see "Brocade Mobility 7131 Series Access Point MAC address assignment" on page 29.
IP Addresses	The displayed *Internet Protocol (IP)* addresses for the Brocade Mobility 7131 Series Access Point WAN port.
Mask	The *Mask* field displays the subnet mask number for the Brocade Mobility 7131 Series Access Point's WAN connection. This value is set on the *WAN* screen.

Link	The *Link* parameter displays *Up* if the WAN connection is active between the Brocade Mobility 7131 Series Access Point 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.

3. Refer to the *Received* field to reference data received over the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 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 access point was last restarted.
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.
RX Frame	The *RX Frame* field displays the number of TCP/IP data frame errors received.

4. Refer to the *Transmitted* field to reference data received over the Brocade Mobility 7131 Series Access Point WAN port.

TX Packets	TX packets are data packets sent over the WAN connection. The displayed number is a cumulative total since the WAN was last enabled or the Brocade Mobility 7131 Series Access Point was last restarted.
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 Brocade Mobility 7131 Series Access Point was last restarted..
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 assess access point 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.
TX Carrier	The *TX Carrier* field displays the number of TCP/IP data carrier errors.

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.

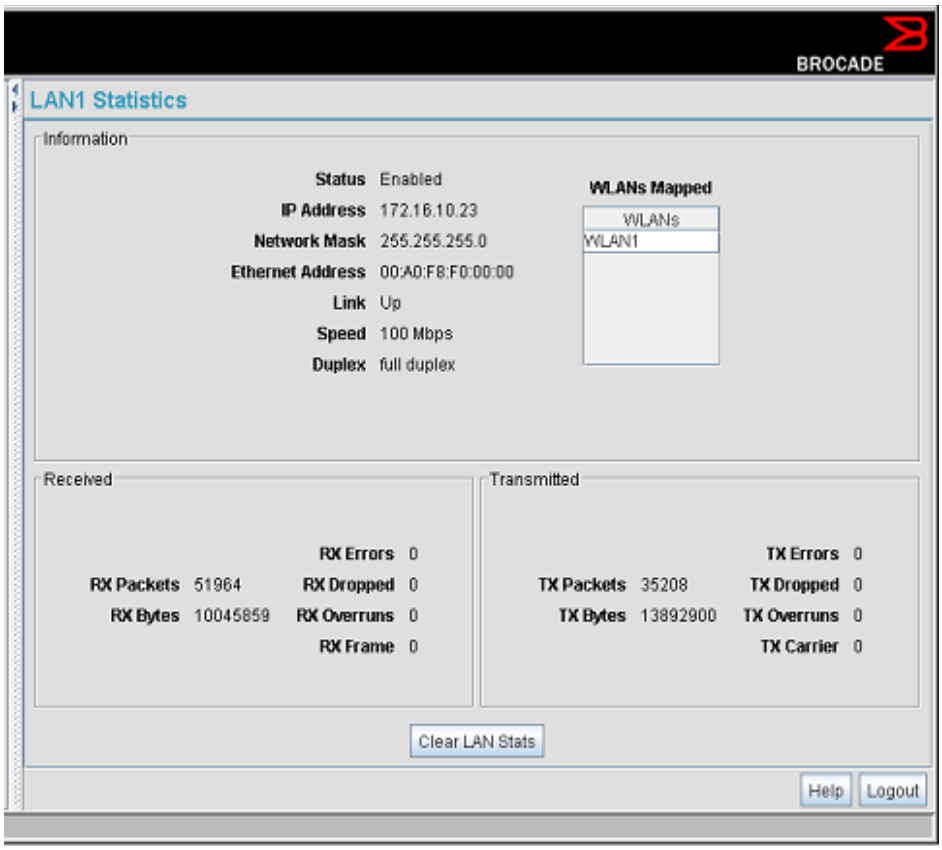
6. Click *Logout* to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

Viewing LAN statistics

Use the *LAN Stats* screen to monitor the activity of the Brocade Mobility 7131 Series Access Point's LAN1 or LAN2 connection. The *Information* field of the LAN Stats screen displays network traffic information as monitored over the Brocade Mobility 7131 Series Access Point LAN1 or LAN2 port. The *Received* and *Transmitted* fields of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted over the LAN1 or LAN2 port since it was last enabled or the Brocade Mobility 7131 Series Access Point was last restarted. The *LAN Stats* screen is view-only with no user configurable data fields.

To view Brocade Mobility 7131 Series Access Point LAN connection stats:

1. Select *Status and Statistics -> LAN Stats -> LAN1 Stats* (or LAN2 Stats) from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Information* field to view the following Brocade Mobility 7131 Series Access Point device address information:

Status	Displays whether this particular LAN has been enabled as viable subnet from within the LAN Configuration screen.
IP Address	The *Internet Protocol (IP)* addresses for the Brocade Mobility 7131 Series Access Point LAN port.
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.

Ethernet Address	The Media Access Control (MAC) address of the Brocade Mobility 7131 Series Access Point. The MAC address is hard coded at the factory and cannot be changed.For more information on how access point MAC addresses are assigned, see "Brocade Mobility 7131 Series Access Point MAC address assignment" on page 29.
Link	The *Link* parameter displays *Up* if the LAN connection is active between the Brocade Mobility 7131 Series Access Point and network, and *Down* if the LAN connection is interrupted or lost. Use this information to assess the current connection status of LAN 1 or LAN2.
Speed	The LAN 1 or LAN 2 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.
Duplex	Displays whether the current LAN connection is full or half duplex.
WLANs Mapped	The *WLANs Mapped* table lists the WLANs mapped to this LAN (either LAN1 or LAN2) as their LAN interface.

3. Refer to the *Received* field to view data received over the Brocade Mobility 7131 Series Access Point LAN port.

RX Packets	RX packets are data packets received over the Brocade Mobility 7131 Series Access Point LAN port. The number is a cumulative total since the LAN connection was last enabled or the Brocade Mobility 7131 Series Access Point was last restarted.
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 Brocade Mobility 7131 Series Access Point was last restarted.
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.
RX Dropped	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.
RX Overruns	RX overruns are buffer overruns on the Brocade Mobility 7131 Series Access Point 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.
RX Frame	The *RX Frame* field displays the number of TCP/IP data frame errors received.

4. Refer to the *Transmitted* field to view statistics transmitted over the Brocade Mobility 7131 Series Access Point LAN port.

TX Packets	TX packets are data packets sent over the Brocade Mobility 7131 Series Access Point LAN port. The displayed number is a cumulative total since the LAN connection was last enabled or the Brocade Mobility 7131 Series Access Point was last restarted.
TX Bytes	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 Brocade Mobility 7131 Series Access Point was last restarted.
TX Errors	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.
TX Dropped	The *TX Dropped* field displays the number of data packets that fail to get sent from the Brocade Mobility 7131 Series Access Point LAN port.
TX Overruns	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.
TX Carrier	The *TX Carrier* field displays the number of TCP/IP data carrier errors.

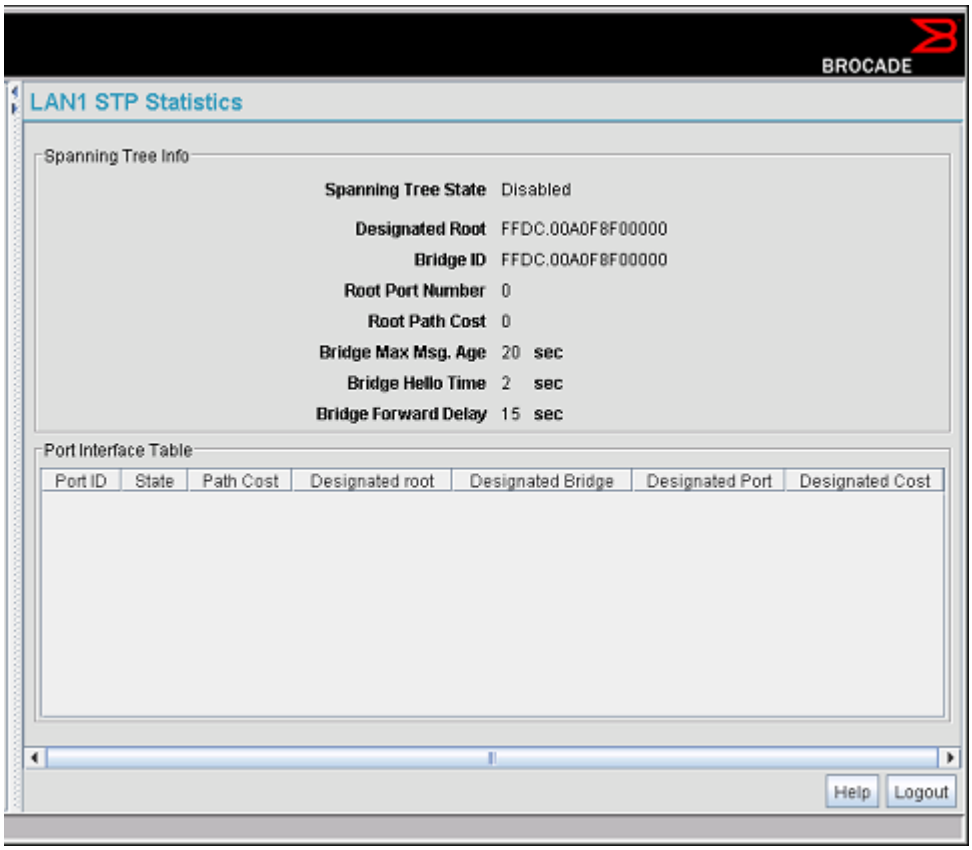
5. Click the *Clear LAN Stats* button to reset each of the data collection counters to zero in order to begin new data collections. The RX/TX Packets and RX/TX Bytes totals remain at their present values and are not cleared.
6. Click the *Logout* button to securely exit the Access Point applet. There will be a prompt confirming logout before the applet is closed.

Viewing a LAN's STP statistics

Each access point LAN has the ability to track its own unique STP statistics. Refer to the LAN STP Stats page when assessing mesh networking functionality for each of the two access point LANs. Access points in bridge mode exchange configuration messages at regular intervals (typically 1 to 4 seconds). If a bridge fails, neighboring bridges detect a lack of configuration messaging and initiate a spanning-tree recalculation (when spanning tree is enabled).

To view Brocade Mobility 7131 Series Access Point LAN's STP statistics:

1. Select *Status and Statistics* -> *LAN Stats* -> *LAN1 Stats* (or LAN2 Stats) > *STP Stats* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Spanning Tree Info* field to for details on spanning tree state, and root access point designation.

Spanning Tree State	Displays whether the spanning tree state is currently enabled or disabled. The spanning tree state must be enabled for a unique spanning-tree calculation to occur when the bridge is powered up or when a topology change is detected.
Designated Root	Displays the access point MAC address of the bridge defined as the root bridge in the Bridge STP Configuration screen.
Bridge ID	The Bridge ID identifies the priority and ID of the bridge sending the message
Root Port Number	Identifies the root bridge by listing its 2-byte priority followed by its 6-byte ID.
Root Path Cost	Bridge message traffic contains information identifying the root bridge and the sending bridge. The root path cost represents the distance (cost) from the sending bridge to the root bridge.
Bridge Max Msg. Age	The Max Msg Age measures the age of received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer. For information on setting the Maximum Message Age.

Bridge Hello Time	The Bridge Hello Time is the time between each bridge protocol data unit sent. This time is equal to 2 seconds (sec) by default, but can tuned between 1 and 10 sec. The 802.1d specification recommends the Hello Time be set to a value less than half of the Max Message age value.
Bridge Forward Delay	The Bridge Forward Delay value is the time spent in a listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec.

3. Refer to the *Port Interface Table* to assess the state of the traffic over the ports listed within the table for the root and bridge and designated bridges.

Port ID	Identifies the port from which the configuration message was sent.
State	Displays whether a bridge is forwarding traffic to other members of the mesh network (over this port) or blocking traffic. Each viable member of the mesh network must forward traffic to extent the coverage area of the mesh network.
Path Cost	The root path cost is the distance (cost) from the sending bridge to the root bridge.
Designated Root	Displays the MAC address of the access point defined with the lowest priority within the Mesh STP Configuration screen.
Designated Bridge	There is only one root bridge within each mesh network. All other bridges are designated bridges that look to the root bridge for several mesh network timeout values.
Designated Port	Each designated bridge must use a unique port. The value listed represents the port used by each bridge listed within the table to route traffic to other members of the mesh network.
Designated Cost	Displays the unique distance between each access point MAC address listed in the Designated Bridge column and the access point MAC address listed in the Designated Root column.

4. Click the *Logout* button to securely exit the Access Point applet. There will be a prompt confirming logout before the applet is closed.

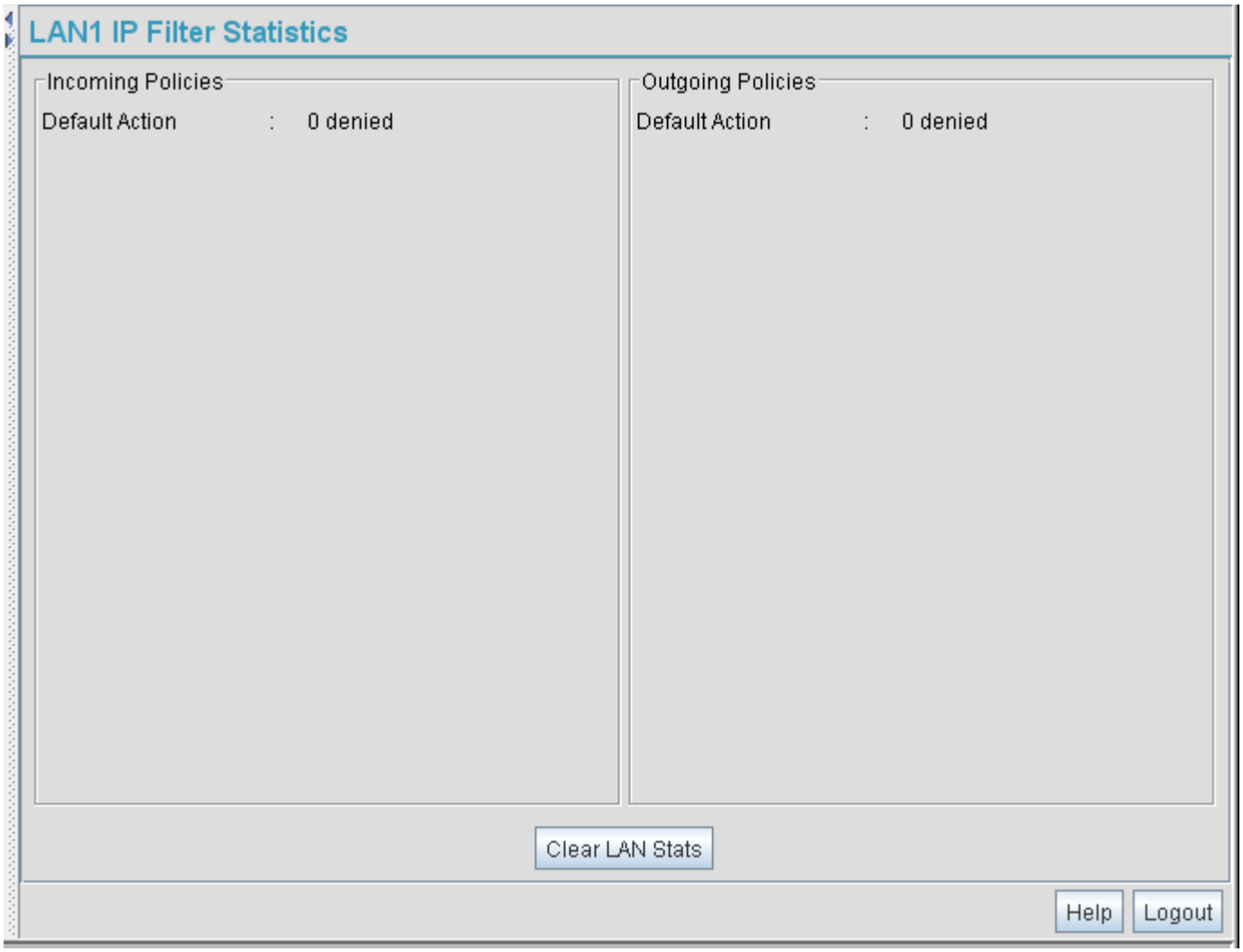
Viewing a LAN's IP filter statistics

Each access point LAN has the ability to track its own unique IP filter statistics. Refer to the LAN IP Filter Stats page to review statistics generated from both incoming and outgoing IP filtering policies. The LAN IP Filter Statistics screen shows a running count of packet traffic either allowed or denied when filter rules fail. These rules determine which IP packets are processed normally by LANs 1 and 2 and which are discarded.

For more information on how IP Filtering works and how its configured on the access point, see "Configuring IP filtering" on page 182.

To view access point LAN's IP filter statistics:

1. Select *Status and Statistics* -> *LAN Stats* -> *LAN1 Stats* (or LAN2 Stats) > *IP Filter Stats* from the access point menu tree.



2. Refer to the *Incoming Policies* field to assess the number of packets either allowed or denied access by the access point's filtering rules. These are packets that are incoming to the access point LAN.
3. Refer to the *Outgoing Policies* field to assess the number of packets either allowed or denied access by the access point's filtering rules. These are packets that are outgoing from the access point LAN.
4. Click the *Clear LAN 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 Access Point applet. There will be a prompt confirming logout before the applet is closed.

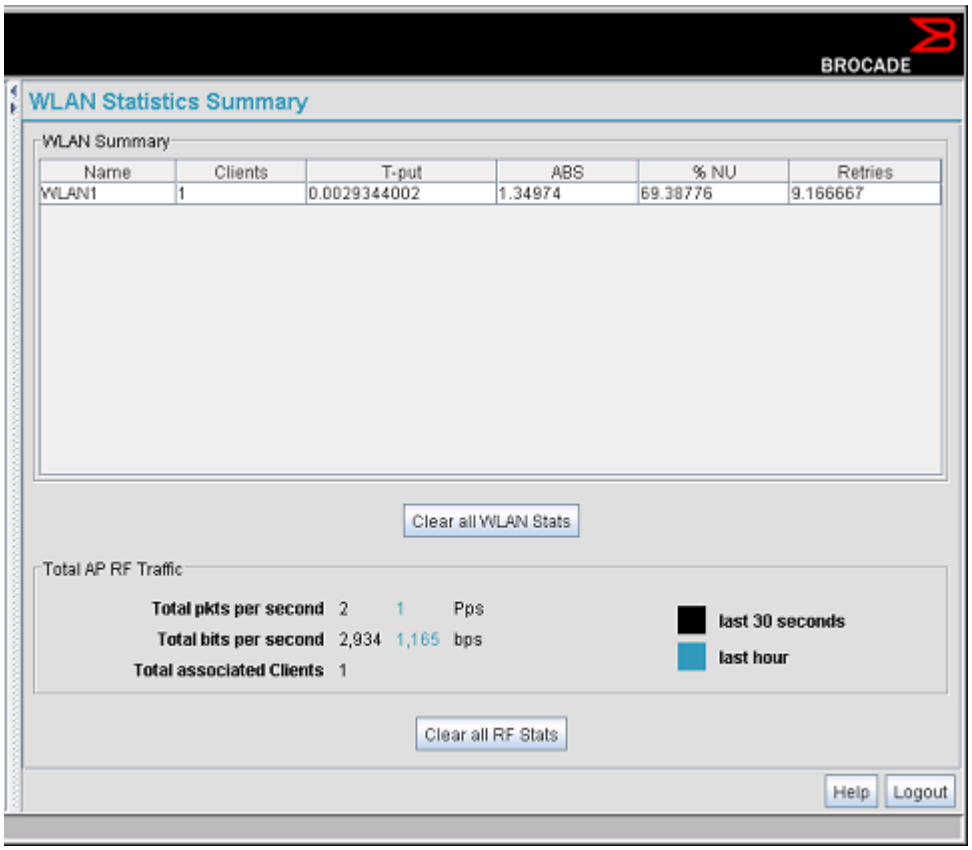
Viewing wireless statistics

Use the *WLAN Statistics Summary* screen to view overview statistics for active (enabled) WLANs on the Brocade Mobility 7131 Series Access Point. The *WLAN Summary* field displays basic information such as number of Wireless Clients and total throughput for each of the active WLANs. The *Total RF Traffic* section displays basic throughput information for all RF activity on the Brocade Mobility 7131 Series Access Point. The WLAN Statistics Summary screen is view-only with no user configurable data fields.

If a WLAN is not displayed within the *Wireless Statistics Summary* screen, see "Enabling wireless LANs (WLANs)" on page 137 to enable the WLAN. For information on configuring the properties of individual WLANs, see "Creating/editing individual WLANs" on page 139.

To view Brocade Mobility 7131 Series Access Point WLAN Statistics:

1. Select *Status and Statistics -> Wireless Stats* from the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point.
clients	Displays the total number of clients currently associated with each enabled WLAN. Use this information to assess if the clients are properly grouped by function within each enabled WLAN.

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.
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.

3. Refer to the *Total AP RF Traffic* field to view throughput information for the Brocade Mobility 7131 Series Access Point and WLAN.

Total pkts per second	Displays the average number of RF packets sent per second across all active WLANs on the Brocade Mobility 7131 Series Access Point. The number in black represents packets for the last 30 seconds and the number in blue represents total pkts per second for the last hour.
Total bits per second	Displays the average bits sent per second across all active WLANs on the access point. The number in black displays this statistic for the last 30 seconds and the number in blue displays this statistic for the last hour.
Total associated clients	Displays the current number of clients associated with the active WLANs on the Brocade Mobility 7131 Series Access Point. If the number is excessive, reduce the maximum number of clients that can associate with the Brocade Mobility 7131 Series Access Point.
Clear all RF Stats	Click the *Clear all RF Stats* button to reset statistic counters for each WLAN, and the Total AP RF totals to 0. Do not clear RF stats if currently in an important data gathering activity or risk losing all data calculations to that point.

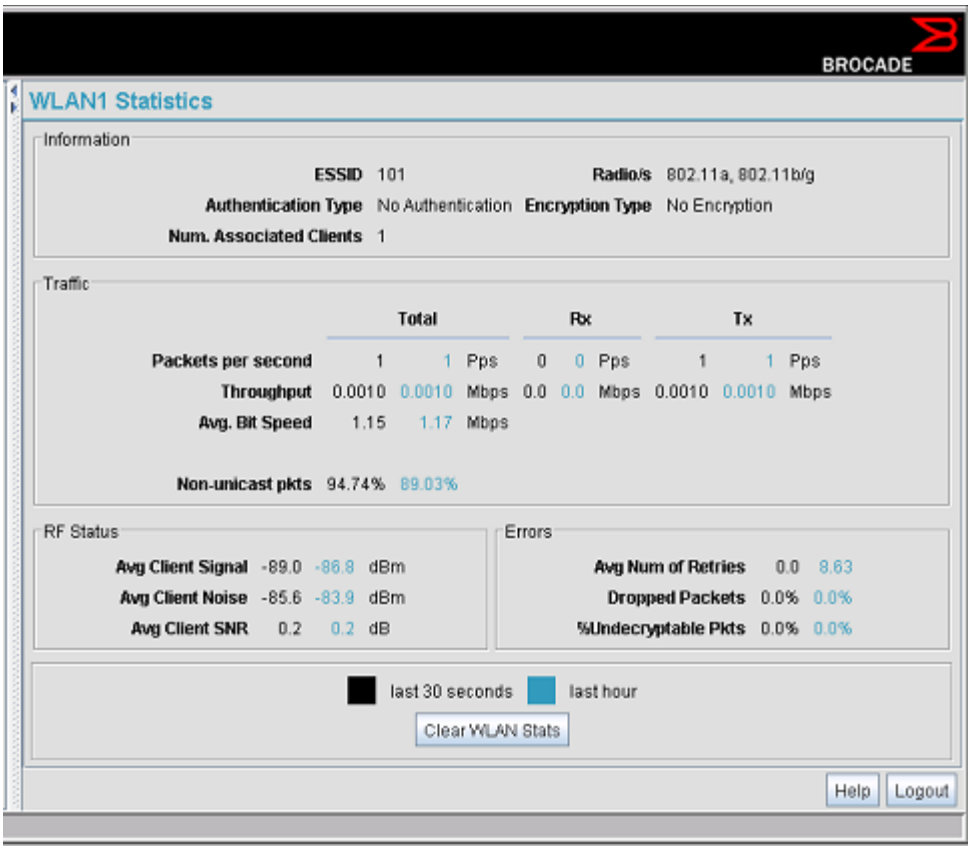
4. Click the *Clear RF Stats* button to reset each of the data collection counters to zero in order to begin new data collections.
5. Click the *Logout* button to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

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 Wireless Clients, 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 clients. 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 Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Information* field to view specific WLAN address, Client and security scheme information for the WLAN selected from the Brocade Mobility 7131 Series Access Point menu tree.

ESSID	Displays the *Extended Service Set ID (ESSID)* for the target WLAN.
Radio/s	Displays the name of the 802.11a/n or 802.11b/g/n radio the target WLAN is using for Brocade Mobility 7131 Series Access Point transmissions.
Authentication Type	Displays the authentication type (802.1x EAP or Kerberos) defined for the WLAN.
Encryption Type	Displays the encryption method defined for the WLAN.
Num. Associated clients	Displays the total number of clients currently associated with the WLAN. If this number seems excessive, consider segregating clients to other WLANs if appropriate.

3. Refer to the *Traffic* field to view performance and throughput information for the WLAN selected from the Brocade Mobility 7131 Series Access Point menu tree.

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 Brocade Mobility 7131 Series Access Point 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 pkts	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 Client signal, noise and performance information for the WLAN selected from the Brocade Mobility 7131 Series Access Point menu tree.

Avg Client Signal	Displays the average RF signal strength in dBm for all clients 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 Client to a different WLAN if a better functional grouping of clients can be determined.
Avg Client Noise	Displays the average RF noise for all clients associated with the selected WLAN. The number in black represents Client noise for the last 30 seconds and the number in blue represents Client noise for the last hour. If Client noise is excessive, consider moving the Client closer to the Brocade Mobility 7131 Series Access Point, or in area with less conflicting network traffic.
Avg Client SNR	Displays the average *Signal to Noise Ratio (SNR)* for all clients associated with the selected WLAN. The Signal to Noise Ratio is an indication of overall RF performance on your wireless networks.

5. Refer to the *Errors* field to view Client association error statistics for the WLAN selected from the Brocade Mobility 7131 Series Access Point menu tree.

Avg Num of Retries	Displays the average number of retries for all clients 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 clients 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 clients 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 access point applet. A prompt displays confirming the logout before the applet is closed.

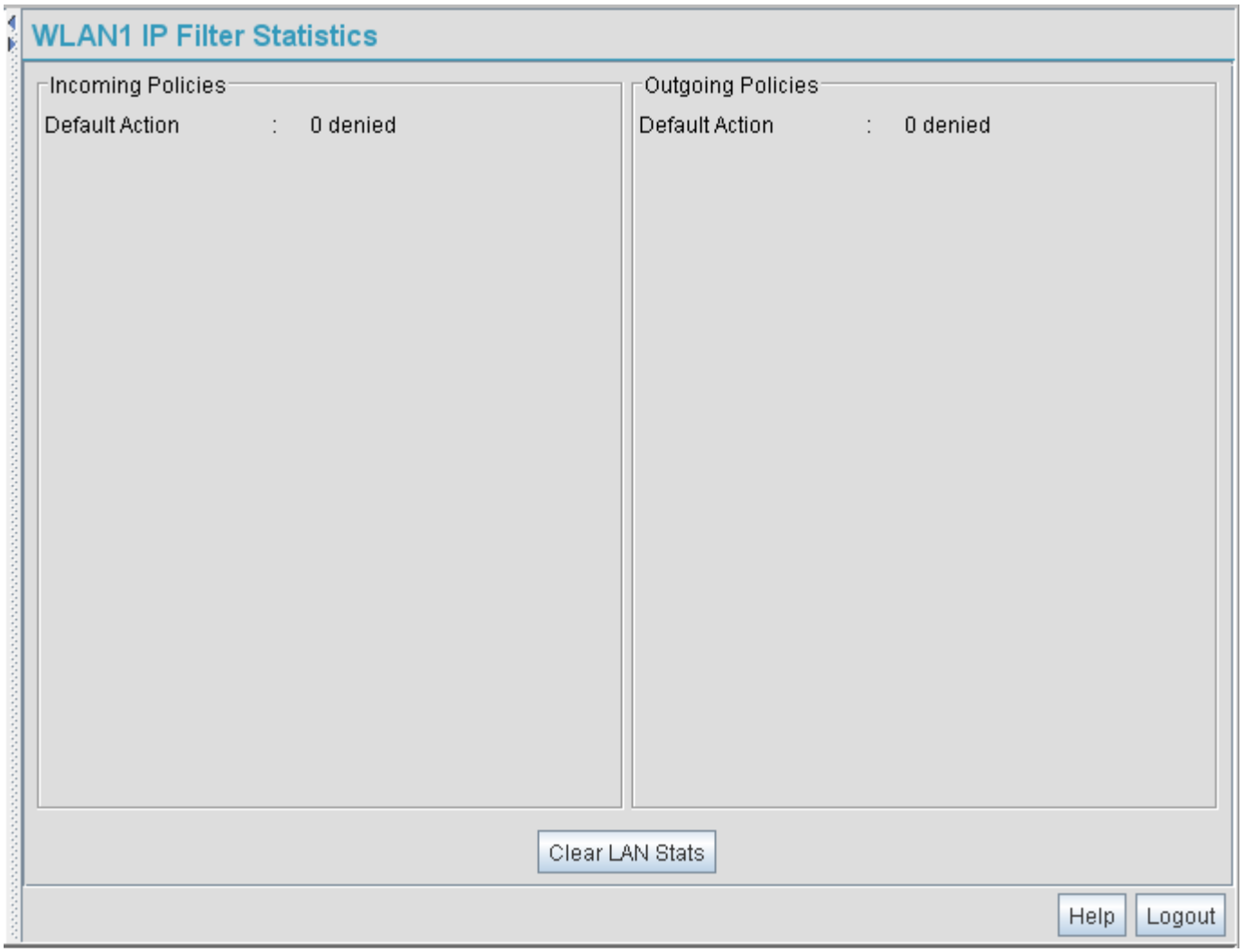
Viewing a WLAN's IP filter statistics

Each access point WLAN has the ability to track its own unique IP filter statistics. Refer to the WLAN IP Filter Stats page to review statistics generated from both incoming and outgoing IP filtering policies supporting impacting the WLAN. The LAN IP Filter Statistics screen shows a running count of packet traffic either allowed or denied when filter rules fail. These rules determine which IP packets are processed normally by the selected WLAN and which are discarded.

For more information on how IP Filtering works and how its configured on the access point, see "Configuring IP filtering" on page 182.

To view access point LAN's IP filter statistics:

1. Select *Status and Statistics* -> *Wireless Stats* -> *WLAN1 Stats* (or any other WLAN) > *IP Filter Stats* from the access point menu tree.



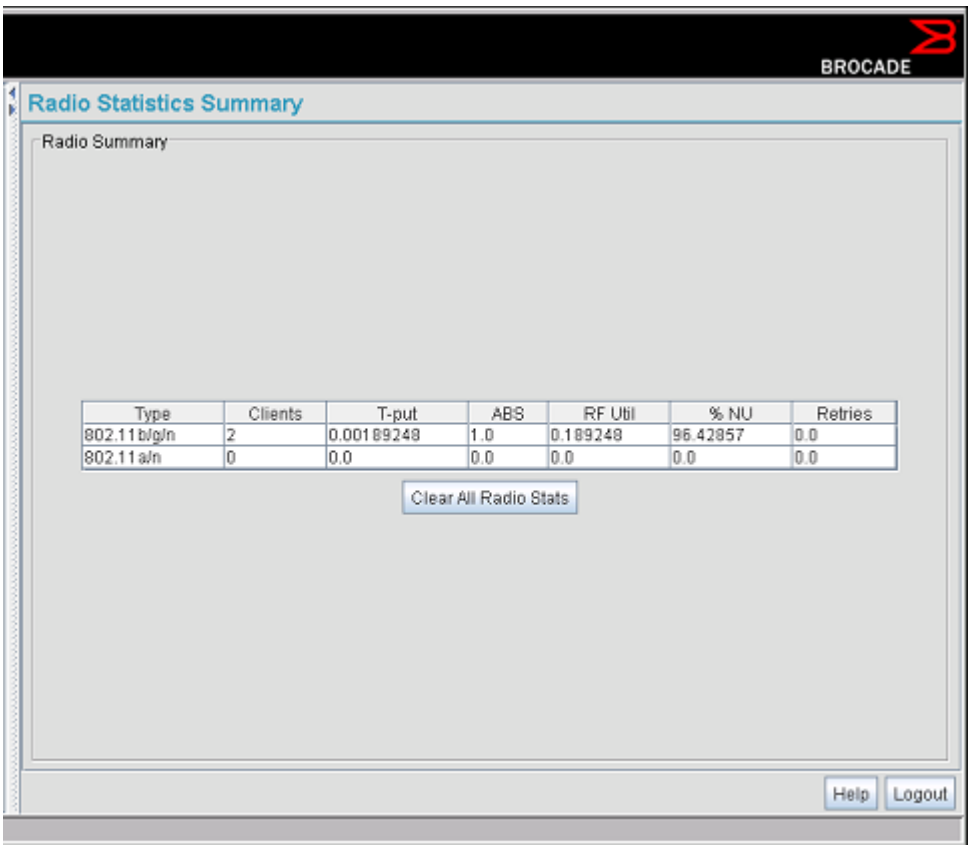
2. Refer to the *Incoming Policies* field to assess the number of packets either allowed or denied access by the access point's filtering rules. These are packets that are incoming to the selected access point WLAN.
3. Refer to the *Outgoing Policies* field to assess the number of packets either allowed or denied access by the access point's filtering rules. These are packets that are outgoing from the selected access point WLAN.
4. Click the *Clear LAN 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 Access Point applet. There will be a prompt confirming logout before the applet is closed.

Viewing radio statistics summary

Select the *Radio Stats Summary* screen to view high-level information (radio name, type, number of associated clients, etc.) for the radio(s) enabled on a Brocade Mobility 7131 Series Access Point. Individual radio statistics can be displayed as well by selecting a specific radio from within the Brocade Mobility 7131 Series Access Point menu tree.

To view high-level Brocade Mobility 7131 Series Access Point radio statistics:

1. Select *Status and Statistics -> Radio Stats* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Radio Summary* field to reference Brocade Mobility 7131 Series Access Point radio information.

Type	Displays the type of radio (either 802.11a/n or 802.11b/g/n) currently deployed by the Brocade Mobility 7131 Series Access Point.
Clients	Displays the total number of clients currently associated with each Brocade Mobility 7131 Series Access Point radio.
T-put	Displays the total throughput in Megabits per second (Mbps) for each Brocade Mobility 7131 Series Access Point radio listed.
ABS	Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each Brocade Mobility 7131 Series Access Point radio.

RF Util	Displays the approximate RF Utilization for each Brocade Mobility 7131 Series Access Point radio
% NU	Displays the percentage of the total packets that are non-unicast. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries per packet on each radio. A high number could indicate network or hardware problems.

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 Brocade Mobility 7131 Series Access Point radio type displayed within the AP Stats Summary screen, see "Viewing radio statistics" on page 276.

4. Click the *Logout* button to securely exit the Access Point applet.

Viewing radio statistics

Refer to the *Radio Stats* screen to view detailed information for the Brocade Mobility 7131 Series Access Point radio (either 802.11a/n or 802.11b/g/n) 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 Client signal, noise and signal to noise ratio information. Finally, the *Errors* field displays retry information as well as data transmissions the Brocade Mobility 7131 Series Access Point radio either dropped or could not decrypt. The information within the 802.11a/n Radio Statistics screen is view-only with no configurable data fields.

To view detailed radio statistics:

1. Select *Status and Statistics -> Radio Stats -> Radio1(802.11b/g/n) Stats* from the Brocade Mobility 7131 Series Access Point menu tree.

2. Refer to the *Information* field to view the Brocade Mobility 7131 Series Access Point 802.11a/n or 802.11b/g/n radio's MAC address, placement and transmission information.

HW Address	The *Media Access Control (MAC)* address of the Brocade Mobility 7131 Series Access Point housing the 802.11a/n radio. The MAC address is set at the factory and can be found on the bottom of the access point.
Radio Type	Displays the radio type (either 802.11a/n or 802.11b/g/n).
Power	The power level in milliwatts (mW) for RF signal strength.
Active WLANs	Lists the Brocade Mobility 7131 Series Access Point WLANs adopted by the 802.11a/n or 802.11b/g/n radio.
Placement	Lists whether the Brocade Mobility 7131 Series Access Point radio is indoors or outdoors.
Current Channel	Indicates the channel for communications between the Brocade Mobility 7131 Series Access Point radio and its associated clients.
Num Associated Clients	Lists the number of wireless clients currently associated with the Brocade Mobility 7131 Series Access Point 802.11a/n or 802.11b/g/n radio.

3. Refer to the *Traffic* field to view performance and throughput information for the target Brocade Mobility 7131 Series Access Point 802.11a/n or 802.11b/g/n radio.

Pkts per second	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.
Throughput	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.
Avg. Bit Speed	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.
Approximate RF Utilization	The approximate RF utilization of the Brocade Mobility 7131 Series Access Point 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.
% Non-unicast pkts	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.

4. Refer to the *RF Status* field to view the following Client signal, noise and performance information for the target Brocade Mobility 7131 Series Access Point 802.11a/n or 802.11b/g/n radio.

Avg Client Signal	Displays the average RF signal strength in dBm for all clients 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 Client to a different WLAN, if a better functional grouping of clients can be determined.
Avg Client Noise	Displays the average RF noise for all clients associated with the Brocade Mobility 7131 Series Access Point radio. The number in black represents Client noise for the last 30 seconds and the number in blue represents Client noise for the last hour. If Client noise is excessive, consider moving the Client closer to the Brocade Mobility 7131 Series Access Point, or in area with less conflicting network traffic.
Avg Client SNR	Displays the average *Signal to Noise Ratio (SNR)* for all clients associated with the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point 802.11a/n 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 clients associated with the Brocade Mobility 7131 Series Access Point 802.11a/n or 802.11b/g/n 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 clients associated with the Brocade Mobility 7131 Series Access Point 802.11a/n or 802.11b/g/n 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 clients associated with the 802.11a/n or 802.11b/g/n 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 Access Point applet.

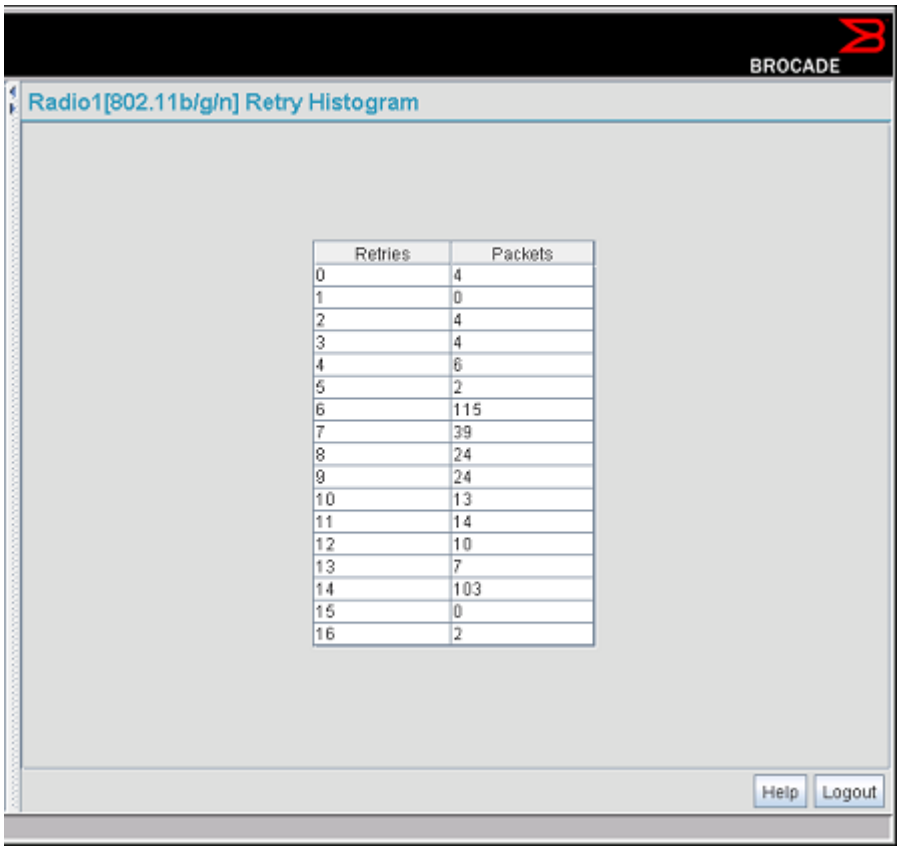
Retry histogram

Refer to the *Retry Histrogram* screen for an overview of the retries transmitted by an access point 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 access point radio:

1. Select *Status and Statistics -> Radio Stats -> Radio1(802.11b/g/n) Stats -> Retry Histogram* from the Brocade Mobility 7131 Series Access Point menu tree.

   A Radio Histogram screen is available for each access point 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 access point 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 access point radio to achieve better performance.

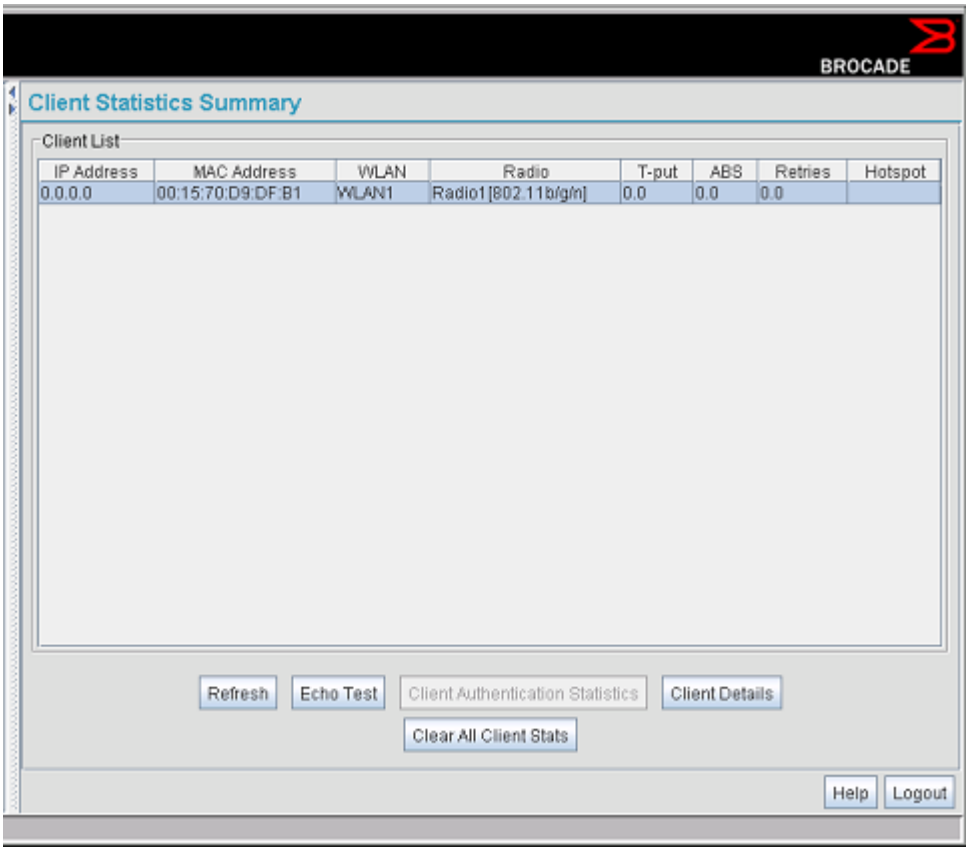
2. Click *Apply* to save any changes to the Radio Histogram screen. Navigating away from the screen without clicking Apply results in changes to the screens being lost.
3. Click *Undo Changes* (if necessary) to undo any changes made to the screen. Undo Changes reverts the settings to the last saved configuration.
4. Click *Logout* to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing client statistics summary

Use the *Client Stats Summary* screen to display overview statistics for wireless clients associated with the Brocade Mobility 7131 Series Access Point. The *Client List* field displays basic information such as IP Address and total throughput for each associated Client. The Client Stats screen is view-only with no user configurable data fields. However, individual clients can be selected from within the Client Stats Summary screen to either ping to assess interoperability or display authentication statistics.

To view Brocade Mobility 7131 Series Access Point overview statistics for all of the clients associated to the Brocade Mobility 7131 Series Access Point:

1. Select *Status and Statistics - > Client Stats* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Refer to the *Client List* field to reference associated Client address, throughput and retry information.

IP Address	Displays the IP address of each of the associated Client.
MAC Address	Displays the MAC address of each of the associated Client.
WLAN	Displays the WLAN name each Client is interoperating with.
Radio	Displays the name of the 802.11a/n or 802.11b/g/n radio each Client is associated with.
T-put	Displays the total throughput in Megabits per second (Mbps) for each associated Client.
ABS	Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each associated Client.
Retries	Displays the average number of retries per packet. A high number retries could indicate possible network or hardware problems.
Hotspot	Displays whether this radio is currently supporting a hotspot.

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 Client.

NOTE
An echo test initiated from the Brocade Mobility 7131 Series Access Point *Client Stats Summary* screen uses WNMP pings. Therefore, target clients that are not Motorola clients are unable to respond to the echo test.

5. Click the *Client Authentication Statistics* button to display a screen with detailed authentication statistics for the Client.

   For information on individual Client authentication statistics, see "Client authentication statistics" on page 284.
6. Click the *Client Details* button to display a screen with detailed statistics for a selected Client.

   For detailed information on individual Client authentication statistics, see "Viewing Client details" on page 282.
7. Click the *Clear All Client Stats* button to reset each of the data collection counters to zero in order to begin new data collections.
8. Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

Viewing Client details

Use the *Client Details* screen to display throughput, signal strength and transmit error information for a specific Client associated with the Brocade Mobility 7131 Series Access Point.

The Client Details screen is separated into four fields; *Client Properties*, *Client Traffic*, *Client Signal*, and *Client Errors*. The *Client Properties* field displays basic information such as hardware address, IP address, and associated WLAN and AP. Reference the *Client Traffic* field for Client RF traffic and throughput data. Use the *RF Status* field to reference information on RF signal averages from the target Client. The *Error* field displays RF traffic errors based on retries, dropped packets and undecryptable packets. The Client Details screen is view-only with no user configurable data fields.

To view details specific to an individual Client:

1. Select *Status and Statistics -> Client Stats* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Highlight a specific Client.
3. Select the *Client Details* button.
4. Refer to the *Client Properties* field to view Client address information.

IP Address	Displays the IP address of the Client.
WLAN Association	Displays the name of the WLAN the Client is associated with. Use this information to assess whether the Client is properly grouped within that specific WLAN.

PSP State	Displays the current PSP state of the Client. The *PSP Mode* field has two potential settings. PSP indicates the Client is operating in Power Save Protocol mode. In PSP, the Client runs enough power to check for beacons and is otherwise inactive. CAM indicates the Client is continuously aware of all radio traffic. Brocade recommends CAM for those clients transmitting with the AP frequently and for periods of time of two hours.
HW Address	Displays the *Media Access Control (MAC)* address for the Client.
Radio Association	Displays the name of the AP Client is currently associated with.
QoS Client Type	Displays the data type transmitted by the client. Possible types include *Legacy*, *Voice*, *WMM Baseline* and *Power Save*.
Encryption	Displays the encryption scheme deployed by the associated Client.

5. Refer to the *Traffic* field to view individual Client RF throughput information.

Packets per second	The *Total* column displays average total packets per second crossing the Client. The *Rx* column displays the average total packets per second received on the Client. The *Tx* column displays the average total packets per second sent on the Client. 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 Client. The *Rx* column displays the average total packets per second received on the Client. The *Tx* column displays the average total packets per second sent on the Client. 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 Client. 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. The associated Client must also be set to the higher rate to interoperate with the Brocade Mobility 7131 Series Access Point at that data rate.
% of Non-unicast pkts	Displays the percentage of the total packets for the selected client 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 Client signal and signal disturbance information.

Avg Client Signal	Displays RF signal strength in dBm for the target Client. 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 Client Noise	Displays RF noise for the target Client. The number in black represents noise for the last 30 seconds, the number in blue represents noise for the last hour.
Avg Client SNR	Displays the *Signal to Noise Ratio (SNR)* for the target Client. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7. Refer to the *Errors* field to view Client retry information and statistics on packets not transmitted.

Avg Num of Retries	Displays the average number of retries for the Client. 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 Client. 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 Client. 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.

Client authentication statistics

The Brocade Mobility 7131 Series Access Point can access and display authentication statistics for individual clients.

To view Brocade Mobility 7131 Series Access Point authentication statistics for a specific Client:

1. Select *Status and Statistics - > Client Stats* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Highlight a target Client from within the *Client List* field.
3. Click the *Client Authentication Statistics* button

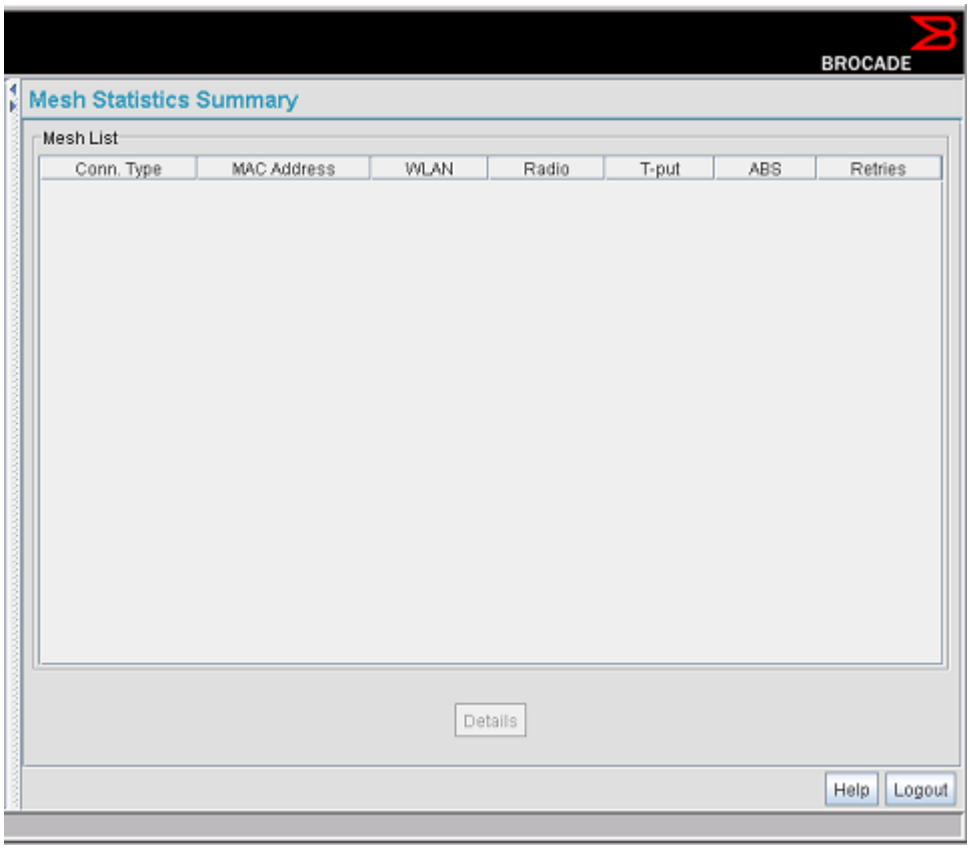
   Use the displayed statistics to determine if the target Client would be better served with a different Brocade Mobility 7131 Series Access Point WLAN or Brocade Mobility 7131 Series Access Point radio.
4. Click *Ok* to return to the Client Stats Summary screen.

Viewing the mesh statistics summary

The Brocade Mobility 7131 Series Access Point has the capability of detecting and displaying the properties of other access points in mesh network (either base bridges or client bridges) mode. This information is used to create a list of known wireless bridges.

To view detected mesh network statistics:

1. Select *Status and Statistics -> Mesh Stats* from the Brocade Mobility 7131 Series Access Point menu tree.

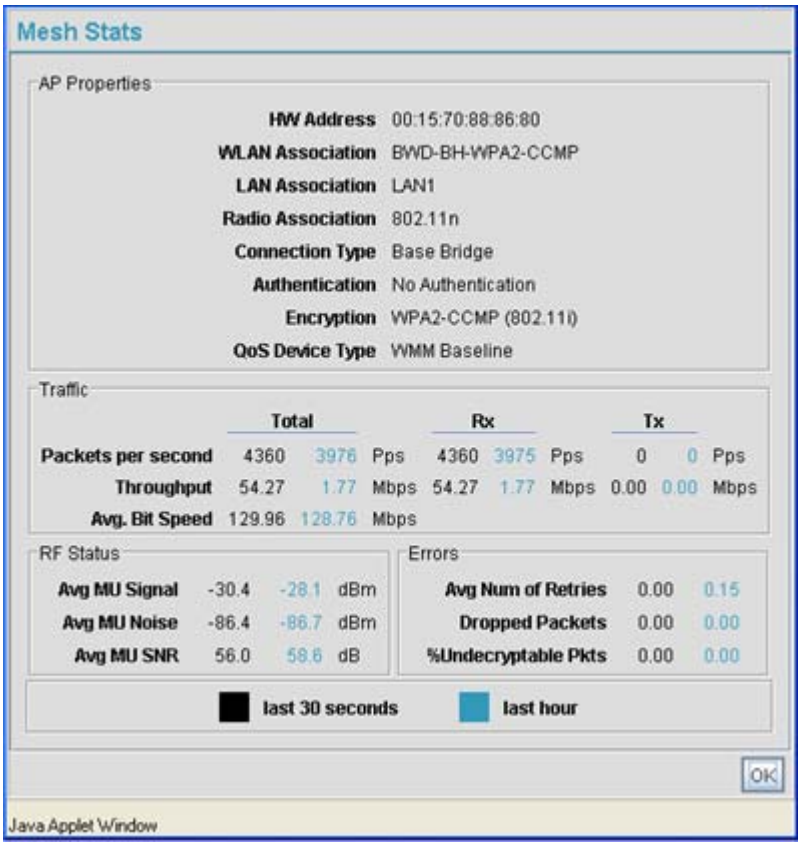


The *Mesh Statistics Summary* screen displays the following information:

Conn Type	Displays whether the bridge has been defined as a base bridge or a client bridge.
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.
WLAN	Displays the WLAN name each wireless bridge is interoperating with.
Radio	Displays the name of the 802.11a/n or 802.11b/g/n radio each bridge is associated with.
T-put	Displays the total throughput in Megabits per second (Mbps) for each associated bridge.
ABS	Displays the *Average Bit Speed (ABS)* in Megabits per second (Mbps) for each associated bridge.
Retries	Displays the average number of retries per packet. A high number retries could indicate possible network or hardware problems.

2. Click the *Refresh* button to update the display of the Mesh Statistics Summary screen to the latest values.

3. Click the *Details* button to display AP properties and radio information for those access points in a mesh configuration with this detecting access point.



4. Click the *Logout* button to securely exit the Access Point applet. A prompt displays confirming the logout before the applet is closed.

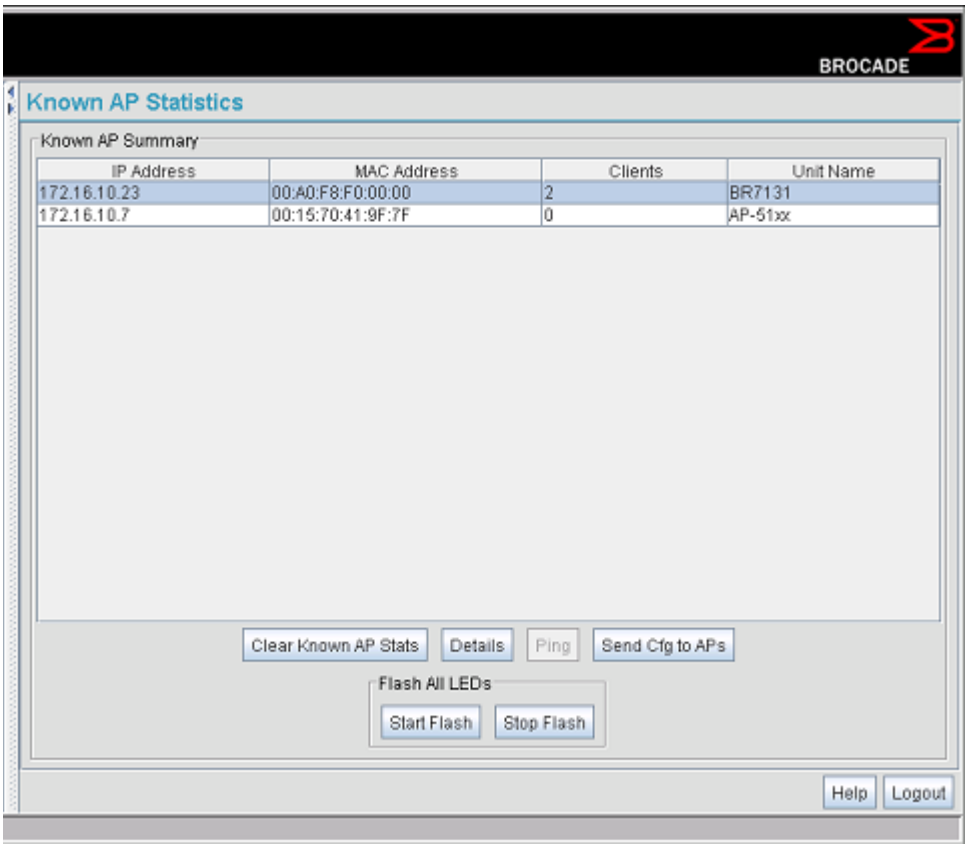
Viewing known access point statistics

The Brocade Mobility 7131 Series Access Point has the capability of detecting and displaying the properties of other Brocade access points located within its coverage area. Detected Brocade Mobility 7131 Series Access Point'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.

NOTE
The *Known AP Statistics* screen only displays statistics for access points located on the same subnet.

To view detected access point statistics:

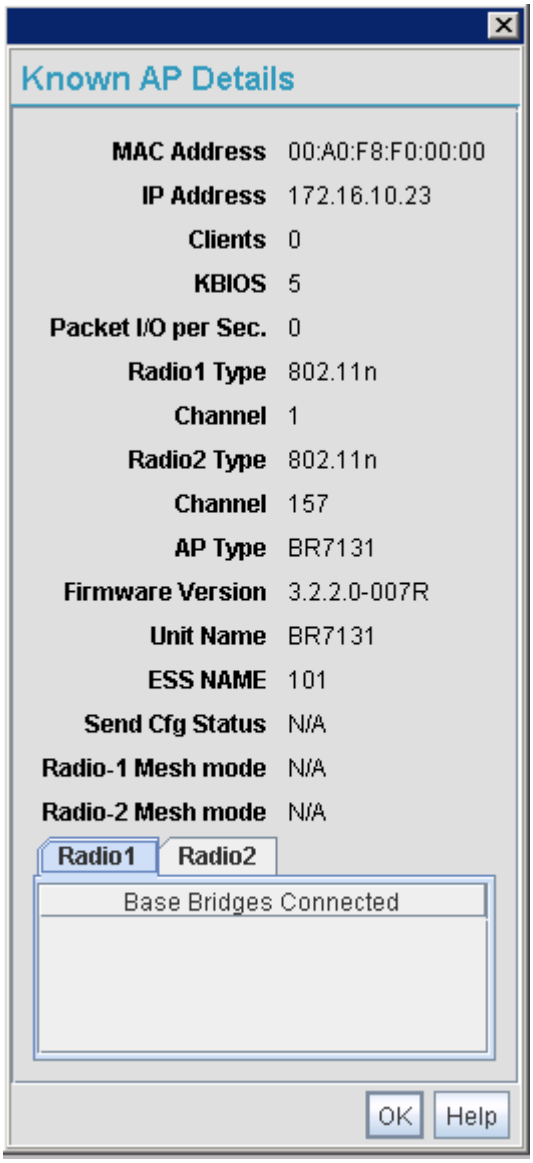
1. Select *Status and Statistics* -> *Known AP Stats* from the Brocade Mobility 7131 Series Access Point menu tree.



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.
Clients	The number clients associated with the located Brocade Mobility 7131 Series Access Point.
Unit Name	Displays the name assigned to the Brocade Mobility 7131 Series Access Point using the System Settings screen.

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 access point address and radio information.



The Known AP Details screen displays the target AP's MAC address, IP address, radio channel, number of associated clients, packet throughput per second, radio type(s), model, firmware version, ESS and client bridges currently connected to the AP radio. Use this information to determine whether this AP provides better Client association support than the locating access point or warrants consideration as a member of a different mesh network.

4. Click the *Ping* button to display a screen for verifying the link with a highlighted access point.

NOTE
A ping test initiated from the Brocade Mobility 7131 Series Access Point *Known AP Statistics* screen uses WNMP pings. Therefore, target devices that are not Brocade access points are unable to respond to the ping test.

5. Click the *Send Cfg to APs* button to send the your access point's configuration to other access point's. The recipient access point must be the same single or dual-radio model as the access point sending the configuration. The sending and recipient access point's must also be running the same major firmware version.

CAUTION

When using the Send Cfg to APs function to migrate an access point's configuration to other access points, it is important to keep in mind mesh network configuration parameters do not get completely sent to other access points. The Send Cfg to APs function will not send the "auto-select" and "preferred list" settings. Additionally, LAN1 and LAN2 IP mode settings will only be sent if the sender's AP mode is DHCP or BOOTP. The WAN's IP mode will only be sent if the sender's IP mode is DHCP.

6. Click the *Start Flash* button to flash the LEDs of other Brocade Mobility 7131 Series Access Points 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 a Brocade Mobility 7131 Series Access Point is highlighted and the Start Flash button is selected, the LEDs on the selected Brocade Mobility 7131 Series Access Point flash. When the *Stop Flash* button is selected, the LEDs on the selected Brocade Mobility 7131 Series Access Point go back to normal operation.

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

Chapter

CLI Reference

8

In this chapter

- Connecting to the CLI 291
- Admin and common commands. 292
- Network commands 300
- Network IP Filter Commands 456
- Statistics commands. 567

The Brocade Mobility 7131 Series Access Point *Command Line Interface (CLI)* is accessed through the serial port or a Telnet session. The Brocade Mobility 7131 Series Access Point 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 CLI treats the following as invalid characters:

< > | " & \ ? ,

In order to avoid problems when using the CLI, these characters should be avoided.

Connecting to the CLI

Accessing the CLI through the serial port

To connect to the Brocade Mobility 7131 Series Access Point CLI through the serial port:

1. Connect one end of a null modem serial cable to the Brocade Mobility 7131 Series Access Point’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 *admin123*. If this is your first time logging into the access point, you are unable to access any of the access point’s commands until the country code is set. A new password will also need to be created.

Accessing the CLI via Telnet

To connect to the Brocade Mobility 7131 Series Access Point CLI through a Telnet connection:

1. If this is your first time connecting to your access point, keep in mind the access point uses a static IP WAN address (10.1.1.1). Additionally, the access point's LAN port is set as a DHCP client.
2. Enter the default username of *admin* and the default password of *admin123*. If this is your first time logging into the access point, you are unable to access any of the access point's commands until the country code is set. A new password will also need to be created.

Admin and common commands

BR7131>admin>

Description

Displays admin configuration options. The items available under this command are shown below.

Syntax

help	Displays general user interface help.
passwd	Changes the admin password.
summary	Shows a system summary.
network	Goes to the network submenu
system	Goes to the system submenu.
stats	Goes to the stats submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>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
                             : resposne from CLI.

admin>
```

BR7131>admin>passwd

Description

Changes the password for the admin login.

Syntax

passwd	Changes the admin password for Brocade Mobility 7131 Series Access Point access. This requires typing the old admin password and entering a new password and confirming it. Passwords can be up to 11 characters. The access point CLI treats the following as invalid characters: ' " \ & $ ^ * + ? [({ | , < > In order to avoid problems when using the access point CLI, these characters should be avoided.

Example

```
admin>passwd

Old Admin Password:******
New Admin Password (0 - 11 characters):******
Verify Admin Password (0 - 11 characters):******
```

For information on configuring passwords using the applet (GUI), see "Setting passwords" on page 192.

BR7131>admin>summary

Description

Displays the Brocade Mobility 7131 Series Access Point's system summary.

Syntax

summary	Displays a summary of high-level characteristics and settings for the WAN, LAN and WLAN.

Example

```
admin>summary

Brocade Mobility 7131 Series Access Point firmware
version              4.1.0.0-xxx
country code                          us
ap-mode                               independent
serial number                         00A0F8716A74
model                                 MOBILITY7131N

WLAN 1:
WLAN Name                                WLAN1
ESS ID                                   101
Radio Band(s)                            12.4 and 5.0 GHz
VLAN                                     VLAN1
Security Policy                          Default
QoS Policy                               Default
Rate Limiting                            disabled

LAN1 Name: LAN1
LAN1 Mode: enable
LAN1 IP: 0.0.0.0
LAN1 Mask: 0.0.0.0
LAN1 DHCP Mode: client

LAN2 Name: LAN2
LAN2 Mode: enable
LAN2 IP: 192.235.1.1
LAN2 Mask: 255.255.255.0
LAN2 DHCP Mode: client

-------------------------------------------------------------------------------
WAN Interface  IP Address    Network Mask     Default Gateway  DHCP Client
-------------------------------------------------------------------------------

enable         172.20.23.10  255.255.255.192  172.20.23.20     enable
```

For information on displaying a system summary using the applet (GUI), see "Basic device configuration" on page 51.

BR7131>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)>
```

BR7131>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>
```

BR7131>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>
```

BR7131>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
```

Network commands

BR7131>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.

Network LAN commands

BR7131>admin(network.lan)>

Description

Displays the LAN submenu. The items available under this command are shown below.

show	Shows current Brocade Mobility 7131 Series Access Point LAN parameters.
set	Sets LAN parameters.
bridge	Goes to the mesh configuration submenu.
wlan-mapping	Goes to the WLAN/Lan/Vlan Mapping submenu.
dhcp	Goes to the LAN DHCP submenu.
type-filter	Goes to the Ethernet Type Filter submenu.
..	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 LAN configuration options using the applet (GUI), see "Configuring the LAN interface" on page 113.

BR7131>admin(network.lan)> show

Description

Displays the Brocade Mobility 7131 Series Access Point LAN settings.

Syntax

show	Shows the settings for the Brocade Mobility 7131 Series Access Point LAN1 and LAN2 interfaces.

Example

```
admin(network.lan)>show

LAN On Ethernet Port                : LAN1
LAN Ethernet Timeout                : disable

802.1x Port Authentication:
      Username                      : admin
      Password                      : ********

Auto-negoitation                    : disable
Speed                               : 100M
Duplex                              : full

** LAN1 Information **
LAN Name                            : LAN1
LAN Interface                       : enable
802.11q Trunking                    : disable
Native VLAN Tag Mode                : untagged

LAN IP mode                         : DHCP client
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

** LAN2 Information **
LAN Name                            : LAN2
LAN Interface                       : disable
802.11q Trunking                    : disable
Native VLAN Tag Mode                : untagged

LAN IP mode                         : DHCP server
IP Address                          : 192.168.1.1
Network Mask                        : 255.255.255.255
Default Gateway                     : 192.168.1.1
Domain Name                         :
Primary DNS Server                  : 192.168.0.2
Secondary DNS Server                : 192.168.0.3
WINS Server                         : 192.168.0.255

admin(network.lan)>
```

For information on displaying LAN information using the applet (GUI), see "Configuring the LAN interface" on page 113.

BR7131>admin(network.lan)> set

Description

Sets the LAN parameters for the LAN port.

Syntax

set	**lan**	<mode>	Enables or disables the Brocade Mobility 7131 Series Access Point LAN interface.
	name	<idx-name >	Defines the LAN name by index.
	ethernet-port-lan	<idx>	Defines which LAN (LAN1 or LAN2) is active on the Ethernet port.
	timeout	<seconds>	Sets the interval (in seconds) the Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point LAN port.
	native-vlan-tag	<mode>	Defines the untagged/tagged 802.1q native VLAN mode for LAN1 and LAN2.
	auto-negotiation	<mode>	Enables or disables auto-negotiation for the access point LAN port.
	speed	<mbps>	Defines the access point LAN port speed as either 10 Mbps or 100 Mbps.
	duplex	<mode>	Defines the access point LAN port duplex as either half or full.
	username	<name>	Specifies user name for 802.1x port authentication over the LAN interface.
	passwd	<password>	The 0-32 character password for the username for the 802.1x port.
	ip-mode	<ip>	Defines the Brocade Mobility 7131 Series Access Point LAN port IP mode.
	ipadr	<ip>	Sets the IP address used by the LAN port.
	mask	<ip>	Defines the IP address used for Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point LAN port.
	dns	<ip>	Sets the IP address of the primary and secondary DNS servers.
	wins	<ip>	Defines the IP address of the WINS server used by the LAN port.

Example

```
admin(network.lan)>
admin(network.lan)>set lan 1 enable
admin(network.lan)>set name 1 engineering
admin(network.lan)>set ethernet-port-lan 1
admin(network.lan)>set timeout 45
admin(network.lan)>set trunking 1 disable
admin(network.lan)>set native-vlan-tag 1 untagged
admin(network.lan)>set auto-negotiation disable
```

```
admin(network.lan)>set speed 100M
admin(network.lan)>set duplex full
admin(network.lan)>set dns 1 192.168.0.1
admin(network.lan)>set wins 1 192.168.0.254
admin(network.lan)>set trunking disable
admin(network.lan)>set username phil
admin(network.lan)>set passwd ea0258c1
```

Related Commands

show	Shows the current settings for the Brocade Mobility 7131 Series Access Point LAN port.

For information on configuring the LAN using the applet (GUI), see "Configuring the LAN interface" on page 113.

Network LAN, bridge commands

BR7131>admin(network.lan.bridge)>

Description

Displays the Brocade Mobility 7131 Series Access Point Bridge submenu.

show	Displays the mesh configuration parameters for the Brocade Mobility 7131 Series Access Point's LANs.
set	Sets the mesh configuration parameters for the Brocade Mobility 7131 Series Access Point's LANs..
..	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 access point's mesh networking options using the applet (GUI), see "Configuring Mesh Networking" on page 583.

BR7131>admin(network.lan.bridge)> show

Description

Displays the mesh bridge configuration parameters for the Brocade Mobility 7131 Series Access Point's LANs.

Syntax

show	Displays mesh bridge configuration parameters for the Brocade Mobility 7131 Series Access Point's LANs.

Example

```
admin(network.lan.bridge)>show

** LAN1 Bridge Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300

** LAN2 Bridge Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300
```

For an overview of the access point's mesh networking options using the applet (GUI), see "Configuring Mesh Networking" on page 583.

BR7131>admin(network.lan.bridge)> set

Description

Sets the mesh configuration parameters for the Brocade Mobility 7131 Series Access Point's LANs.

Syntax

set	**priority**	<LAN-idx>	<seconds>	Sets bridge priority time in seconds (0-65535) for specified LAN.
	hello	<LAN-idx>	<seconds>	Sets bridge hello time in seconds (0-10) for specified LAN.
	msgage	<LAN-idx>	<seconds>	Sets bridge message age time in seconds (6-40) for specified LAN.
	fwddelay	<LAN-idx>	<seconds>	Sets bridge forward delay time in seconds (4-30) for specified LAN.
	ageout	<LAN-idx>	<seconds>	Sets bridge forward table entry time in seconds (4-3600) for specified LAN.

Example

```
admin(network.lan.bridge)>set priority 2 63335
admin(network.lan.bridge)>set hello 2 2
admin(network.lan.bridge)>set msgage 2 20
admin(network.lan.bridge)>set fwddelay 2 15
admin(network.lan.bridge)>set ageout 2 300

admin(network.lan.bridge)>show

** LAN1 Mesh Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300

** LAN2 Mesh Configuration **
Bridge Priority              :63335
Hello Time (seconds)         :2
Message Age Time (seconds)   :20
Forward Delay Time (seconds) :15

Entry Ageout Time (seconds)  :300
```

For an overview of the access point's mesh networking options using the applet (GUI), see "Configuring Mesh Networking" on page 583.

Network LAN, WLAN-mapping commands

BR7131>admin(network.lan.wlan-mapping)>

Description

Displays the WLAN/Lan/Vlan Mapping submenu.

show	Displays the VLAN list currently defined for the Brocade Mobility 7131 Series Access Point.
set	Sets the Brocade Mobility 7131 Series Access Point VLAN configuration.
create	Creates a new Brocade Mobility 7131 Series Access Point VLAN.
edit	Edits the properties of an existing Brocade Mobility 7131 Series Access Point VLAN.
delete	Deletes a VLAN.
lan-map	Maps Brocade Mobility 7131 Series Access Point existing WLANs to an enabled LAN.
vlan-map	Maps Brocade Mobility 7131 Series Access Point existing 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 access point's VLAN configuration options using the applet (GUI), see "Configuring VLAN support" on page 116.

BR7131>admin(network.lan.wlan-mapping)> show

Description

Displays the VLAN list currently defined for the Brocade Mobility 7131 Series Access Point.. These parameters are defined with the set command.

Syntax

show	**name**	Displays the existing list of VLAN names.
	vlan-cfg	Shows WLAN-VLAN mapping and VLAN configuration.
	lan-wlan	Displays a WLAN-LAN mapping summary.
	wlan	Displays the WLAN summary list.

Example

```
admin(network.lan.wlan-mapping)>show name

-------------------------------------------------------------------------------
Index     VLAN ID   VLAN Name
-------------------------------------------------------------------------------

1         1         VLAN_1
2         2         VLAN_2
3         3         VLAN_3
4         4         VLAN_4

admin(network.lan.wlan-mapping)>show vlan-cfg

-------------------------------------------------------------------------------
LAN No.     Management VLAN Tag      Native VLAN Tag
-------------------------------------------------------------------------------
      1                          1                  1
      2                          1                  1
          WLAN      :WLAN1
mapped to VLAN      :<none>
     VLAN Mode      :static

admin(network.lan.wlan-mapping)>show lan-wlan

WLANs on LAN1:
               :WLAN1
               :WLAN2
               :WLAN3
WLANs on LAN2:

admin(network.lan.wlan-mapping)>show wlan

WLAN1:
WLAN Name              :WLAN1
ESSID                  :101
Radio                  :
VLAN                   :
Security Policy        :Default
QoS Policy             :Default
```

For information on displaying the VLAN screens using the applet (GUI), see “Configuring VLAN support” on page 116.

BR7131>admin(network.lan.wlan-mapping)> set

Description

Sets VLAN parameters for the Brocade Mobility 7131 Series Access Point.

Syntax

set	**mgmt-tag**	<id>	Defines the Management VLAN tag index (1 or 2) to tag number (1-4095).
	native-tag	<id>	Sets the Native VLAN tag index (1 or 2) to tag number (1-4095).
	mode	<wlan-idx>	Sets WLAN VLAN mode (WLAN 1-16) to either dynamic or static.

Example

```
admin(network.lan.wlan-mapping)>set mgmt-tag 1 10
admin(network.lan.wlan-mapping)>set native-tag 1 12
admin(network.lan.wlan-mapping)>set mode 1 static

admin(network.lan.wlan-mapping)>show vlan-cfg

--------------------------------------------------------------------------------
LAN No.     Management VLAN Tag      Native VLAN Tag
--------------------------------------------------------------------------------
      1                          10                  12
      2                          1                   1
          WLAN       :WLAN1
mapped to VLAN       :<none>
     VLAN Mode       :static
```

For information on configuring VLANs using the applet (GUI), see “Configuring VLAN support” on page 116.

BR7131>admin(network.lan.wlan-mapping)> create

Description

Creates a VLAN for the Brocade Mobility 7131 Series Access Point.

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.wlan-mapping)>
admin(network.lan.wlan-mapping)>create 5 vlan-5
```

For information on creating VLANs using the applet (GUI), see “Configuring VLAN support” on page 116.

BR7131>admin(network.lan.wlan-mapping)> edit

Description

Modifies a VLAN's name and ID.

Syntax

edit	**name**	<name>	Modifies an exisiting 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 116.

BR7131>admin(network.lan.wlan-mapping)> delete

Description

Deletes a specific VLAN or all VLANs.

Syntax

delete	< VLAN id>	Deletes a specific VLAN ID (1-16).
	all	Deletes all defined VLAN entries.

For information on deleting VLANs using the applet (GUI), see “Configuring VLAN support” on page 116.

BR7131>admin(network.lan.wlan-mapping)> lan-map

Description

Maps a Brocade Mobility 7131 Series Access Point VLAN to a WLAN.

Syntax

lan-map	<wlan name>	Maps an existing WLAN to an enabled LAN. All names and IDs are case-sensitive.
	<lan name>	Defines enabled LAN name. All names and IDs are case-sensitive.

```
admin(network.lan.wlan-mapping)>lan-map wlan1 lan1
```

For information on mapping VLANs using the applet (GUI), see “Configuring VLAN support” on page 116.

BR7131>admin(network.lan.wlan-mapping)> vlan-map

Description

Maps a Brocade Mobility 7131 Series Access Point VLAN to a WLAN.

Syntax

vlan-map	<wlan name>	Maps an existing WLAN to an enabled LAN. All names and IDs are case-sensitive.
	<vlan name>	Defines the existing VLAN name. All names and IDs are case-sensitive.

```
admin(network.lan.wlan-mapping)>vlan-map wlan1 vlan1
```

For information on mapping VLANs using the applet (GUI), see “Configuring VLAN support” on page 116.

Network LAN, DHCP commands

BR7131>admin(network.lan.dhcp)>

Description

Displays the Brocade Mobility 7131 Series Access Point 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.

BR7131>admin(network.lan.dhcp)> show

Description

Shows DHCP parameter settings.

Syntax

show	Displays DHCP parameter settings for the Brocade Mobility 7131 Series Access Point. These parameters are defined with the set command.

Example

```
admin(network.lan.dhcp)>show
**LAN1 DHCP Information**
DHCP Address Assignment Range:
     Starting IP Address  : 192.168.0.100
     Ending IP Address    : 192.168.0.254

Lease Time           : 86400

**LAN2 DHCP Information**
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 113.

BR7131>admin(network.lan.dhcp)> set

Description

Sets DHCP parameters for the LAN port.

Syntax

set	**range**	<LAN-idx>	<ip1>	<ip2>	Sets the DHCP assignment range from IP address <ip1> to IP address <ip2> for the specified LAN.
	lease	<LAN-idx>	<lease>		Sets the DHCP lease time <lease> in seconds (1-999999) for the specified LAN.

Example

```
admin(network.lan.dhcp)>set range 1 192.168.0.100 192.168.0.254
admin(network.lan.dhcp)>set lease 1 86400

admin(network.lan.dhcp)>show
**LAN1 DHCP Information**
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 113.

BR7131>admin(network.lan.dhcp)> add

Description

Adds static DHCP address assignments.

Syntax

add	<LAN-idx>	<mac>	<ip>	Adds a reserved static IP address to a MAC address for the specified LAN

Example

```
admin(network.lan.dhcp)>add 1 00A0F8112233 192.160.24.6
admin(network.lan.dhcp)>add 1 00A0F1112234 192.169.24.7
admin(network.lan.dhcp)>list 1

-------------------------------------------------------------------------------
Index   MAC Address     IP Address
-------------------------------------------------------------------------------

1       00A0F8112233   192.160.24.6
2       00A0F8112234   192.169.24.7
```

For information on adding client MAC and IP address information using the applet (GUI), see "Configuring advanced DHCP server settings" on page 122.

BR7131>admin(network.lan.dhcp)> delete

Description

Deletes static DHCP address assignments.

Syntax

delete	<LAN-idx>	<entry>	Deletes the static DHCP address entry for the specified LAN.
	<LAN-idx>	**all**	Deletes all static DHCP addresses.

Example

```
admin(network.lan.dhcp)>list 1

-------------------------------------------------------------------------------
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 1 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 122.

BR7131>admin(network.lan.dhcp)> list

Description

Lists static DHCP address assignments.

Syntax

list	<LAN-idx>	Lists the static DHCP address assignments for the specified LAN (1-LAN1, 2 LAN2).

Example

```
admin(network.lan.dhcp)>list 1

------------------------------------------------------------------------------
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)>
```

For information on listing client MAC and IP address information using the applet (GUI), see "Configuring advanced DHCP server settings" on page 122.

Network Type Filter commands

BR7131>admin(network.lan.type-filter)>

Description

Displays the Brocade Mobility 7131 Series Access Point 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.

BR7131>admin(network.lan.type-filter)> show

Description

Displays the Brocade Mobility 7131 Series Access Point's current Ethernet Type Filter configuration.

Syntax

show	<LAN-idx>	Displays the existing Type-Filter configuration for the specified LAN.

Example

```
admin(network.lan.type-filter)>show 1

Ethernet Type Filter mode              : allow
--------------------------------------------------------------------------------
index                   ethernet type
--------------------------------------------------------------------------------
1                       8137
```

For information on displaying the type filter configuration using the applet, see "Setting the type filter configuration" on page 124.

BR7131>admin(network.lan.type-filter)> set

Description

Defines the Brocade Mobility 7131 Series Access Point Ethernet Type Filter configuration.

Syntax

set	**mode**	<LAN-idx>	<mode> allow or deny	Allows or denies the Brocade Mobility 7131 Series Access Point from processing a specified Ethernet data type for the specified LAN.

Example

```
admin(network.lan.type-filter)>set mode 1 allow
```

For information on configuring the type filter settings using the applet (GUI), see "Setting the type filter configuration" on page 124.

BR7131>admin(network.lan.type-filter)> add

Description

Adds an Ethernet Type Filter entry.

Syntax

add	<LAN-idx>	<type>	Adds entered Ethernet Type to list of data types either allowed or denied Brocade Mobility 7131 Series Access Point processing permissions for the specified LAN (either LAN1 or LAN2).

Example

```
admin(network.lan.type-filter)>

admin(network.wireless.type-filter)>add 1 8137
admin(network.wireless.type-filter)>add 2 0806
admin(network.wireless.type-filter)>show 1

Ethernet Type Filter mode              : allow
-------------------------------------------------------------------------------
index                  ethernet type
-------------------------------------------------------------------------------
1                      8137
2                      0806
3                      0800
4                      8782
```

For information on configuring the type filter settings using the applet (GUI), see “Setting the type filter configuration” on page 124.

BR7131>admin(network.lan.type-filter)> delete

Description

Removes an Ethernet Type Filter entry individually or the entire Type Filter list.

Syntax

delete	<LAN-idx>	<index>	Deletes the specified Ethernet Type index entry (1 through 16).
	<LAN-idx>	**all**	Deletes all Ethernet entries currently in list.

Example

```
admin(network.lan.type-filter)>delete 1 1
admin(network.lan.type-filter)>show 1

Ethernet Type Filter mode              : allow
-------------------------------------------------------------------------------
index                  ethernet type
-------------------------------------------------------------------------------
1                      0806
2                      0800
3                      8782

admin(network.lan.type-filter)>delete 2 all
admin(network.lan.type-filter)>show 2

Ethernet Type Filter mode              : allow
-------------------------------------------------------------------------------
index                  ethernet type
-------------------------------------------------------------------------------
```

For information on configuring the type filter settings using the applet (GUI), see "Setting the type filter configuration" on page 124.

Network WAN commands

BR7131>admin(network.wan)>

Description

Displays the WAN submenu. The items available under this command are shown below.

show	Displays the Brocade Mobility 7131 Series Access Point WAN configuration and the Brocade Mobility 7131 Series Access Point's current PPPoE configuration.
set	Defines the Brocade Mobility 7131 Series Access Point's WAN and PPPoE configuration.
delete	Deletes WWAN CRM remote gateways.
nat	Displays the NAT submenu, wherein Network Address Translations (NAT) can be defined.
vpn	Goes to the VPN submenu, where the Brocade Mobility 7131 Series Access Point VPN tunnel configuration can be set.
content	Goes to the outbound content filtering menu.
dyndns	Displays the Dynamic DNS submenu, wherein dyndns settings can be defined.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the Brocade Mobility 7131 Series Access Point system flash.
quit	Quits the CLI and exits the current session.

For an overview of the WAN configuration options using the applet (GUI), see "Configuring WAN settings" on page 125.

BR7131>admin(network.wan)> show

Description

Displays the Brocade Mobility 7131 Series Access Point 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

Status                              : enable
Primary DNS Server                  : 0.0.0.0
Secondary DNS Server                : 0.0.0.0

Auto-negotiation                    : disable
Speed                               : 100M
Duplex                              : full

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
PPPoE State

admin(network.wan)>
```

For an overview of the WAN configuration options available using the applet (GUI), see "Configuring WAN settings" on page 125.

BR7131>admin(network.wan)> set

Description

Defines the configuration of the Brocade Mobility 7131 Series Access Point WAN port.

Syntax

set	**wan**	**enable/disable**		Enables or disables the Brocade Mobility 7131 Series Access Point WAN port.
	dhcp	**enable/disable**		Enables or disables WAN DHCP Client mode.
	ipadr	<idx>	<a.b.c.d>	Sets up to 8 (using <indx> from 1 to 8) IP addresses <a.b.c.d> for the Brocade Mobility 7131 Series Access Point WAN interface.
	mask	<a.b.c.d>		Sets the subnet mask for the Brocade Mobility 7131 Series Access Point WAN interface.
	dgw	<a.b.c.d>		Sets the default gateway IP address to <a.b.c.d>.
	dns	<idx>	<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.
	auto-negotiation	**enable/disable**		Enables or disables auto-negotiation for the access point WAN port.
	speed	<mbps>		Defines the access point WAN port speed as either 10 Mbps or 100 Mbps.
	duplex	<mode>		Defines the access point WAN port duplex as either half or full.
	pppoe	**mode**	**enable/disable**	Enables or disables PPPoE.
		user	<name>	Sets PPPoE user name.
		passwd	<password>	Defines the PPPoE password.
		ka	**enable/disable**	Enables or disables PPPoE keepalive.
		idle	<time>	Sets PPPoE idle time.
		type	<auth-type>	Sets PPPoE authentication type.

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 auto-negotiation disable
admin(network.wan)>set speed 10M
admin(network.wan)>set duplex half
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 jk
```

```
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 WAN configuration options available using the applet (GUI), see "Configuring WAN settings" on page 125.

Network WAN NAT commands

BR7131>admin(network.wan.nat)>

Description

Displays the NAT submenu. The items available under this command are shown below.

show	Displays the Brocade Mobility 7131 Series Access Point's current NAT parameters for the specified index.
set	Defines the Brocade Mobility 7131 Series Access Point 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 NAT configuration options available using the applet (GUI), see "Configuring Network Address Translation (NAT) settings" on page 131.

BR7131>admin(network.wan.nat)> show

DescriptionDescription:

Displays Brocade Mobility 7131 Series Access Point NAT parameters.

Syntax

show	<idx> <cr>	Displays Brocade Mobility 7131 Series Access Point NAT parameters for the specified NAT index (1-8).

Example

```
admin(network.wan.nat)>show 2

WAN IP Mode                          : enable
WAN IP Address                       : 157.235.91.2
NAT Type                             : 1-to-many
Inbound Mappings                     : Port Forwarding

unspecified port forwarding mode  : enable
unspecified port fwd. ip address  : 111.223.222.1
one to many nat mapping

-------------------------------------------------------------------------------
--
LAN No.               WAN IP
-------------------------------------------------------------------------------
--
1                    157.235.91.2
2                    157.235.91.2

admin(network.wan.nat)>
```

For an overview of the NAT options available using the applet (GUI), see “Configuring Network Address Translation (NAT) settings” on page 131.

BR7131>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>.
	inb	<index>	<ip> <mode>	Sets inbound IP address for specified index <index> <ip address> Sets inbound mode for specified index <index> <enable/disable>
	outb	<index>	<ip> <from> <to>	Sets outbound IP address for specified index <index> <ip address> Sets outbound NAT destination <LAN1 or LAN2> <WAN ip 1-8 or None>.

Example

```
admin(network.wan.nat)>set type 2 1-to-many
admin(network.wan.nat)>set ip 2 10.1.1.1 (this command is used when NAT is
1-to-1)

admin(network.wan.nat)>show 2

WAN IP Mode                          : enable
WAN IP Address                       : 157.235.91.2
NAT Type                             : 1-to-many
Inbound Mappings                     : Port Forwarding

unspecified port forwarding mode  : enable
unspecified port fwd. ip address  : 111.223.222.1
one to many nat mapping

------------------------------------------------------------------------------
--
LAN No.               WAN IP
------------------------------------------------------------------------------
--
1                     157.235.91.2
2                     10.1.1.1
```

For an overview of the NAT options available using the applet (GUI), see “Configuring Network Address Translation (NAT) settings” on page 131.

BR7131>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    Transport  start port   end port   internal ip     translation

-------------------------------------------------------------------------------

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 NAT options available using the applet (GUI), see “Configuring Network Address Translation (NAT) settings” on page 131.

BR7131>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    Transport  start port   end port   internal ip     translation

-------------------------------------------------------------------------------

1       special tcp        20          21         192.168.42.16   21

admin(network.wan.nat)>delete 1 1
admin(network.wan.nat)>list 1
-------------------------------------------------------------------------------

index   name    Transport  start port   end port   internal ip     translation

-------------------------------------------------------------------------------
```

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 NAT options available using the applet (GUI), see “Configuring Network Address Translation (NAT) settings” on page 131.

BR7131>admin(network.wan.nat)> list

Description

Lists Brocade Mobility 7131 Series Access Point NAT entries for the specified index.

Syntax

list	<idx>	Lists the inbound NAT entries associated with the WAN index (1-8).

Example

```
admin(network.wan.nat)>list 1
-------------------------------------------------------------------------------

index   name    Transport  start port   end port   internal ip     translation

-------------------------------------------------------------------------------

1       special tcp        20           21         192.168.42.16   21
```

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 NAT options available using the applet (GUI), see "Configuring Network Address Translation (NAT) settings" on page 131.

Network WAN, VPN commands

BR7131>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 VPN options available using the applet (GUI), see "Configuring VPN tunnels" on page 220.

BR7131>admin(network.wan.vpn)> add

Description

Adds a VPN tunnel entry.

Syntax

add	<name>	<idx>	<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 2 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)>
```

For information on configuring VPN using the applet (GUI), see “Configuring VPN tunnels” on page 220.

BR7131>admin(network.wan.vpn)> set

Description

Sets VPN entry parameters.

Syntax

set	**type**	<name>	<tunnel type>	Sets the tunnel type <name> to **Auto** or **Manual** for the specified tunnel name.
	authalgo	<name>	<authalgo>	Sets the authentication algorithm for <name> to (**None**, **MD5**, or **SHA1**).
	authkey	<name>	<dir> <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	<name>	<esptype>	Sets the Encapsulating Security Payload (ESP) type. Options include **None**, **ESP**, or **ESP-AUTH**.
	esp-encalgo	<name>	<escalgo>	Sets the ESP encryption algorithm. Options include **DES**, **3DES**, **AES128**, **AES192**, or **AES256**).
	esp-enckey	<name>	<dir> <enckey>	Sets the Manual Encryption Key in ASCII for tunnel <name> and direction **IN** or **OUT** to the key <enc-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	<name>	<authalgo>	Sets the ESP authentication algorithm. Options include **MD5** or **SHA1**.
	esp-authkey	<name>	<dir> <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**, then provide 32 hex characters. If authalgo is set to **SHA1**, provide 40 hex characters.

spi	<name>	<algo> <dir>	<value>	Sets 6 character **IN**(bound) or **OUT**(bound) for **AUTH** (Manual Authentication) or **ESP** for <name> to <spi> (a hex value more than 0xFF) <value>.
usepfs	<name>	<mode>		Enables or disables Perfect Forward Secrecy for <name>.
salife	<name>	<lifetime>		Defines the name of the tunnnel <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 **Aggr**(essive).
	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> (**PSK** or **RSA**).
	authalgo	<name>	<authalgo>	Sets the IKE Authentication Algorithm for <name> to **MD5** or **SHA1**.
	phrase	<name>	<phrase>	Sets the IKE Authentication passphrase 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 life time 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 220.

BR7131>admin(network.wan.vpn)> delete

Description

Deletes VPN tunnel entries.

Syntax

delete	**all**	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
-------------------------------------------------------------------------
Eng2EngAnnex  Manual  192.168.32.2/24    192.168.33.1    192.168.24.198
SJSharkey     Manual  206.107.22.45/27   206.107.22.2    209.235.12.55

admin(network.wan.vpn)>delete Eng2EngAnnex
admin(network.wan.vpn)>list
-------------------------------------------------------------------------
Tunnel Name   Type    Remote IP/Mask     Remote Gateway  Local WAN IP
-------------------------------------------------------------------------
SJSharkey     Manual  206.107.22.45/27   206.107.22.2    209.235.12.55

admin(network.wan.vpn)>
```

For information on configuring VPN using the applet (GUI), see “Configuring VPN tunnels” on page 220.

BR7131>admin(network.wan.vpn)> list

Description

Lists VPN tunnel entries.

Syntax

list	<cr>	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
-------------------------------------------------------------------------------
Tunnel Name   Type    Remote IP/Mask     Remote Gateway  Local WAN IP
-------------------------------------------------------------------------------
Eng2EngAnnex  Manual  192.168.32.2/24    192.168.33.1    192.168.24.198
SJSharkey     Manual  206.107.22.45/27   206.107.22.2    209.235.12.55

admin(network.wan.vpn)>list SJSharkey
-------------------------------------------------------------------------------
Detail listing of VPN entry:
-------------------------------------------------------------------------------
Name                       : SJSharkey
Local Subnet               : 1
Tunnel Type                : Manual
Remote IP                  : 206.107.22.45
Remote IP Mask             : 255.255.255.224
Remote Security Gateway    : 206.107.22.2
Local Security Gateway     : 209.239.160.55
AH Algorithm               : None
Encryption Type            : ESP
Encryption Algorithm       : DES
ESP Inbound SPI            : 0x00000100
ESP Outbound SPI           : 0x00000100
```

For information on displaying VPN information using the applet (GUI), see “Viewing VPN status” on page 233.

BR7131>admin(network.wan.vpn)> reset

Description

Resets all of the Brocade Mobility 7131 Series Access Point's VPN tunnels.

Syntax

reset	Resets all VPN tunnel states.

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 220.

BR7131>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
--------------------------------------------------------------------------------

Tunnel Name    Status      SPI(OUT/IN)        Life Time         Bytes(Tx/Rx)
--------------------------------------------------------------------------------

Eng2EngAnnex   Not Active
SJSharkey      Not Active
```

For information on displaying VPN information using the applet (GUI), see “Viewing VPN status” on page 233.

BR7131>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 230.

BR7131>admin(network.wan.content)>

Description

Displays the Outbound Content Filtering menu. The items available under this command include:

addcmd	Adds control commands to block outbound traffic.
delcmd	Deletes control commands to block outbound traffic.
list	Lists application control commands.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wan.content)> addcmd

Description

Adds control commands to block outbound traffic.

Syntax

addcmd	**web**		Adds WEB commands to block outbound traffic.
		proxy	Adds a Web proxy command.
		activex	Adds activex files.
		file	Adds Web URL extensions (10 files maximum)
	smtp		Adds SMTP commands to block outbound traffic.
		helo	helo command
		mail	mail command
		rcpt	rcpt command
		data	data command
		quit	quit command
		send	send command
		saml	saml command
		reset	reset command
		vrfy	vrfy command
		expn	expn command
	ftp		Adds FTP commands to block outbound traffic.
		put	store command
		get	retreive command
		ls	directory list command
		mkdir	create directory command
		cd	change directory command
		pasv	passive mode command

Example

```
admin(network.wan.content)>addcmd web proxy
admin(network.wan.content)>addcmd smtp data
admin(network.wan.content)>addcmd ftp put
```

BR7131>admin(network.wan.content)> delcmd

Description

Deletes control commands to block outbound traffic.

Syntax

delcmd	**web**		Deletes WEB commands to block outbound traffic.
		proxy	Deletes a Web proxy command.
		activex	Deletes activex files.
		file	Deletes Web URL extensions (10 files maximum)
	smtp		Deletes SMTP commands to block outbound traffic.
		helo	helo command
		mail	mail command
		rcpt	rcpt command
		data	data command
		quit	quit command
		send	send command
		saml	saml command
		reset	reset command
		vrfy	vrfy command
		expn	expn command
	ftp		Deletes FTP commands to block outbound traffic.
		put	store command
		get	retreive command
		ls	directory list command
		mkdir	create directory command
		cd	change directory command
		pasv	passive mode command

Example

```
admin(network.wan.content)>delcmd web proxy
admin(network.wan.content)>delcmd smtp data
admin(network.wan.content)>delcmd ftp put
```

BR7131>admin(network.wan.content)> list

Description

Lists application control commands.

Syntax

list	**web**	Lists WEB application control record.
	smtp	Lists SMTP application control record.
	ftp	Lists FTP application control record.

Example

```
admin(network.wan.content)>list web

HTTP Files/Commands
Web Proxy                    : deny
ActiveX                      : allow
filename                     :

admin(network.wan.content)>list smtp

SMTP Commands
HELO                    : deny
MAIL                    : allow
RCPT                    : allow
DATA                    : deny
QUIT                    : allow
SEND                    : allow
SAML                    : allow
RESET                   : allow
VRFY                    : allow
EXPN                    : allow

admin(network.wan.content)>list ftp

FTP Commands
Storing Files           : deny
Retreiving Files        : allow
Directory Files         : allow
Create Directory        : allow
Change Directory        : allow
Passive Operation       : allow
```

Network WAN, Dynamic DNS commands

BR7131>admin(network.wan.dyndns)>

Description

Displays the Dynamic DNS submenu. The items available under this command include:

set	Sets Dynamic DNS parameters.
update	Sets a manual Dynamic DNS update operation.
show	Shows the Dynamic DNS configuration.
..	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 Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 135.

BR7131>admin(network.wan.dyndns)> set

Description

Sets the access point's Dynamic DNS configuration.

Syntax

set	**mode**	**enable/disable**	Enables or disbales the Dynamic DNS service for the access point.
	username	<name>	Enter a 1 - 32 character username for the account used for the access point.
	password	<password>	Enter a 1 - 32 character password for the account used for the access point.
	hostname	<host>	Enter a 1 - 32 character hostname for the account used for the access point.

Example

```
admin(network.wan.dyndns)>set mode enable
admin(network.wan.dyndns)>set username percival
admin(network.wan.dyndns)>set password mudskipper
admin(network.wan.dyndns)>set host greengiant
```

For an overview of the Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 135.

BR7131>admin(network.wan.dyndns)> update

Description

Updates the access point's current WAN IP address with the DynDNS service.

Syntax

update	Updates the access point's current WAN IP address with the DynDNS service.

Example

```
admin(network.wan.dyndns)>update

IP Address                    : 157.235.91.231
Hostname                      : greengiant
```

For an overview of the Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 135.

BR7131>admin(network.wan.dyndns)> show

Description

Shows the current Dynamic DNS configuration.

Syntax

show	Shows the access point's current Dynamic DNS configuration.

Example

```
admin(network.wan.dyndns)>show

DynDNS Configuration

Mode                          : enable
Username                      : percival
Password                      : ********
Hostname                      : greengiant

DynDNS Update Response

IP Address                    : 157.235.91.231
Hostname                      : greengiant
Status                        : OK
```

For an overview of the Dynamic DNS options available using the applet (GUI), see "Configuring Dynamic DNS" on page 135.

Network wireless commands

BR7131>admin(network.wireless)

Description

Displays the Brocade Mobility 7131 Series Access Point wireless submenu. The items available under this command include:

set	Sets the Brocade Mobility 7131 Series Access Point's wireless (proxy arp) configuration.
show	Displays the access point's wireless (proxy arp) configuration.
wlan	Displays the WLAN submenu used to create and configure up to 16 WLANs per Brocade Mobility 7131 Series Access Point.
security	Displays the security submenu used to create encryption and authentication based security policies for use with Brocade Mobility 7131 Series Access Point WLANs.
acl	Displays to the *Access Control List* (ACL) submenu to restrict or allow Client access to Brocade Mobility 7131 Series Access Point WLANs.
radio	Displays the radio configuration submenu used to specify how the 802.11a/n 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.
rate-limiting	Displays the Rate Limiting submenu.
rogue-ap	Displays the Rogue-AP submenu to configure devices located by the Brocade Mobility 7131 Series Access Point as friendly or threatening for interoperablity.
wips	Goes to the *Wireless Intrusion Protection System* (WIPS) submenu.
Client-locationing	Displays the Client locationing submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless)>set

Description

Sets the access point's wireless (proxy arp) configuration.

Syntax

show	<mode>	**enable/disable**	Enables/disables proxy-arp support.

Example

```
admin(network.wireless)>set proxy-arp enable
```

For informarton on configuring proxy arp support using the applet (GUI), see "Enabling wireless LANs (WLANs)" on page 137.

BR7131>admin(network.wireless)>show

Description

Displays the access point's wireless (proxy arp) configuration.

Syntax

show	Displays the access point's wireless (proxy arp) configuration.

Example

```
admin(network.wireless)>show

Proxy ARP                          : dynamic
```

For informarton on configuring proxy arp support using the applet (GUI), see "Enabling wireless LANs (WLANs)" on page 137.

Network WLAN commands

BR7131>admin(network.wireless.wlan)>

Description

Displays the Brocade Mobility 7131 Series Access Point wireless LAN (WLAN) submenu. The items available under this command include:

show	Displays the Brocade Mobility 7131 Series Access Point'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.
hotspot	Displays the WLAN hotspot menu.
..	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 using the applet (GUI), see "Enabling wireless LANs (WLANs)" on page 137.

BR7131>admin(network.wireless.wlan)> show

Description

Displays the Brocade Mobility 7131 Series Access Point's current WLAN configuration.

Syntax

show	**summary**		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 summary

WLAN1
WLAN Name                          : Lobby
ESSID                              : 101
Radio Band(s)                      : 2,4 and 5.0 GHz
VLAN                               : <none>
Security Policy                    : Default
QoS Policy                         : Default

admin(network.wireless.wlan)>show wlan 1

ESS Identifier                     : 101
WLAN Name                          : Lobby
802.11n (5.0 GHz) Radio            : available
802.11n (2.4 GHz) Radio            : not available
Client Bridge Mesh Backhaul        : available
Hotspot                            : not available
Maximum clients                       : 127
Client Idle Timeout                   : 30
Security Policy                    : Default
Client Access Control                 : Default
Kerberos User Name                 :
Kerberos Password                  : ********
disallow Client to Client          : disable
Use Secure Beacon                  : disable
answer Broadcast ess               : enable
QoS Policy                         : Default
```

For information on displaying WLAN infromation using the applet (GUI), see "Enabling wireless LANs (WLANs)" on page 137.

BR7131>admin(network.wireless.wlan)> create

Description

Defines the parameters of a new WLAN.

Syntax

create				
	show	**wlan**	<number>	Displays newly created WLAN and policy number.
	set	**ess**	<essid>	Defines the ESSID for a target WLAN.
		wlan-name	<name>	Determines the name of this particlular WLAN (1-32).
		5.0GHz	<mode>	Enables or disables access to the Brocade Mobility 7131 Series Access Point 5.0 GHz radio.
		2.4Ghz	<mode>	Enables or disables access to the Brocade Mobility 7131 Series Access Point 2.4 GHz radio.
		mesh	<mode>	Enables or disables the Client Bridge Mesh Backhaul option.
		hotspot	<mode>	Enables or disables the Hotspot mode.
		max-Client	<number>	Defines the maximum number of Client able to operate within the WLAN (default = 127 clients).
		Client idle timeout	<minutes>	Sets the interval the access point uses to timeout idle clients from WLAN inclusion. Set between 1 -65532 minutes. Default is 30 minutes.
		security	<name>	Sets the security policy to the WLAN (1-32).
		acl	<name>	Sets the Client 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-Client-Client	<mode>	Enables or disables clients associated to the same WLAN to not communicate with each other.
		sbeacon	<mode>	Enables or disables the AP from transmitting the ESSID in the beacon.
		bcast	<mode>	Enables or disables the Brocade Mobility 7131 Series Access Point from accepting broadcast IDs from clients. Broadcast IDs are transmitted without security.
		qos	<name>	The index name representing the QoS policy used with this WLAN.
	add-wlan			Apply the changes to the modified WLAN and exit.

Example

```
admin(network.wireless.wlan.create)>show wlan

ESS Identifier                    :
WLAN Name                         :
802.11n (5.0 GHz) Radio           : available
```

```
802.11n (2.4 GHz) Radio           : not available
Client Bridge Mesh Backhaul       : not available
Hotspot                           : not available
Maximum clients                       : 127
Client Idle Timeout                   : 30
Security Policy                   : Default
Client Access Control                 :
Kerberos User Name                : Default
Kerberos Password                 : ********
disallow Client to Client                 : disable
Use Secure Beacon                 : disable
answer Broadcast ess              : disable
QoS Policy                        : Default

admin(network.wireless.wlan.create)>show security
-------------------------------------------------------------------------
Secu Policy Name      Authen      Encryption      Associated WLANs
-------------------------------------------------------------------------
1 Default             Manual      no encrypt      Front Lobby
2 WEP Demo            Manual      WEP 64          2nd Floor
3 Open                Manual      no encrypt      1st Floor

WPA Countermeasure    enable

admin(network.wireless.wlan.create)>show acl
-------------------------------------------------------------------------
ACL Policy Name           Associated WLANs
-------------------------------------------------------------------------
1 Default                 Front Lobby
2 Admin                   3rd Floor
3 Demo Room               5th Floor

admin(network.wireless.wlan.create)>show qos
-------------------------------------------------------------------------
QOS Policy Name           Associated WLANs
-------------------------------------------------------------------------
1 Default                 Front Lobby
2 Voice                   Audio Dept
3 Video                   Video Dept
```

The CLI treats the following as invalid characters, thus they should not be used in the creation of an ESSID (or other):

' " \ & $ ^ * + ? [({ | , < >

For information on creating a WLAN using the applet (GUI), see “Creating/editing individual WLANs” on page 139.

BR7131>admin(network.wireless.wlan)> edit

Description

Edits the properties of an existing WLAN policy.

Syntax

edit	<index>	Edits the properties of an existing (and specified) WLAN policy (1 -16).
	show	Displays the WLANs pamaters and summary.
	set	Edits the same WLAN parameters that can be modified using the create command.
	change	Completes the WLAN edits and exits the CLI session.
	..	Cancel the WLAN edits and exit the CLI session.

For information on editing a WLAN using the applet (GUI), see "Creating/editing individual WLANs" on page 139.

BR7131>admin(network.wireless.wlan)> delete

Description

Deletes an existing WLAN.

Syntax

delete	<wlan-name>	Deletes a target WLAN using the name supplied.
	all	Deletes all WLANs defined (except default WLAN).

For information on deleting a WLAN using the applet (GUI), see "Creating/editing individual WLANs" on page 139.

BR7131>admin(network.wireless.wlan.hotspot)>

Description

Displays the Hotspot submenu. The items available under this command include:

show	Show hotspot parameters.
redirection	Goes to the hotspot redirection menu.
radius	Goes to the hotspot Radius menu.
white-list	Goes to the hotspot white-list menu.
set	Sets the WLAN's hotspot configuration.
hs_import	Imports hotspot configuraiton files from a dedicated server.
hs_export	Exports hotspot configuraiton files to a dedicated server.
default	Stores default hotspot configuration files for a specified WLAN.
delete	Deletes hotspot files supporting a specified WLAN.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring the Hotspot options available to the using the applet (GUI), see "Configuring WLAN hotspot support" on page 152.

BR7131>admin(network.wireless.wlan.hotspot)> show

Description

Displays the current Brocade Mobility 7131 Series Access Point Rogue AP detection configuration.

Syntax

show	**hotspot**	<idx>	Shows hotspot parameters per wlan index (1-16).

Example

```
admin(network.wireless.wlan.hotspot)>show hotspot 1

WLAN1
Hotspot Mode                        : enable
Hotspot Page Location               : default
External Login URL                  : www.sjsharkey.com
External Welcome URL                :
External Fail URL                   :

Primary Server Ip adr               :157.235.21.21
Primary Server Port                 :1812
Primary Server Secret               :******
Secondary Server Ip adr             :157.235.32.12
Secondary Server Port               :1812
Secondary Server Secret             :******
Accounting Mode                     :disable
Accounting Server Ip adr            :0.0.0.0
Accounting Server Port              :1813
Accounting Server Secret            :********
Accoutning Timeout                  :10
Accoutning Retry-count              :3
Session Timeout Mode                :enable
Session Timeout                     :15

Whitelist Rules
-------------------------------------------------------------------------------
            Idx             IP Address
-------------------------------------------------------------------------------
            1               157.235.121.12
HOTSPOT CONFIGURATION PARAMETERS
customized filename                 : login.html
cfg filepath                        :
server ip address                   : 157.235.21.21
user name                           : mudskipper
password                            : **********
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

BR7131>admin(network.wireless.wlan.hotspot)> redirection

Description

Goes to the hotspot redirection menu.

Syntax

redirection	**set**	<page-loc>	Sets the hotspot http-re-direction by index (1-16) for the specified URL.
		<exturl>	Shows hotspot http-redirection details for specifiec index (1-16) for specified page (login, welcome, fail) and target URL..
	show		Shows hotspot http-redirection details.
	save		Saves the updated hotspot configuration to flash memory.
	quit		Quits the CLI session.
	..		Goes to the parent menu.
	/		Goes to the root menu.

Example

```
admin(network.wireless.wlan.hotspot.redirection)>set page-loc 1
www.sjsharkey.com
admin(network.wireless.wlan.hotspot.redirection)>set exturl 1 fail
www.sjsharkey.com
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

BR7131>admin(network.wireless.wlan.hotspot)> radius

Description

Goes to the hotspot Radius menu.

Syntax

set	Sets the Radius hotspot configuration.
show	Shows Radius hotspot server details.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

BR7131>admin(network.wireless.wlan.hotspot.radius)> set

Description

Sets the Radius hotspot configuration.

Syntax

set	**server**	<idx>	<srvr_type>	<ipadr>	Sets the Radius hotpost server IP address per wlan index (1-16)
	port	<idx>	<srvr_type>	<port>	Sets the Radius hotpost server port per wlan index (1-16)
	secret	<idx>	<srvr_type>	<secret>	Sets the Radius hotspot server shared secret password.
	acct-mode	<idx>	<mode>		Sets the Radius hotspot server accounting mode (enable/disable)
	acct-server	<idx>	<ipadr>		Sets the Radius hotspot accounting server IP address per wlan index (1-16).
	acct-port	<idx>	<port>		Sets the Radius hotspot accounting server port per wlan index (1-16).
	acct-secret	<idx>	<secret>		Sets the Radius hotspot server shared secret password per wlan index (1-16).
	acct-timeout	<idx>	<timeout>		Sets the Radius hotspot server accounting timeout period in seconds (1-25).
	acct-retry	<idx>	<retry_count>		Sets the Radius hotspot server accounting accounting retry interval (1-10).
	sess-mode	<idx>	<mode>		Enables or disbales the use of a hotspot timeout interval for the specified wlan index (1-16).
	sess-timeout	<idx>	<timeout>		Sets the Radius hotspot server timeout interval for the specified index (1-16) between 15 - 180 minutes.

Example

```
admin(network.wireless.wlan.hotspot.radius)>set server 1 primary 157.235.121.1
admin(network.wireless.wlan.hotspot.radius)>set port 1 primary 1812
admin(network.wireless.wlan.hotspot.radius)>set secret 1 primary sjsharkey
admin(network.wireless.wlan.hotspot.radius)>set acct-mode 1 enable
admin(network.wireless.wlan.hotspot.radius)>set acct-server 1 157.235.14.14
admin(network.wireless.wlan.hotspot.radius)>set acct-port 1 1812
admin(network.wireless.wlan.hotspot.radius)>set acct-secret 1 londonfog
admin(network.wireless.wlan.hotspot.radius)>set acct-timeout 1 25
admin(network.wireless.wlan.hotspot.radius)>set acct-retry 1 10
admin(network.wireless.wlan.hotspot.radius)>set sess-mode 1 enable
admin(network.wireless.wlan.hotspot.radius)>set sess-timeout 1 15
```

For information on configuring the Hotspot options available to the access ointusing the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

BR7131>admin(network.wireless.wlan.hotspot.radius)> show

Description

Shows Radius hotspot server details.

Syntax

show	**radius**	<idx>	Displays Radius hotspot server details per index (1-16)

Example

```
admin(network.wireless.wlan.hotspot.radius)>show radius 1
WLAN 1
Hotspot Mode                      : enable
Primary Server Ip adr             : 157.235.12.12
Primary Server Port               : 1812
Primary Server Secret             : ******
Secondary Server Ip adr           : 0.0.0.0
Secondary Server Port             : 1812
Secondary Server Secret           : ******
Accounting Mode                   : enable
Accounting Server Ip adr          : 157.235.15.16
Accounting Server Port            : 1813
Accounting Server Secret          : ******
Accounting Timeout                : 10
Accounting Retry-count            : 3
Session Timeout Mode              : enable

admin(network.wireless.wlan.hotspot.radius)>
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN hotspot support" on page 152.

BR7131>admin(network.wireless.wlan.hotspot)> white-list

Description

Goes to the hotspot white-list menu.

Syntax

white-list	**add**	<rule>	Adds hotspot whitelist rules by index (1-16) for specified IP address.
	clear		Clears hotspot whitelist rules for specified index (1-16).
	show		Shows hotspot whitelist rules for specified index (1-16).
	save		Saves the updated hotspot configuration to flash memory.
	quit		Quits the CLI session.
	..		Goes to the parent menu.
	/		Goes to the root menu.

Example

```
admin(network.wireless.wlan.hotspot.whitelist)>add rule 1 157.235.21.21
admin(network.wireless.wlan.hotspot.whitelist)>show white-rule 1

WLAN 1
Hotspot Mode                          disable
WhiteList Rules
------------------------------------------------------------------------------
---
Idx                                    IP Address
------------------------------------------------------------------------------
---
1                                    157.235.21.21
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

BR7131>admin(network.wireless.wlan.hotspot)>set

Description

Goes to the hotspot white-list menu.

Syntax

set	**file**	<wlan-idx> <file1> <file2>	Sets the hotspot customized file name(s) for the specified WLAN index <wlan-idx>. There's a maximum of 10 files and file names should be separated by a space.
	path	<path>	Sets the 0 to 39 character path name used to route imported and exported hotspot files.
	server	<ipadr>	Sets the IP address of the server used to import and export hotspot files with the access point.
	user	<name>	Defines the user accessing the server supporting the access point's hotspot.
	passwd	<passwd>	Establishes a password for the user.
	..		Goes to the parent menu.
	/		Goes to the root menu.

Example

```
admin(network.wireless.wlan.hotspot)>set file 2 login.html
admin(network.wireless.wlan.hotspot)>set path \\ftp:shareddrive/
admin(network.wireless.wlan.hotspot)>set server 157.235.112.1
admin(network.wireless.wlan.hotspot)>set user george
admin(network.wireless.wlan.hotspot)>set passwd just4you
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN hotspot support" on page 152.

BR7131>admin(network.wireless.wlan.hotspot)>hs_import

Description

Imports hotspot configuration parameters for a specified WLAN index <wlan-idx>.

Syntax

hs_import	<wlan-idx>	Imports hotspot configuration parameters for a specified WLAN index <wlan-idx> (1 - 16).

Example

```
admin(network.wireless.wlan.hotspot)>hs_import 2

Import Operation                  : [Started]
File Transfer                     : [In Progress]

File Transfer                     : [Completed]
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN hotspot support" on page 152.

BR7131>admin(network.wireless.wlan.hotspot)>hs_export

Description

Exports hotspot configuration parameters for a specified WLAN index <wlan-idx>.

Syntax

hs_export	<wlan-idx>	Exports hotspot configuration parameters for a specified WLAN index <wlan-idx> (1-16).

Example

```
admin(network.wireless.wlan.hotspot)>hs_export 2

Export Operation                  : [Started]
File Transfer                     : [In Progress]

File Transfer                     : [Completed]
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see "Configuring WLAN hotspot support" on page 152.

BR7131>admin(network.wireless.wlan.hotspot)>default

Description

Restores default hotspot files to a specified WLAN index <wlan-idx>.

Syntax

default	<wlan-idx>	Restores default hotspot files to a specified WLAN index <wlan-idx>.

Example

```
admin(network.wireless.wlan.hotspot)>default 2
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

BR7131>admin(network.wireless.wlan.hotspot)>delete

Description

Deletes hotspot files from a specified WLAN index <wlan-idx>.

Syntax

delete	<wlan-idx>	Deletes hotspot files from a specified WLAN index <wlan-idx>.

Example

```
admin(network.wireless.wlan.hotspot)>delete 2
Warning: This will delete all the files from the corresponding directory.
```

For information on configuring the Hotspot options available to the access point using the applet (GUI), see “Configuring WLAN hotspot support” on page 152.

Network security commands

BR7131>admin(network.wireless.security)>

Description

Displays the Brocade Mobility 7131 Series Access Point wireless security submenu. The items available under this command include:

show	Displays the Brocade Mobility 7131 Series Access Point's current security configuration.
set	Enables/disables the WPA countermeasure.
create	Creates 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 on the security configuration options available to the access point using the applet (GUI), see "Configuring security options" on page 192.

BR7131>admin(network.wireless.security)>show

Description

Displays the Brocade Mobility 7131 Series Access Point's current security configuration.

Syntax

show	**summary**		Displays list of existing security policies (1-16).
	policy	<id>	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

WPA Countermeasure    enable

admin(network.wireless.security)>show policy 1

Policy Name                       : Default
Authentication type               : 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 194.

BR7131>admin(network.wireless.security)>set

Description

Enables/disables the WPA countermeasure.

Syntax

set	<mode>	Enables/disables WPA countermeasures.

Example

```
admin(network.wireless.security)set wpa-countermeasure enable
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

WPA Countermeasure    enable
```

Related Commands

create	Creates 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 194.

BR7131>admin(network.wireless.security)>create

Description

Defines the parameter of Brocade Mobility 7131 Series Access Point 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). *The default password is "admin123".*
	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.
		server	<ip>	Set external Radius server IP address.
		port	<port>	Set external Radius server port number.
		secret	<secret>	Set external Radius server shared secret password.
		timeout	<period>	Defines Client timout period in seconds (1-255).
		retry	<number>	Sets the maximum number of Client retries to <retry> (**1**-**10**).
		syslog	<mode>	Enable or disable syslog messages.
		ip	<ip>	Defines syslog server IP address.
	adv	**Client-quiet**	<time>	Set the EAP Client/supplicant quiet period to <time> seconds (**1**-**65535**).
		Client-timeout	<timeout>	Sets the EAP Client/supplicant timeout in seconds (**1**-**255**).
		Client-tx	<time>	Sets the EAP Client/supplicant TX period <time> in seconds (**1**-**65535**).
		Client-retry	<count>	Sets the EAP maximum number of Client 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**	<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>.
		mixed-mode	<mode>		Enables or disables interoperation with WEP128 clients.
					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**).
		allow-wpa2-tkip	<mode>		Enables or disables the interoperation with wpa2-tkip clients.
		preauth	<mode>		Enables or disables preauthentication (fast roaming).
		opp-pmk-caching			Enables or disables opportunistic PMK.
		ptk-timeout	<time>		Sets the PTK timeout in milliseconds (1-100).

		ptk-retry	<count>	Sets the PTK retry count (1-10).
		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.
		phrase	<ascii phrase>	Sets the CCMP ASCII pass phrase to <ascii phrase> (8-63 characters).
		key	<256 bit key>	Sets the CCMP key to <256 bit key>.
		mixed-mode -with-tkip	<mode>	Enables or disables mixed mode (allowing WPA-TKIP clients).
		mixed-mode -with-wep	<mode>	Enables or disables mixed mode (allowing WPA-WEP clients).
		preauth	<mode>	Enables or disables preauthentication (fast roaming).
		opp-pmk-ca ching		Enables or disables opportunistic PMK.
		ptk-timeout	<time>	Sets the PTK timeout in milliseconds (1-100).
		ptk-retry	<count>	Sets the PTK retry count (1-10).
	add-policy			Adds the policy and exits.
	..			Disregards the policy creation and exits the CLI session.

For information on configuring the encryption and authentication options available to the access point using the applet (GUI), see "Configuring security options" on page 192.

BR7131>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. The values subject to modification, are the same ones created using the *BR7131>admin(network.wireless.security)>create* command.
change		Completes policy changes and exits the session.
..		Cancels the changes made and exits the session.

Example

```
admin(network.wireless.security)>edit 1
admin(network.wireless.security.edit)>show

Policy Name                          : Default
Authentication type                  : Manual Pre-shared key/No Authentication

Encryption type                      : no encryption
```

For information on configuring the encryption and authentication options available to the access point using the applet (GUI), see "Configuring security options" on page 192.

BR7131>admin(network.wireless.security)> delete

Description

Deletes a specific security policy.

Syntax

delete	<sec-name>	Removes the specified security policy from the list of supported policies.
	<all>	Removes all security policies except the default policy.

For information on configuring the encryption and authentication options available to the access point using the applet (GUI), see “Configuring security options” on page 192.

Network ACL commands

BR7131>admin(network.wireless.acl)>

Description

Displays the Brocade Mobility 7131 Series Access Point Client *Access Control List* (ACL) submenu. The items available under this command include:

show	Displays the Brocade Mobility 7131 Series Access Point's current ACL configuration.
create	Creates an Client ACL policy.
edit	Edits the properties of an existing Client ACL policy.
delete	Removes an Client ACL policy.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.acl)> show

Description

Displays the Brocade Mobility 7131 Series Access Point's current ACL configuration.

Syntax

show	**summary**		Displays the list of existing Client ACL policies.
	policy	<index>	Displays the requested Client ACL index policy.

Example

```
admin(network.wireless.acl)>show summary
-------------------------------------------------------------------
ACL Policy Name            Associated WLANs
-------------------------------------------------------------------
1 Default                  Front Lobby, WLAN1
2 Admin                    Administration
3 Demo Room                Customers

admin(network.wireless.acl)>show policy 1

Policy Name                       : Default
Policy Mode                       : allow

-------------------------------------------------------------------------
index                  start mac                 end mac
-------------------------------------------------------------------------
1                      00A0F8348787              00A0F8348798
```

For information on configuring the ACL options available to the access point using the applet (GUI), see "Configuring a WLAN Access Control List (ACL)" on page 144.

BR7131>admin(network.wireless.acl)> create

Description

Creates an Client ACL policy.

Syntax

create	**show**		<acl-name>	Displays the parameters of a new ACL policy.
	set	**acl-name**	<index>	Sets the Client ACL policy name.
		mode	<acl-mode>	Sets the ACL mode for the defined index (1-16). Allowed clients can access the Brocade Mobility 7131 Series Access Point 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

-------------------------------------------------------------------------------
index                  start mac                  end mac
-------------------------------------------------------------------------------
1                      00A0F8334455               00A0F8334455
2                      00A0F8400000               00A0F8402001


admin(network.wireless.acl.create)>set acl-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 access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 144.

BR7131>admin(network.wireless.acl.edit)>

Description

Edits the properties of an existing Client ACL policy.

Syntax

show	Displays Client ACL policy and its parameters.
set	Modifies the properties of an existing Client ACL policy.
add-addr	Adds an Client ACL table entry.
delete	Deletes an Client 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 access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 144.

BR7131>admin(network.wireless.acl)> delete

Description

Removes an Client ACL policy.

Syntax

delete	<name>	Deletes a partilcular Client ACL policy.
	all	Deletes all Client ACL policies.

For information on configuring the ACL options available to the access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 144.

Network radio configuration commands

BR7131>admin(network.wireless.radio)>

Description

Displays the Brocade Mobility 7131 Series Access Point Radio submenu. The items available under this command include:

show	Summarizes Brocade Mobility 7131 Series Access Point radio parameters at a high-level.
set	Defines the access point radio configuration.
radio1	Displays the 2.4 GHz radio submenu.
radio2	Displays the 5.0 GHz radio submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.radio)> show

Description

Displays the Brocade Mobility 7131 Series Access Point's current radio configuration.

Syntax

show	Displays the Brocade Mobility 7131 Series Access Point's current radio configuration.

Example

```
admin(network.wireless.radio)>show

Radio Configuration

Radio 1
Name                                : Radio 1
Radio Mode                          : enable
RF Band of Operation                : 802.11n(2.4 GHz)

Wireless AP Configuration:
  Base Bridge Mode                  : enable
  Max Wireless AP Clients           : 6
  Client Bridge Mode                : disable
  Clitn Bridge WLAN                 : WLAN1
  Mesh Connection Timeout           : enable

Radio 2
Name                                : Radio 2
Radio Mode                          : enable
Radio Function                      : WLAN
RF Band of Operation                : 802.11n(5 GHz)

Wireless Mesh Configuration:
  Base Bridge Mode                  : enable
  Max Wireless Mesh Clients         : 5
  Client Bridge Mode                : disable
  Roaming Client Bridge Mode        : enable
  Client Bridge WLAN                : WLAN1
  Mesh Connection Timeout           : WLAN1

Dot11 Auth Algorithm                : open-system-only

Radio 3
Name                                : Radio 3
Radio Mode                          : enable
Radio Function                      : WIPS

Dot11 Auth Algorithm                : open-system-only

DSCP QoS Mappings                   :
DSCP Values                         :
```

For information on configuring the Radio Configuration options available to the access point using the applet (GUI), see "Setting the WLAN's radio configuration" on page 161.

BR7131>admin(network.wireless.radio)> set

Description

Enables a Brocade Mobility 7131 Series Access Point Radio and defines the RF band of operation.

Syntax

set	**11a**	<mode>	Enables or disables the Brocade Mobility 7131 Series Access Point's 5.0 GHz radio.
	11bg	<mode>	Enables or disables the Brocade Mobility 7131 Series Access Point's 2.4 GHz radio.
	mesh-base	<mode>	Enables or disables base bridge mode.
	mesh-max		Sets the maximum number of wireless bridge clients.
	mesh-client	<mode>	Enables or Disables client bridge mode.
	mesh-roaming-client	<mode>	Enables or disables the mesh roaming client mode.
	mesh-timeout	<mode>	Sets the client bridge link timeout.
	mesh-wlan	<name>	Defines the client bridge WLAN name.
	dot11-auth	<auth-algorithm>	Defines dot11 level authentication algorithm to either *open-system-only* of *shared-key-allowed*.

Example

```
admin(network.wireless.radio)>set 11a enable
admin(network.wireless.radio)>set 11bg enable
admin(network.wireless.radio)>set mesh-base 1 enable
admin(network.wireless.radio)>set mesh-max 1 11
admin(network.wireless.radio)>set mesh-client 1 disable
admin(network.wireless.radio)>set mesh-roaming-client 1 enable
admin(network.wireless.radio)>set mesh-wlan wlan1
admin(network.wireless.radio)>set dot11-auth shared-key-allowed
```

Three Radio SKU

set	**radio-config**	<value 1-8>	
		1	Radio 1 WLAN, Radio 2 WLAN, Radio 3 WIPS
		2	Radio 1 WLAN, Radio 2 WIPS, Radio 3 WIPS
		3	Radio 1 WIPS, Radio 2 WLAN, Radio 3 WIPS
		4	Radio 1 WLAN, Radio 2 WLAN, Radio 3 Disabled
		5	Radio 1 WIPS, Radio 2 WIPS, Radio 3 Disabled
		6	Radio 1 WLAN, Radio 2 Disabled, Radio 3 Disabled
		7	Radio 1 Disabled, Radio 2 WLAN, Radio 3 Disabled
		8	Radio 1 Disabled, Radio 2 Disabled, Radio 3 Disabled

Two Radio SKU

set	**radio-config**	<value 1-7>		
			1	Radio 1 WLAN, Radio 2 WIPS
			2	Radio 1 WIPS, Radio 2 WLAN
			3	Radio 1 WLAN, Radio 2 WLAN
			4	Radio 1 WIPS, Radio 2 WIPS
			5	Radio 1 WLAN, Radio 2 Disabled
			6	Radio 1 Disabled, Radio 2 WLAN
			7	Radio 1 Disabled, Radio 2 Disabled

Single Radio SKU

set	**radio-config**	<value 1-4>		
			1	Radio 1 WIPS
			2	Radio 1 WLAN (B/G/N)
			3	Radio 1 WLAN (A/N)
			4	Radio 1 Disabled

For information on the options available to the access point, see “Setting the WLAN’s radio configuration” on page 161.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz])>

Description

Displays a specific 802.11n 2.4 GHz radio 1 submenu. The items available under this command include:

Syntax

show	Displays 802.11n (2.4 GHz) radio settings.
set	Defines specific 802.11n (2.4 GHz) radio parameters.
advanced	Displays the Adavanced radio settings submenu.
mesh	Goes to the Wireless AP Connections 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 access point using the applet (GUI), see “Setting the WLAN’s radio configuration” on page 161.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz])>show

Description

Displays specific 802.11n (2.4 GHz) radio settings.

Syntax

show	**radio**	Displays specific 802.11n (2.4 GHz) radio settings.
	rates	Displays specific 802.11n (2.4 GHz) radio rate settings.
	aggr	Displays specific 802.11n (2.4 GHz) aggregation settings.
	qos	Displays specific 802.11n (2.4 GHz) radio WMM QoS settings.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz])>show radio

Radio Setting Information

Placement                          : indoor
MAC Address                        : 00A0F8715920
Radio Type                         : 802.11n (2.4 GHz)
ERP Protection                     : Off
HT Protection Mode                 : Pure HT

Channel Setting                    : user selection
Power Level                        : 5 dbm (4 mW)

802.11 rate compatibility mode     : B, G, and N

Beacon Interval                    : 100 K-usec
DTIM Interval                      : 10 beacon intvls

short preamble                     : disable
RTS Threshold                      : 2341 bytes

QBSS Channel Util Beacon Intervl   : 10 beacon intvls
QBSS Load Element Mode             : enable
admin(network.wireless.radio.802-11n[2.4 GHz])>show rates

Single Anetenna                    : disable
Dynamic Chain Selection            : disable
TKIP HT rates compatibility        : disable
Current BCMC-Tx-Speed for          : range optimization

Basic Rates              1 2 5.5 11
Supported Rates          1 2 5.5 6 9 11 12 18 24 36 48 54
Short Guard Interval     disable
-------------------------------------------------------------------------------
MCS Index      Basic/Supported     20 MHz Rate     40 MHz Rate
-------------------------------------------------------------------------------
0              Supported            6.5 Mbps       13.5 Mbps
1              Supported           13.0 Mbps       27.0 Mbps
2              Supported           19.5 Mbps       40.5 Mbps
3              Supported           26.0 Mbps       54.0 Mbps
4              Supported           39.0 Mbps       81.0 Mbps
5              Supported           52.0 Mbps       108.0 Mbps
```

```
6               Supported           58.5 Mbps       121.5 Mbps
7               Supported           65.0 Mbps       135.0 Mbps
8               Supported           13.0 Mbps       27.0 Mbps
9               Supported           26.0 Mbps       54.0 Mbps
10              Supported           39.0 Mbps       81.0 Mbps
11              Supported           52.0 Mbps       108.0 Mbps
12              Supported           78.0 Mbps       162.0 Mbps
13              Supported          104.0 Mbps       216.0 Mbps
14              Supported          117.0 Mbps       243.0 Mbps
15              Supported          130.0 Mbps       270.0 Mbps

admin(network.wireless.radio.802-11n[2.4 GHz])>

admin(network.wireless.radio.802-11n[2.4 GHz])>show aggr

Radio Aggregation Settings
Receive A-MSDU Buffer Limit             :3839 bytes

Enable Transmit A-MPDU                  :enable
Transmit A-MPDU Size Limit              :65536 bytes
Receive A-MPDU Size Limit               :65536 bytes
Receive A-MPDU Minimum Spacing          :0 usec

admin(network.wireless.radio.802-11n[2.4 GHz])>

admin(network.wireless.radio.802-11n[2.4 GHz])>show qos

Radio QOS Parameter Set              11n-default
--------------------------------------------------------------------------------
Access Category      CWMin      CWMax      AIFSN      TXOPs (32 usec) TXOPs ms
--------------------------------------------------------------------------------
Background           15         1023       7          0               0.000
Best Effort          15         63         3          31              0.992
Video                7          15         1          94              3.008
Voice                3          7          1          47              1.504
```

CAUTION

If you do NOT include the index number (for example, "set dtim 50"), the DTIMs for all four BSSIDs will be changed to 50. To change individual DTIMs for BSSIDs, specify the BSS Index number (for example, "set dtim 2 50). This will change the DTIM for BSSID 2 to 50.

For information on configuring the Radio 1 Configuration options available to the access point using the applet (GUI), see "Configuring a WLAN Access Control List (ACL)" on page 144.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz])> set

Description

Defines specific 802.11n (2.4 GHz) radio parameters.

Syntax

set	**placement**	Defines the Brocade Mobility 7131 Series Access Point radio placement as indoors or outdoors.
	ch-mode	Determines how the radio channel is selected (user, auto-20 or auto-40).
	channel	Defines the radio channel used. Channel allowed depends on actual country of operation.
	power	Defines the antenna power transmit level. Depends on radio type, channel and country.
	antenna-type	Sets the numerical antenna type used with the access point (0-7). Antenna types include: 0-Default antenna, 1-Dual band antenna, 2-Omni antenna, 3-Yagi antenna, 4-Embedded antenna, 5-Panel antenna, 6-Patch antenna, 7-Sector antenna.
	antenna-gain	Sets the gain used by the selected antenna type (between 0.00 - 30.00 dBm)
	rf-mode	Sets the default rates for the 802.11 mode selected (b-only, g-only, n-only, b-and-g, or bg-and-n).
	rates	Sets the supported radio transmit rates.
	beacon	Sets the beacon interval used by the radio.
	dtim	Defines the DTIM interval (by index) used by the radio.
	aggr	Sets the radio's aggregation.
	shortgi	Enables/disables a short guard interval of 40MHz.
	single-antenna	Enables/disables single antenna support. Enable (default setting) to decrease sensitivity and device retries.
	preamble	Enables/disables short preamble support for the radio (this is 2.4 GHz radio specific).
	rts	Defines the RTS Threshold value for the radio.
	range	Sets the radio's extended range (in miles 0-50).
	qos	Defines the cwmin, cwmax, aifsn and txops levels for the QoS policy used for the radio.
	qbss-beacon	Sets the QBSS Channel Util Beacon Interval in kilo-usec (10 - 200).
	qbss-mode	Enables/disables the QBSS load element.
	dynamic-chain-selection	Enables/disables dynamic chain selection for the radio. For more information, see "Dynamic chain selection" on page 5.
	tkip-ht-compatibility	Enables/disables TKIP-HT rates compatibility.
	bcmc-tx-speed	Sets the transmission speed to either range or throughout mode.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz])>set placement indoor
admin(network.wireless.radio.802-11n[2.4 GHz])>set ch-mode user
admin(network.wireless.radio.802-11n[2.4 GHz])>set channel 11
```

```
admin(network.wireless.radio.802-11n[2.4 GHz])>set power 4
admin(network.wireless.radio.802-11n[2.4 GHz])>set antenna-type 1
admin(network.wireless.radio.802-11n[2.4 GHz])>set antenna-gain 10.00
admin(network.wireless.radio.802-11n[2.4 GHz])>set rf-mode b-only
admin(network.wireless.radio.802-11n[2.4 GHz])>set rates
admin(network.wireless.radio.802-11n[2.4 GHz])>set beacon 100
admin(network.wireless.radio.802-11n[2.4 GHz])>set dtim 1 40
admin(network.wireless.radio.802-11n[2.4 GHz])>set aggr ampdu enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set shortgi disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set single-antenna disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set preamble disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set rts 2341
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos cwmin 125
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos cwmax 255
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos aifsn 7
admin(network.wireless.radio.802-11n[2.4 GHz])>set qos txops 0
admin(network.wireless.radio.802-11n[2.4 GHz])>set qbss-beacon 110
admin(network.wireless.radio.802-11n[2.4 GHz])>set qbss-mode enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set dynamic-chain-selection
enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set tkip-ht-compatibility
disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set bcmc-tx-speed range
```

For information on configuring the Radio 1 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n radio” on page 167.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>

Description

Displays the advanced submenu for the 802.11n (2.4 GHz) radio. The items available under this command include:

Syntax

show	Displays advanced radio settings for the 802.11n (2.4 GHz) radio.
set	Defines advanced parameters for the 802.11n (2.4 GHz) radio.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].advanced)> show

Description

Displays the BSSID to WLAN mapping for the 802.11n (2.4 GHz) radio.

Syntax

show	**advanced**	Displays advanced settings for the 802.11n (2.4 GHz) radio.
	wlan	Displays WLAN summary list for the 802.11n (2.4 GHz) radio.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>show advanced

--------------------------------------------------------------------------------
      WLAN      BSS ID      BC/MC Cipher      Status      Message
--------------------------------------------------------------------------------

      Lobby     1           Open              good        configuration is ok
      HR        2           Open              good        configuration is ok
      Office    3           Open              good        configuration is ok

--------------------------------------------------------------------------------
      BSSID      Primary WLAN
--------------------------------------------------------------------------------

      1          Lobby
      2          HR
      3          Office

admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>show wlan

WLAN 1:
WLAN name                       : WLAN1
ESS ID                          : 101
Radio Band(s)                   : 2.4 and 5.0 GHz
VLAN                            : <none>
Security Policy                 : Default
QoS Policy                      : Default
```

For information on configuring Radio 1 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n radio” on page 167.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].advanced)> set

Description

Defines advanced parameters for the target 802.11n (2.4 GHz) radio.

Syntax

set	**wlan**	<wlan-name>	<bssid>	Defines advanced WLAN to BSSID mapping for the target radio.
	bss	<bss-id>	<wlan name>	Sets the BSSID to primary WLAN definition.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>set wlan demoroom 1
admin(network.wireless.radio.802-11n[2.4 GHz].advanced)>set bss 1 demoroom
```

For information on configuring Radio 1 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n radio” on page 167.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>

Description

Displays the mesh configuration submenu for the 802.11n (2.4 GHz) radio. The items available under this command include:

Syntax

show	Displays mesh settings and status for the 802.11n (2.4 GHz) radio.
set	Defines mesh parameters for the 802.11n (2.4 GHz) radio.
add	Adds a 802.11n (2.4 GHz) radio mesh connection.
delete	Deletes a 802.11n (2.4 GHz) radio mesh connection.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)> show

Description

Displays mesh settings and status for the 802.11n (2.4 GHz) radio.

Syntax

show	**config**	Displays the connection list configuration.
	status	Shows the available mesh connection status.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show config

Mesh Connection Auto Select                  : enable

admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show status
--------------------------------------------------------------------------------
idx      AP MAC Address     Channel     Signal (dBm)
--------------------------------------------------------------------------------

admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>
```

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)> set

Description

Defines mesh parameters for the 802.11n (2.4 GHz) radio.

Syntax

set	<mode>	Defines mesh parameters for the 802.11n (2.4 GHz) radio..

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>set auto-select enable
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>show config

Mesh Connection Auto Select                  : enable
```

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)> add

Description

Adds a 802.11n (2.4 GHz) radio mesh connection.

Syntax

add	<priority>	Defines the connection priority (1-16).
	<mac>	Sets the access point MAC address.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>add 2 AA21DCDD12DE
```

BR7131>admin(network.wireless.radio.802-11n[2.4 GHz].mesh)> delete

Description

Deletes a 802.11n (2.4 GHz) radio mesh connection by specified index or by removing all entries.

Syntax

delete	<idx>	Deletes a mesh connection by specified index (1-16).
	<all>	Removes all mesh connections.

Example

```
admin(network.wireless.radio.802-11n[2.4 GHz].mesh)>delete 2
```

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz])>

Description

Displays a specific 802.11n (5.0 GHz) radio 2 submenu. The items available under this command include:

Syntax

show	Displays 802.11n (5.0 GHz) radio settings
set	Defines specific 802.11n (5.0 GHz) radio parameters.
advanced	Displays the Advanced radio settings submenu.
mesh	Goes to the Mesh Connections submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz])> show

Description

Displays specific 802.11n (5.0 GHz) radio settings.

Syntax

show	**radio**	Displays specific 802.11n (5.0 GHz) radio settings.
	rates	Displays specific 802.11n (5.0 GHz) radio rate settings.
	aggr	Displays specific 802.11n (5.0 GHz) aggregation settings.
	qos	Displays specific 802.11n (5.0 GHz) radio WMM QoS settings.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz])>show radio

Radio Setting Information

Placement                          : indoor
MAC Address                        : 00A0F8715920
Radio Type                         : 802.11n (5.0 GHz)
HT Protection Mode                 : Pure HT

Channel Setting                    : uniform spreading
Power Level                        : 20 dbm (100 mW)

802.11 rate compatibility mode     : A and N

Beacon Interval                    : 100 K-usec
DTIM Interval                      : 10 beacon intvls

RTS Threshold                      : 2341 bytes

QBSS Channel Util Beacon Intervl   : 10 beacon intvls
QBSS Load Element Mode             : enable

Single Antenna                     : disable
Dynamic Chain Selection            : disable
TKIP HT rates compatibility        : disable
Current BCMC-Tx-Speed for          : range optimization

admin(network.wireless.radio.802-11n[5.0 GHz])>show rates

Basic Rates              6 12 24
Supported Rates          6 9 12 18 24 36 48 54
Short Guard Interval     disable
-------------------------------------------------------------------------
MCS Index      Basic/Supported     20 MHz Rate     40 MHz Rate
-------------------------------------------------------------------------
0              Supported            6.5 Mbps       13.5 Mbps
1              Supported           13.0 Mbps       27.0 Mbps
2              Supported           19.5 Mbps       40.5 Mbps
3              Supported           26.0 Mbps       54.0 Mbps
4              Supported           39.0 Mbps       81.0 Mbps
5              Supported           52.0 Mbps       108.0 Mbps
6              Supported           58.5 Mbps       121.5 Mbps
```

```
7               Supported           65.0 Mbps       135.0 Mbps
8               Supported           13.0 Mbps       27.0 Mbps
9               Supported           26.0 Mbps       54.0 Mbps
10              Supported           39.0 Mbps       81.0 Mbps
11              Supported           52.0 Mbps       108.0 Mbps
12              Supported           78.0 Mbps       162.0 Mbps
13              Supported          104.0 Mbps       216.0 Mbps
14              Supported          117.0 Mbps       243.0 Mbps
15              Supported          130.0 Mbps       270.0 Mbps

admin(network.wireless.radio.802-11n[5.0 GHz])>

admin(network.wireless.radio.802-11n[5.0 GHz])>show aggr

Radio Aggregation Settings
Receive A-MSDU Buffer Limit             :3839 bytes
Transmit A-MSDU Buffer Limit            :3839 bytes

Enable Transmit A-MPDU                  :enable
Transmit A-MPDU Size Limit              :65536 bytes
Receive A-MPDU Size Limit               :65536 bytes
Receive A-MPDU Minimum Spacing          :0 usec

admin(network.wireless.radio.802-11n[5.0 GHz])>

admin(network.wireless.radio.802-11n[5.0 GHz])>show qos

Radio QOS Parameter Set              11n-default
--------------------------------------------------------------------------------
Access Category      CWMin      CWMax      AIFSN      TXOPs (32 usec) TXOPs ms
--------------------------------------------------------------------------------
Background           15         1023       7          0               0.000
Best Effort          15         63         3          31              0.992
Video                7          15         1          94              3.008
Voice                3          7          1          47              1.504
```

For information on configuring the Radio 2 Configuration options available to the access point using the applet (GUI), see “Configuring a WLAN Access Control List (ACL)” on page 144.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz])> set

Description

Defines specific 802.11n (5.0 GHz) radio parameters.

Syntax

set	**placement**	Defines the Brocade Mobility 7131 Series Access Point radio placement as indoors or outdoors.
	ch-mode	Determines how the radio channel is selected.
	channel	Defines the actual channel used by the radio. Channel allowed depends on actual country of operation.
	power	Defines the antenna power transmit level. Depends on radio type, channel and country.
	antenna-type	Sets the numerical antenna type used with the access point (0-7). Antenna types include: 0-default antenna, 1-dual band antenna, 2-Omni antenna, 3-Yagi antenna, 4-Embedded antenna, 5-Panel antenna, 6-Patch antenna, 7-Sector antenna.
	antenna-gain	Sets the gain used by the selected antenna type (between 0.00 - 30.00 dBm)
	rf-mode	Sets the default rates for the 802.11 mode selected (a-only, n-only, or a-and-n).
	rates	Sets the supported radio transmit rates.
	beacon	Sets the beacon interval used by the radio.
	dtim	Defines the DTIM interval (by index) used by the radio.
	aggr	Sets the radio's aggregation.
	shortgi	Enables/disables a short guard interval of 40MHz.
	single-antenna	Enables/disables single antenna support. Enable (default setting) to decrease sensitivity and device retries.
	rts	Defines the RTS Threshold value for the radio.
	range	Sets the radio's extended range (in miles 0-50).
	qos	Defines the param-set, cwmin, cwmax, aifsn and txops levels for the QoS policy used for the 5.0 GHz radio.
	qbss-beacon	Sets the QBSS Channel Util Beacon Interval in kilo-usec (10 - 200).
	qbss-mode	Enables/disables the QBSS load element.
	dynamic-chain-selection	Enables/disables dynamic chain selection for the radio. For more information, see "Dynamic chain selection" on page 5.
	tkip-ht-compatibility	Enables/disables TKIP-HT rates compatibility.
	bcmc-tx-speed	Sets the transmission speed to either range or throughout mode.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz])>

admin(network.wireless.radio.802-11n[5.0 GHz])>set placement indoor
admin(network.wireless.radio.802-11n[5.0 GHz])>set ch-mode auto-40
```

```
admin(network.wireless.radio.802-11n[5.0 GHz])>set channel 11
admin(network.wireless.radio.802-11n[5.0 GHz])>set antenna-type 2
admin(network.wireless.radio.802-11n[5.0 GHz])>set antenna-gain 10.00
admin(network.wireless.radio.802-11n[5.0 GHz])>set power 4
admin(network.wireless.radio.802-11n[5.0 GHz])>set rates 10
admin(network.wireless.radio.802-11n[5.0 GHz])>set beacon 100
admin(network.wireless.radio.802-11n[5.0 GHz])>set dtim 1 10
admin(network.wireless.radio.802-11n[2.4 GHz])>set aggr ampdu enable
admin(network.wireless.radio.802-11n[2.4 GHz])>set shortgi disable
admin(network.wireless.radio.802-11n[2.4 GHz])>set single-antenna disable
admin(network.wireless.radio.802-11n[5.0 GHz])>set rts 2341
admin(network.wireless.radio.802-11n[5.0 GHz])>set range 40
admin(network.wireless.radio.802-11n[5.0 GHz])>set qbss-beacon 110
admin(network.wireless.radio.802-11n[5.0 GHz])>set qbss-mode enable
admin(network.wireless.radio.802-11n[5.0 GHz])>set single-antenna disable
admin(network.wireless.radio.802-11n[5.0 GHz])>set dynamic-chain-selection
enable
admin(network.wireless.radio.802-11n[5.0 GHz])>set tkip-ht-compatibility
disable
admin(network.wireless.radio.802-11n[5.0 GHz])>set bcmc-tx-speed range
```

For information on configuring the Radio 2 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n radio” on page 167.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>

Description

Displays the advanced submenu for the 802.11n (5.0 GHz) radio. The items available under this command include:

Syntax

show	Displays advanced radio settings for the 802.11n (5.0 GHz) radio.
set	Defines advanced parameters for the 802.11n (5.0 GHz) radio.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].advanced)> show

Description

Displays the BSSID to WLAN mapping for the 802.11n (5.0 GHz) radio.

Syntax

show	**advanced**	Displays advanced settings for the 802.11n (5.0 GHz) radio.
	wlan	Displays WLAN summary list for 802.11n (5.0 GHz) radio.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>show advanced

--------------------------------------------------------------------------------
      WLAN      BSS ID      BC/MC Cipher      Status      Message
--------------------------------------------------------------------------------

      Lobby     1           Open              good        configuration is ok
      HR        2           Open              good        configuration is ok
      Office    3           Open              good        configuration is ok

--------------------------------------------------------------------------------
      BSSID      Primary WLAN
--------------------------------------------------------------------------------

      1          Lobby
      2          HR
      3          Office

admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>show wlan

WLAN 1:
WLAN name                       : WLAN1
ESS ID                          : 101
Radio                           : 2.4 and 5.0 GHz
VLAN                            : <none>
Security Policy                 : Default
QoS Policy                      : Default
```

For information on configuring the Radio 2 Configuration options available to the access point using the applet (GUI), see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].advanced)> set

Description

Defines advanced parameters for the target 802.11n (5.0 GHz) radio.

Syntax

set	**wlan**	<wlan-name>	<bssid>	Defines advanced WLAN to BSSID mapping for the target 5.0 GHz radio.
	bss	<bss-id>	<wlan name>	Sets the BSSID to primary WLAN definition.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>set wlan demoroom 1
admin(network.wireless.radio.802-11n[5.0 GHz].advanced)>set bss 1 demoroom
```

For information on configuring Radio 2 Configuration options available to the access point using the applet (GUI), see “Configuring the 802.11a/n or 802.11b/g/n radio” on page 167.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>

Description

Displays the mesh configuration submenu for the 802.11n (5.0 GHz) radio. The items available under this command include:

Syntax

show	Displays mesh settings and status for the 802.11n (5.0 GHz) radio.
set	Defines mesh parameters for the 802.11n (5.0 GHz) radio.
add	Adds a 802.11n (5.0 GHz) radio mesh connection.
delete	Deletes a 802.11n (5.0 GHz) radio mesh connection.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)> show

Description

Displays mesh settings and status for the 802.11n (5.0 GHz) radio.

Syntax

show	**config**	Displays the connection list configuration.
	status	Shows the available mesh connection status.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show config

Mesh Connection Auto Select                  : enable

admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show status
--------------------------------------------------------------------------------
idx      AP MAC Address     Channel     Signal (dBm)
--------------------------------------------------------------------------------

admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>
```

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)> set

Description

Defines mesh parameters for the 802.11n (5.0 GHz) radio.

Syntax

set	<mode>	Defines mesh parameters for the 802.11n (5.0 GHz) radio.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>set auto-select enable
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>show config

Mesh Connection Auto Select                  : enable
```

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)> add

Description

Adds a 802.11n (5.0 GHz) radio mesh connection.

Syntax

add	<priority>	Defines the connection priority (1-16).
	<mac>	Sets the access point MAC address.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>add 2 AA21DCDD12DE
```

BR7131>admin(network.wireless.radio.802-11n[5.0 GHz].mesh)> delete

Description

Deletes a 802.11n (5.0 GHz) radio mesh connection by specified index or by removing all entries.

Syntax

delete	<idx>	Deletes a mesh connection by specified index (1-16).
	<all>	Removes all mesh connections.

Example

```
admin(network.wireless.radio.802-11n[5.0 GHz].mesh)>delete 2
```

Network Quality of Service (QoS) commands

BR7131>admin(network.wireless.qos)>

Description

Displays the Brocade Mobility 7131 Series Access Point *Quality of Service* (QoS) submenu. The items available under this command include:

show	Displays Brocade Mobility 7131 Series Access Point 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.

BR7131>admin(network.wireless.qos)> show

Description

Displays the Brocade Mobility 7131 Series Access Point's current QoS policy by summary or individual policy.

Syntax

show	**summary**		Displays all exisiting QoS policies that have been defined.
	policy	<index>	Displays the configuration for the requested QoS policy.

Example

```
admin(network.wireless.qos)>show summary

------------------------------------------------------------------------
QOS Policy Name            Associated WLANs
------------------------------------------------------------------------
1 Default                  WLAN1, mudskipper
2 IP Phones                Audio Dept
3 Video                    Vidio Dept

admin(network.wireless.qos)>show policy 1

Policy Name                          Default
Support Legacy Voice Mode            disable
Multicast (Mask) Address 1           01005E000000
Multicast (Mask) Address 2           09000E000000
WMM QOS Mode                         disable
WMM QOS Parameter Set                11ag-default
```

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see "Setting the WLAN Quality of Service (QoS) policy" on page 147.

BR7131>admin(network.wireless.qos.create)>

Description

Defines a Brocade Mobility 7131 Series Access Point QoS policy.

Syntax

show				Displays QoS policy parameters.
set	**qos-name**	<index>		Sets the QoS name for the specified index entry.
	vop	<index>		Enables or disables support (by index) for legacy VOIP devices.
	mcast	<mac>		Defines primary and secondary Multicast MAC address.
	wmm-qos	<index>		Enables or disables the QoS policy index specified.
	param-set	<set-name>		Defines the data type used with the qos policy and mesh network. When set to a value other then manual, editing the access category values is not necessary. Options include; 11g-default, 11b-default, 11g-wifi, 11b-wifi, 11g-voice, 11b-voice or manual for advanced users).
	cwmin	<access category>	<index>	Defines Minimum Contention Window (CW-Min) for specified access categoiry and index.
	cwmax	<access category>	<index>	Defines Maximum Contention Window (CW-Max) for specified access categoiry and index.
	aifsn	<access category>	<index>	Sets Arbitrary Inter-Frame Space Number (AIFSN) for specified access categoiry and index.
	txops	<access category>	<index>	Configures Opportunity to Transmit Time (TXOPs Time) for specified access categoiry and index.
	default		<index>	Defines CWMIN, CWMAX, AIFSN and TXOPs default values.
add-policy				Completes the policy edit and exits the session.
..				Cancels the changes and exits.

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see “Setting the WLAN Quality of Service (QoS) policy” on page 147.

BR7131>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.
	vop	<index>		Enables or disables support (by index) for legacy VOIP devices.
	mcast	<mac>		Defines primary and secondary Multicast MAC address.
	wmm-qos	<index>		Enables or disables the QoS policy index specified.
	param-set	<set-name>		Defines the data type used with the qos policy and mesh network. When set to a value other then manual, editing the access category values is not necessary. Options include; 11g-default, 11b-default, 11g-wifi, 11b-wifi, 11g-voice, 11b-voice or manual for advanced users).
	cwmin	<access category>	<index>	Defines the Minimum Contention Window (CW-Min) for specified access categoiry and index.
	cwmax	<access category>	<index>	Defines the Maximum Contention Window (CW-Max) for specified access categoiry and index.
	aifsn	<access category>	<index>	Sets the Arbitrary Inter-Frame Space Number (AIFSN) for specified access categoiry and index.
	txops	<access category>	<index>	Configures Opportunity to Transmit Time (TXOPs Time) for specified access categoiry and index.
	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 access point using the applet (GUI), see "Setting the WLAN Quality of Service (QoS) policy" on page 147.

BR7131>admin(network.wireless.qos)> delete

Description

Removes a QoS policy.

Syntax

delete	<qos-name> <all>	Deletes the specified QoS polciy index, or all of the policies (except default policy).

For information on configuring the WLAN QoS options available to the access point using the applet (GUI), see “Setting the WLAN Quality of Service (QoS) policy” on page 147.

Network bandwith management commands

BR7131>admin(network.wireless.bandwidth)>

Description

Displays the Brocade Mobility 7131 Series Access Point Bandwidth Management submenu. The items available under this command include:

show	Displays Bandwidth Management information for how data is processed by the Brocade Mobility 7131 Series Access Point.
set	Defines Bandwidth Management parameters for the Brocade Mobility 7131 Series Access Point.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.bandwidth)> show

Description

Displays the Brocade Mobility 7131 Series Access Point's current Bandwidth Management configuration.

Syntax

show	**summary**	Displays the current Bandwidth Management configuration for defined WLANs and how they are weighted.
	wlan	

Example

```
admin(network.wireless.bandwidth)>show summary

Bandwidth Share Mode Radio 1              : First In First Out

Bandwidth Share Mode Radio 2              : First In First Out

admin(network.wireless.bandwidth)>show wlan

WLAN 1
WLAN Name                   WLAN1
ESSID                       101
Radio Band(s)               2.4 and 5.0 GHz
VLAN                        <none>
Security Policy             Default
QoS Policy                  Default
```

For information on configuring the Bandwidth Management options available to the access point using the applet (GUI), see "Configuring client rate limiting" on page 177.

BR7131>admin(network.wireless.bandwidth)> set

Description

Defines the Brocade Mobility 7131 Series Access Point Bandwidth Management configuration.

Syntax

set	**mode**	<bw-mode>	Defines bandwidth share mode of First In First Out <fifo>, Round Robin <rr> or Weighted Round Robin <wrr>
	weight	<num>	Assigns a bandwidth share allocation for the WLAN <index 1-16 > when Weighted Round Robin <wrr> is selected. The weighting is from 1-10.

For information on configuring the Bandwidth Management options available to the access point using the applet (GUI), see “Configuring client rate limiting” on page 177.

Network Rogue-AP commands

BR7131>admin(network.wireless.rogue-ap)>

Description

Displays the Rogue AP submenu. The items available under this command include:

show	Displays the current Brocade Mobility 7131 Series Access Point Rogue AP detection configuration.
set	Defines the Rogue AP detection method.
Client-scan	Goes to the Rogue AP Client-uscan 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.

BR7131>admin(network.wireless.rogue-ap)> show

Description

Displays the current Brocade Mobility 7131 Series Access Point Rogue AP detection configuration.

Syntax

show	Displays the current Brocade Mobility 7131 Series Access Point Rogue AP detection configuration.

Example

```
admin(network.wireless.rogue-ap)>show

Client Scan                              : disable
Client Scan Interval                     : 60 minutes
On-Channel                             : disable
Detector Radio Scan                    : enable

Auto Authorize Brocade APs            : disable

Approved APs age out                    : 0 minutes
Rogue APs age out                       : 0 minutes
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see "Configuring rogue AP detection" on page 238.

BR7131>admin(network.wireless.rogue-ap)> set

Description

Defines the Brocade Mobility 7131 Series Access Point ACL rogue AP method.

Syntax

set	**Client-scan**	<mode>	Enables or disables to permit clients to scan for rogue APs.
	interval	<minutes>	Define an interval for associated clients to beacon in attempting to locate rogue APs. Value not available unless Client-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).
	ABG-scan	<mode>	Enables or disables A/BG Detector Scan Mode on both bands.
	brocade-ap	<mode>	Enables or disables the Authorize Any AP with a Brocade 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 Client-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 ABG-scan disable
admin(network.wireless.rogue-ap)>set brocade-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

Client Scan                          : enable
Client Scan Interval                 : 10 minutes
On Channel                         : disable
Detector Radio Scan                : disable

Auto Authorize Brocade APs       : enable

Approved AP age out                : 10 minutes
Rogue AP age out                   : 10 minutes
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring rogue AP detection” on page 238.

BR7131>admin(network.wireless.rogue-ap.Client-scan)>

Description

Displays the Rogue-AP Client-scan submenu.

Syntax

add	Add all or just one scan result to Allowed AP list.
show	Displays all APs located by the Client scan.
start	The access point initiates an immediate scan for known and associated clients.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.rogue-ap.Client-scan)> start

Description

Initiates an Client scan from a user provided MAC address.

Syntax

start	<Client-mac>	Initiates Client scan from user provided MAC address.

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see "Configuring rogue AP detection" on page 238.

BR7131>admin(network.wireless.rogue-ap.Client-scan)> show

Description

Displays the results of an Client scan.

Syntax

show	Displays all APs located by the Client scan.

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring rogue AP detection” on page 238.

BR7131>admin(network.wireless.rogue-ap.allowed-list)>

Description

Displays the Rogue-AP allowed-list submenu.

show	Displays the rogue AP allowed list
add	Adds an AP MAC address and ESSID to the allowed list.
delete	Deletes an entry or all entries from the allowed list.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>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

            Allowed AP List
-------------------------------------------------------------------------------
index            ap mac             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 access point using the applet (GUI), see “Configuring rogue AP detection” on page 238.

BR7131>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>	Adds an AP MAC address and ESSID to existing allowed list. “ffffffffffffffff” means any MAC Use a “*” for any ESSID.

Example

```
admin(network.wireless.rogue-ap.allowed-list)>add 00A0F83161BB 103
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        fffffffffff
3          00:A0:F8:40:20:01        Marketing
4          00:A0:F8:31:61:BB        103
```

For information on configuring the Rogue AP options available to the access point using the applet (GUI), see “Configuring rogue AP detection” on page 238.

BR7131>admin(network.wireless.rogue-ap.allowed-list)> delete

Description

Deletes an AP MAC address and ESSID to existing allowed list.

Syntax

delete	<idx> (1-50) <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 access point using the applet (GUI), see "Configuring rogue AP detection" on page 238.

WIPS commands

BR7131>admin(network.wireless.wips)>

Description

Displays the WIPS submenu. The items available under this command include:

show	Displays the current WLAN Intrusion Prevention configuration.
set	Sets WLAN Intrusion Prevention parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.wips)> show

Description

Shows the WLAN Intrusion Prevention configuration.

Syntax

show	Displays the existing Wireless Intrusion Protection System (WIPS) configuration.

Example

```
admin(network.wireless.wips)>show

WIPS Server #1
   IP Address               : 192.168.0.21

WIPS Server #2
   IP Address               : 10.1.1.1
```

admin(network.wireless.wips)>

BR7131>admin(network.wireless.wips)> set

Description

Sets the WLAN Intrusion Prevention configuration.

Syntax

set	<idx 1 and 2> <ip>	Defines the WLAN Intrusion Prevention Server IP Address for (server IPs 1 and 2).

Example

```
admin(network.wireless.wips)>set server 1 192.168.0.21
admin(network.wireless.wips)>
```

Network Client locationing commands

BR7131>admin(network.wireless.Client-locationing)>

Description

Displays the Client Locationing submenu. The items available under this command include:

show	Displays the current Client Locationing configuration.
set	Defines Client Locationing parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.wireless.Client-locationing)> show

Description

Displays the Client probe table configuration

Syntax

show	Displays the MU locationing probe table configuration.

Example

```
admin(network.wireless.Client-locationing)>show

Client Probe Table Mode               : disable
Client Probe Table Size               : 200

admin(network.wireless.Client-locationing)>
```

BR7131>admin(network.wireless.Client-locationing)> set

Description

Defines the Client probe table configuration used for locating clients.

Syntax

set		Defines the Client probe table configuration.
	mode	Enables/disables Client locationing.
	size	Defines the number of clients in the locationing table (the maximum allowed is 200).

Example

```
admin(network.wireless.Client-locationing)>set

admin(network.wireless.Client-locationing)>set mode enable
admin(network.wireless.Client-locationing)>set size 200

admin(network.wireless.Client-locationing)>
```

Network firewall commands

BR7131>admin(network.firewall)>

Description

Displays the Brocade Mobility 7131 Series Access Point firewall submenu. The items available under this command include:

show	Displays the Brocade Mobility 7131 Series Access Point's current firewall configuration.
set	Defines the Brocade Mobility 7131 Series Access Point's firewall parameters.
access	Enables/disables firewall permissions through the LAN and WAN ports.
advanced	Displays interoperaility 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.

BR7131>admin(network.firewall)> show

Description

Displays the Brocade Mobility 7131 Series Access Point firewall parameters.

Syntax

show	Shows all Brocade Mobility 7131 Series Access Point firewall settings.

Example

```
admin(network.firewall)>show

Firewall Status                    : disable
NAT Timeout                        : 10 minutes

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 bytes
max mime headers                   : 16 headers
```

For information on configuring the Firewall options available to the access point using the applet (GUI), see “Configuring firewall settings” on page 213.

BR7131>admin(network.firewall)> set

Description

Defines the Brocade Mobility 7131 Series Access Point firewall parameters.

Syntax

set	**mode**	<mode>	Enables or disables the firewall.
	nat-timeout	<interval>	Defines the NAT timeout value.
	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.
	ip	<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> (with value in range 256 - 34463).
	hdr	<count>	Sets the max number of headers as specified in <count> (with value in range 12 - 34463).

Example

```
admin(network.firewall)>set mode 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
```

BR7131>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. for the specified LAN.
..	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.lan-wan-access)>list lan1

-------------------------------------------------------------------------------
index      from      to      name      prot      start port      end port
-------------------------------------------------------------------------------

1          lan       wan     HTTP      tcp       80              80
2          lan       wan     abc       udp        0              0
3          lan       wan     123456    ah        1440            2048
4          lan       wan     654321    tcp       2048            2048
5          lan       wan     abc       ah        100             1000
```

For information on configuring the Firewall options available to the access point using the applet (GUI), see “Configuring firewall settings” on page 213.

BR7131>admin(network.firewall)> advanced

Description

Displays whether a Brocade Mobility 7131 Series Access Point firewall rule is intended for inbound traffic to an interface or outbound traffic from that interface..

Syntax

show	Shows advanced subnet access parameters.
set	Sets advanced subnet access parameters.
import	Imports rules from subnet 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.adv-lan-access)>inbound
admin(network.firewall.adv-lan-access.inb)>list
-------------------------------------------------------------------------------
Idx  SCR IP-Netmask  Dst IP-Netmask  TP  SPorts  DPorts  Rev  NAT  Action
-------------------------------------------------------------------------------
1    1.2.3.4         2.2.2.2         all 1:      1:      0.0.0.0   deny
     255.0.0.0       255.0.0.0           65535   65535   nat port 33
2    33.3.0.0        10.10.1.1       tcp 1:      1:      11.11.1.0 allow
     255.255.255.0   255.255.255.0       65535   65535   nat port 0
```

For information on configuring the Firewall options available to the access point using the applet (GUI), see “Configuring firewall settings” on page 213.

Network router commands

BR7131>admin(network.router)>

Description

Displays the router submenu. The items available under this command are:

show	Displays the existing Brocade Mobility 7131 Series Access Point router configuration.
set	Sets the RIP parameters.
add	Adds user-defined routes.
delete	Deletes user-defined routes.
list	Lists user-defined routes.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.router)> show

Description

Shows the access point route table.

Syntax

show	**rip**	Displays the rounter's RIP parameters.
	routes	Displays connected routes.

Example

```
admin(network.router)>show rip
rip type                          : off
rip direction                     : both
rip authentication type           : none
rip simple auth password          : *********
rip md5 id 1                      : 1
rip md5 key 1                     : *********
rip md5 id 2                      : 1
rip md5 key 2                     : *********

admin(network.router)>show routes
-------------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
-------------------------------------------------------------------------------
1      192.168.2.0      255.255.255.0    0.0.0.0          lan1        0
2      192.168.1.0      255.255.255.0    0.0.0.0          lan2        0
3      192.168.0.0      255.255.255.0    0.0.0.0          lan1        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         1

Default gateway Interface: wan
```

For information on configuring the Router options available to the access point using the applet (GUI), see "Configuring router settings" on page 178.

BR7131>admin(network.router)> set

Description

Shows the access point route table.

Syntax

set	**auth**	Sets the RIP authentication type (none, simple or MD5).
	dir	Sets RIP direction (rx, tx or both)
	id	Sets MD5 authetication ID (1-256) for specific index (1-2).
	key	Sets MD5 authetication key (up to 16 characters) for specified inded (1-2).
	passwd	Sets the password (up to 16 characters) for simple authentication.
	type	Defines the RIP type (off, ripv1, ripv2, or ripv1v2).
	dgw-iface	Sets the default gateway interface (lan1, lan2, wan or none).

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring router settings” on page 178.

BR7131>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 LAN1, LAN2 or WAN <iface>, and metric set to <metric> (1-65536).

Example

```
admin(network.router)>add 192.168.3.0 255.255.255.0 192.168.2.1 LAN1 1

admin(network.router)>list
------------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
------------------------------------------------------------------------------
1      192.168.3.0      255.255.255.0  192.168.2.1      lan1        1
```

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring router settings” on page 178.

BR7131>admin(network.router)> delete

Description

Deletes user-defined routes.

Syntax

delete	<idx>	Deletes the user-defined route <idx> (1-20) from list.
	all	Deletes all user-defined routes.

Example

```
admin(network.router)>list
-------------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
-------------------------------------------------------------------------------
1      192.168.2.0      255.255.255.0    192.168.0.1      lan1        1
2      192.168.1.0      255.255.255.0    0.0.0.0          lan2        0
3      192.168.0.0      255.255.255.0    0.0.0.0          lan2        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          lan1        0
2      192.168.0.0      255.255.255.0    0.0.0.0          lan1        0

admin(network.router)>
```

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring router settings” on page 178.

BR7131>admin(network.router)> list

Description

Lists user-defined routes.

Syntax

list	Displays a list of user-defined routes.

Example

```
admin(network.router)>list

-------------------------------------------------------------------------------
index  destination      netmask          gateway          interface   metric
-------------------------------------------------------------------------------
1      192.168.2.0      255.255.255.0    192.168.0.1      lan1        1
2      192.168.1.0      255.255.255.0    0.0.0.0          lan2        0
3      192.168.0.0      255.255.255.0    0.0.0.0          lan1        0
```

For information on configuring the Router options available to the access point using the applet (GUI), see “Configuring router settings” on page 178.

Network IP Filter Commands

BR7131>admin(network.ipfilter)>

Description

Displays the ipfilter submenu. The items available under this command are:

show	Displays Global IP Filter table entries.
set	Sets Global IP Filter table entries.
add	Adds a filter to the Global IP Filter table
delete	Deletes a filter from the Global IP Filter table .
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.ipfilter)>show

Description

Displays Global IP Filter table entries.

Syntax

show	Displays Global IP Filter table entries.

Example

```
admin(network.ipfilter)>show

-------------------------------------------------------------------------------
Idx name  Protocol  Port-Start-End  SrcIP-Start-End  DestIP-Start-End  In-Use
-------------------------------------------------------------------------------

admin(network.ipfilter)>
```

BR7131>admin(network.ipfilter)>set

Description

Sets Global IP Filter table entries.

Syntax

set	Sets Global IP Filter table entries.

Example

```
admin(network.ipfilter)>set

name                        : Sets name of IP Filters
protocol                    : Sets the protocol of the IP filter
port-start                  : Sets the starting port of the IP Filter
port-end                    : Sets the end port of the IP Filter
saddr-start                 : Sets the source address start of the IP Filter
saddr-end                   : Sets the source address end of the IP Filter
daddr-start                 : Sets the destination address start of the IP
Filter
daddr-end                   : Sets the destination address end of the IP Filter

admin(network.ipfilter)>
```

BR7131>admin(network.ipfilter)>add

Description

Adds a filter to the Global IP Filter table.

Syntax

add	**filter-name**	<name>	Adds name to IP Filter (up to 20 characters).
	protocol	<loc>	Adds protocol for IP Filter.
	start-port	<port>	Adds a starting port for IP Filter.
	end-port	<port>	Adds an ending port for IP Filter.
	start-src-address	<ip>	Adds a starting source IP address for IP Filter.
	end-src-address	<ip>	Adds an ending source IP address for IP Filter.
	start-dest-address	<ip>	Adds a starting destination IP address for IP Filter.
	end-dest-address	<ip>	Adds an ending destination IP address for IP Filter.

```
admin(network.ipfilter)>
```

BR7131>admin(network.ipfilter)>delete

Description

Deletes a filter from the Global IP Filter table.

Syntax

delete	**index**	<idx>	Deletes a filter index from the Global IP Filter table.
	all		Deletes all filters from the Global IP Filter table.

Example

```
admin(network.ipfilter)>delete all
admin(network.ipfilter)>
```

Network DHCP Client Hostname Option Commands

BR7131>admin(network.dhcpc-host-opt)>

Description

Displays the DHCP client hotsname option submenu. The items available under this command are:

show	Displays the DHCP client hostname option.
set	Sets the DHCP client hostname option.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(network.dhcpc-host-opt)>show

Description

Displays the DHCP client hostname option..

Syntax

show	Displays the DHCP client hostname option.

Example

```
admin(network.dhcpc-host-opt)>show

DHCP Client Hostname Option Mode              : Disable
admin(network.dhcpc-host-opt)>
```

BR7131>admin(network.dhcpc-host-opt)>set

Description

Sets the DHCP client hostname option.

Syntax

show	Sets the DHCP client hostname option mode to either enable or disable.

Example

```
admin(network.dhcpc-host-opt)>set mode disable
admin(network.dhcpc-host-opt)>show

DHCP Client Hostname Option Mode              : Disable
admin(network.dhcpc-host-opt)>
```

System commands

BR7131>admin(system)>

Description

Displays the System submenu. The items available under this command are shown below.

restart	Restarts the Brocade Mobility 7131 Series Access Point.
show	Shows Brocade Mobility 7131 Series Access Point system parameter settings.
set	Defines Brocade Mobility 7131 Series Access Point system parameter settings.
lastpw	Displays last debug password.
exec	Goes to a Linux command menu.
arp	Dispalys the access point's arp table.
power-setup	Goes to the Power Settings submenu.
aap-setup	Goes to the Adaptive AP Settings submenu.
lldp	Goes to the LLDP submenu.
access	Goes to the Brocade Mobility 7131 Series Access Point access submenu where Brocade Mobility 7131 Series Access Point access methods can be enabled.
cmgr	Goes the Certificate Manager submenu.
snmp	Goes to the SNMP submenu.
userdb	Goes to the user database submenu.
radius	Goes to the Radius submenu.
ntp	Goes to the Network Time Protocol submenu.
logs	Displays the log file submenu.
config	Goes to the configuration file update submenu.
fw-update	Goes to the firmware update submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(system)>restart

Description

Restarts the Brocade Mobility 7131 Series Access Point access point.

Syntax

restart	Restarts the Brocade Mobility 7131 Series Access Point.

Example

```
admin(system)>restart

*********************************WARNING************************************
** Unsaved configuration changes will be lost when the access point is reset.
** Please be sure to save changes before resetting.
****************************************************************************

Are you sure you want to restart the Brocade Mobility 7131 Series Access
Point?? (yes/no):

Brocade Mobility 7131 Series Access Point Boot Firmware Version 4.1.0.0-xxx
Copyright(c) Brocade 2010. 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 access point using the applet (GUI), see "Configuring system settings" on page 63.

BR7131>admin(system)>show

Description

Displays high-level system information helpful to differentiate this access point.

Syntax

show	Displays Brocade Mobility 7131 Series Access Point system information.

Example

```
admin(system)>show

system name                          : Brocade Mobility 7131 Series Access Point
system location                      : Atlanta Field Office
admin email address                  : johndoe@mycompany.com
system uptime                        : 0 days 4 hours 41 minutes
led state                            : disable

Brocade Mobility 7131 Series Access Point firmware version          :
4.1.0.0-026D
country code                         : us
ap-mode                              : independent
serial number                        : 05224520500336
model                                : BR7131N

admin(system)>
```

For information on displaying System Settings using the applet (GUI), see “Configuring system settings” on page 63.

BR7131>admin(system)>set

Description

Sets Brocade Mobility 7131 Series Access Point system parameters.

Syntax

set	**name**	<name>	Sets the Brocade Mobility 7131 Series Access Point system name to <name> (1 to 59 characters). The access point does not allow intermediate space characters between characters within the system name. For example, “BR7131 sales” must be changed to “BR7131sales” to be a valid system name.
	loc	<loc>	Sets the Brocade Mobility 7131 Series Access Point system location to <loc> (1 to 59 characters).
	email	<email>	Sets the Brocade Mobility 7131 Series Access Point admin email address to <email> (1 to 59 characters).
	cc	<code>	Sets the Brocade Mobility 7131 Series Access Point country code using two-letters <code>.
	led	<mode>	Sets the access point’s LED state.

```
admin(system)>set name phils
admin(system)>set loc engineering
admin(system)>set email mudskipper@yahoo.com
admin(system)>set cc us
```

NOTE
This name will appear in the WIPS server when one of the radios is configured as a sensor and the WIPS functionality connects to the WIPS server. The WIPS module only accepts names with up to 20 characters, keep that if intending to use this AP as a sensor.

For information on configuring System Settings using the applet (GUI), see “Configuring system settings” on page 63.

BR7131>admin(system)>lastpw

Description

Displays last expired debug password.

Example

```
admin(system)>lastpw

Brocade Mobility 7131 Series Access Point MAC Address is 00:15:70:02:7A:66
Last debug password was brocade
Current debug password used 0 times, valid 4 more time(s)

admin(system)>
```

BR7131>admin(system)>arp

Description

Dispalys the access point's arp table.

Example

```
admin(system)>arp

Address                  HWtype  HWaddress           Flags
Mask            Iface

157.235.92.210           ether   00:11:25:14:61:A8   C                     ixp1
157.235.92.179           ether   00:14:22:F3:D7:39   C                     ixp1
157.235.92.248           ether   00:11:25:B2:09:60   C                     ixp1
157.235.92.180           ether   00:0D:60:D0:06:90   C                     ixp1
157.235.92.3             ether   00:D0:2B:A0:D4:FC   C                     ixp1
157.235.92.181           ether   00:15:C5:0C:19:27   C                     ixp1
157.235.92.80            ether   00:11:25:B2:0D:06   C                     ixp1
157.235.92.95            ether   00:14:22:F9:12:AD   C                     ixp1
157.235.92.161           ether   00:06:5B:97:BD:6D   C                     ixp1
157.235.92.126           ether   00:11:25:B2:29:64   C                     ixp1

admin(system)>
```

Power setup commands

BR7131>admin(system)>power-setup

Description

Displays the Power Setup submenu.

show	Displays the current power setting configuration.
set	Defines the access point's power setting configuration.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the Brocade Mobility 7131 Series Access Point system flash.
quit	Quits the CLI and exits the current session.

For information on configuring power settings using the applet (GUI), see "Configuring power settings" on page 67.

BR7131>admin(system.power-setup)>show

Description

Displays the access point's current power configuration.

Syntax

show	Displays the access point's current power configuration.

Example

```
admin(system.power-setup)>show

Power Mode                                    : 3af
Power Status                                  : Mid Power
Default Radio                                 : Radio2

admin(system.power-setup)>
```

For information on configuring power settings using the applet (GUI), see "Configuring power settings" on page 67.

BR7131>admin(system.power-setup)>set

Description

Sets Brocade Mobility 7131 Series Access Point's power consumption configuration.

Syntax

set	**mode**	Sets the power mode to either Auto or 3af. Changing the mode requires restarting the access point.
	power-option	Defines the power option.
	def-radio	Defines the access point's default radio (1-Radio1, 2-Radio2).

```
admin(system.power-setup)>set mode Auto
admin(system.power-setup)>set def-radio 1
```

For information on configuring power settings using the applet (GUI), see "Configuring power settings" on page 67..

Adaptive AP setup commands

BR7131>admin(system)>aap-setup

Description

Displays the Adaptive AP submenu.

show	Displays Adaptive AP information.
set	Defines the Adaptive AP configuration.
delete	Deletes static controller address assignments.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the Brocade Mobility 7131 Series Access Point system flash.
quit	Quits the CLI and exits the current session.

For information on configuring adaptive AP using the applet (GUI), see "Adaptive AP setup" on page 72.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP" on page 613.

BR7131>admin(system.aap-setup)>show

Description

Displays the access point's Adaptive AP configuration.

Syntax

show	Displays the access point's Adaptive AP configuration.

Example

```
admin(system.aap-setup)>show

Auto Discovery Mode                          : disable
Controller Name                              : greg
Static IP Port                               : 24576
Static IP Address                            :
IP Address 1                                 : 0.0.0.0
IP Address 2                                 : 0.0.0.0
IP Address 3                                 : 0.0.0.0
IP Address 4                                 : 0.0.0.0
IP Address 5                                 : 0.0.0.0
IP Address 6                                 : 0.0.0.0
IP Address 7                                 : 0.0.0.0
IP Address 8                                 : 0.0.0.0
IP Address 9                                 : 0.0.0.0
IP Address 10                                : 0.0.0.0
IP Address 11                                : 0.0.0.0
IP Address 12                                : 0.0.0.0

Tunnel to Controller                         : disable
AC Keepalive                                 : 5
Load Balancing                               : enable
Inactivity Timeout                           : 60

Current Controller                          : 157.235.22.11
AP Adoption State                             : AAP not adopted

admin(system.aap-setup)>
```

For information on configuring adaptive AP using the applet (GUI), see "Adaptive AP setup" on page 72.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP" on page 613.

BR7131>admin(system.aap-setup)>set

Description

Sets Brocade Mobility 7131 Series Access Point's Adaptive AP configuration.

Syntax

set	**auto-discovery**	Sets the controller auto-discovery mode (enable/disable).
	ipadr	Defines the controller IP address used.
	name	Defines the controller name for DNS lookups (up to 127 characters).
	port	Sets the port.
	passphrase	Defines the pass phrase or key for controller connection.
	tunnel-to-controller	Enables/disables the tunnel between controller and access point.
	ac-keepalive	Defines the keepalive interval.

```
admin(system.aap-setup)>set auto-discovery enable
admin(system.aap-setup)>set ipadr 192.235.111.10
admin(system.aap-setup)>set port 1812
admin(system.aap-setup)>set passphrase mudskipper
```

For information on configuring adaptive AP using the applet (GUI), see "Adaptive AP setup" on page 72.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP" on page 613.

BR7131>admin(system.aap-setup)>delete

Description

Deletes static controller address assignments.

Syntax

delete	<idx>	Deletes static controller address assignments by selected index.
	<all>	Deletes all assignments.

Example

```
admin(system.aap-setup)>delete 1

admin(system.aap-setup)>
```

For information on configuring Adaptive AP using the applet (GUI), see "Adaptive AP setup" on page 72.

For an overview of adaptive AP functionality and its implications, see "Adaptive AP" on page 613.

LLDP Commands

BR7131>admin(system)>lldp

Description

Displays the LLDP submenu.

show	Displays LLDP information.
set	Sets LLDP parameters.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the access point system flash.
quit	Quits the CLI and exits the current session.

For information on configuring LLDP using the applet (GUI), see “Configuring LLDP settings” on page 98.

BR7131>admin(system.lldp)>show

Description

Displays LLDP information.

Syntax

show	Displays LLDP information.

```
admin(system.lldp)>show
LLDP Status                     :enable
LLDP Refresh Interval           :30
LLDP Holdtime Mutiplier         :4
admin(system.lldp)>
```

For information on configuring LLDP using the applet (GUI), see “Configuring LLDP settings” on page 98.

BR7131>admin(system.lldp)>set

Description

Sets the LLDP configuration.

Syntax

set		Sets the LLDP configurarion.
	lldp-mode	Enables or disables LLDP support.
	lldp-refresh	Sets the LLDP refresh interval between 15 - 32768 seconds
	lldp-mulitplier	Sets the LLDP holdtime multiplier between 2 - 10.

```
admin(system.lldp)>set lldp-mode enable
admin(system.lldp)>set lldp-refresh 100
admin(system.lldp)>set lldp-holdtime 2
admin(system.lldp)>
```

For information on configuring LLDP using the applet (GUI), see “Configuring LLDP settings” on page 98.

System access commands

BR7131>admin(system)>access

Description

Displays the access point access submenu.

show	Displays Brocade Mobility 7131 Series Access Point system access capabilities.
set	Goes to the Brocade Mobility 7131 Series Access Point system access submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the Brocade Mobility 7131 Series Access Point system flash.
quit	Quits the CLI and exits the current session.

BR7131>admin(system.access)>set

Description

Defines the permissions to access the Brocade Mobility 7131 Series Access Point applet, CLI, SNMP as well as defining their timeout values.

Syntax

set	**applet**		Defines the applet HTTP/HTTPS access parameters.
	app-timeout	<minutes>	Sets the applet timeout. Default is 300 Mins.
	sslv2	<mode>	Enables/disables SSL v2 support.
	cli		Defines CLI Telnet access parameters. Enables/disables access from lan and wan.
	ssh		Sets the CLI SSH access parameters.
	auth-timout	<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.
	snmp		Sets SNMP access parameters for the AP's LAN and WAN ports.
	admin-auth		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 (up to 31 characters).
	mode	<mode>	Enables/disables the access point message mode.
	msg		Defines the access point login message text (up to 511 characters).

For information on configuring access point access settings using the applet (GUI), see "Configuring data access" on page 74.

BR7131>admin(system.access)>show

Description

Displays the current Brocade Mobility 7131 Series Access Point access permissions and timeout values.

Syntax

show	Shows all of the current system access settings for the Brocade Mobility 7131 Series Access Point..

Example

```
admin(system.access)>show

--------------------------------From LAN1-------From LAN2-------From WAN
applet http access                enable          enable          enable
applet http access                enable          enable          enable
cli telnet access                 enable          enable          enable
cli ssh access                    enable          enable          enable
snmp access                       enable          enable          enable

SSLV2                                          : enable

http/s timeout                                 : 0
ssh server authetnication timeout              : 120
ssh server inactivity timeout                  : 120
admin authetnication mode                      : local
Login Message Mode                             : disable
Login Message                                :
```

Related Commands

set	Defines the Brocade Mobility 7131 Series Access Point system access capabilities and timeout values.

For information on configuring access point access settings using the applet (GUI), see “Configuring data access” on page 74.

System certificate management commands

BR7131>admin(system)>cmgr

Description

Displays the Certificate Manager submenu. The items available under this command include:

genreq	Generates a Certificate Request.
delself	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.
expcert	Exports the certificaqte file.
impcert	Imports the certificate file.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>admin(system.cmgr)> genreq

Description

Generates a certificate request.

Syntax

genreq	<IDname>	<Subject>	[-ou <OrgUnit>]	[-on <OrgName>]	[-cn <City>]	[-st <State>]	. . .
	. . .	[-p <PostCode>]	[-cc <CCode>]	[-e <Email>]	[-d <Domain>]	[-i <IP>]	[-sa <SAlgo>]
		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	Organization Unit (up to 49 chars)
<Department>	Organization Name (up to 49 chars)
-on <OrgName>	City Name of Organization (up to 49 chars)
-cn <City>	State Name (up to 49 chars)
-st <State>	Postal code (9 digits)
-p <PostCode>	Country code (2 chars)
-cc <CCode>	E-mail Address (up to 49 chars)
-e <Email>	Domain Name (up to 49 chars)
-d <Domain>	IP Address (a.b.c.d)
-i <IP>	Signature Algorithm (one of MD5-RSA or SHA1-RSA
-sa <SAlgo>	Key size in bits (one of 512, 1024, or 2048)
-k <KSize>	

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
Retreiving the certificate request
The certificate request is
-----BEGIN CERTIFICATE REQUEST-----
MIHzMIGeAgEAMDkxEjAQBgNVBAoTCU15Q29tcGFueTEPMA0GA1UECxMGTXlEZXB0
MRIwEAYDVQQDEwlNeVN1YmplY3QwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAtKcX
plKFCFAJymTFX71yuxY1fdS7UEhKjBsH7pdqnJnsASK6ZQGAqerjpKScWV1mzYn4
1q2+mgGnCvaZUlIo7wIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCClQ5LHdbG/C1f
Bj8AszttSo/bA4dcX3vHvhhJcmuuWO9LHS2imPA3xhX/d6+Q1SMbs+tG4RP0lRSr
iWDyuvwx
-----END CERTIFICATE REQUEST-----
```

For information on configuring certificate management settings using the applet (GUI), see "Managing certificate authority (CA) certificates" on page 78.

BR7131>admin(system.cmgr)> delself

Description

Deletes a self certificate.

Syntax

delself	<IDname>	Deletes the self certificate named <IDname>.

Example

```
admin(system.cmgr)>delself MyCert2
```

For information on configuring self certificate settings using the applet (GUI), see "Creating self certificates for accessing the VPN" on page 80.

BR7131>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> (7 characters).

For information on configuring self certificate settings using the applet (GUI), see "Creating self certificates for accessing the VPN" on page 80.

BR7131>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 for accessing the VPN" on page 80.

BR7131>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 79.

BR7131>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 79.

BR7131>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 79.

BR7131>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 79.

BR7131>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 for accessing the VPN" on page 80.

BR7131>admin(system.cmgr)> listprivkey

Description

Lists the names of private keys.

Syntax

listprivkey	Lists all private keys and displays their certificate associations.

For information on configuring certificate settings using the applet (GUI), see “Importing a CA certificate” on page 79.

BR7131>admin(system.cmgr)> expcert

Description

Exports the certificate file to a user defined location.

Syntax

expcert	Exports the access point's CA or Self certificate file.

To export certificate information from a Brocade Mobility 7131 Series Access Point model access point:

```
admin(system.cmgr)>expcert ?

<type> <file name> <cr>            : type: ftp/tftp
                                   : file name: Certificate file name
                                   : Server options for this file are the same
                                   : as that for the configuration file

admin(system.cmgr)>expcert tftp AP-71x1certs.txt
```

To configue certificate management settings while conducting a firmware update or restoring a factory default configuratrion:

```
admin(system.cmgr)> ?

genreq                             : generate a certificate request
delself                            : deletes a signed certificate
loadself                           : loads a signed certficiate signed by the
CA listself                           : lists the loaded signed self
certificate
loadca                             : loads the root CA certificate
delca                              : deletes the root CA certificate
listca                             : lists the loaded root CA certificate
showreq                            : displays certificate request in PEM
format
delprivkey                         : deletes the private key
listprivkey                        : lists the names of the private keys
expcert                            : exports the target certficate file
impcert                            : imports the target certficate file
(..)                               : goes to the parent menu
/                                  : goes to the root menu
save                               : saves the configuration to system flash
quit                               : quits the CLI session
```

For information on configuring certificate settings using the applet (GUI), see "Importing a CA certificate" on page 79.

BR7131>admin(system.cmgr)> impcert

Description

Imports the target certificate file.

impcert	Imports the target certificate file.

To import certificate information from a Brocade Mobility 7131 Series Access Point model access point:

```
admin(system.cmgr)>impcert ?

<type> <file name> <cr>            : type: ftp/tftp
                                   : file name: Certificate file name
                                   : Server options for this file are the same
                                   : as that for the configuration file

admin(system.cmgr)>impcert tftp Brocade Mobility 7131 Series Access
Pointcerts.txt
```

To configue certificate management settings while conducting a firmware update or restoring a factory default configuratrion:

```
admin(system.cmgr)> ?

genreq                             : generate a certificate request
delself                            : deletes a signed certificate
loadself                           : loads a signed certficiate signed by the
CA listself                           : lists the loaded signed self
certificate
loadca                             : loads the root CA certificate
delca                              : deletes the root CA certificate
listca                             : lists the loaded root CA certificate
showreq                            : displays certificate request in PEM
format
delprivkey                         : deletes the private key
listprivkey                        : lists the names of the private keys
expcert                            : exports the target certficate file
impcert                            : imports the target certficate file
(..)                               : goes to the parent menu
/                                  : goes to the root menu
save                               : saves the configuration to system flash
quit                              : quits the CLI session
```

For information on configuring certificate settings using the applet (GUI), see “Importing a CA certificate” on page 79.

System SNMP commands

BR7131>admin(system)> snmp

Description

Displays the SNMP submenu. The items available under this command are shown below.

access	Goes to the SNMP access submenu.
traps	Goes to the SNMP traps submenu.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

System SNMP access commands

BR7131>admin(system.snmp.access)

Description

Displays the SNMP Access menu. The items available under this command are shown below.

show	Shows SNMP v3 engine ID.
add	Adds SNMP access entries.
delete	Deletes SNMP access entries.
list	Lists SNMP access entries.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to system flash.
quit	Quits the CLI.

BR7131>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-713X 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 90.

BR7131>admin(system.snmp.access)> add

Description

Adds SNMP access entries for specific v1v2 and v3 user definitions.

Syntax

add	**acl**	<ip1>	<ip2>	Adds an entry to the SNMP access control list with <ip1> as the starting IP address and <ip2> and as the ending IP address.	
	v1v2c	<comm>	<access>	<oid>	
				: comm - community string 1 to 31 characters : access - read/write access - (ro,rw) : oid - string 1 to 127 chars - E.g. 1.3.6.1	
	v3	<user>	<access>	<oid>	<sec>
		<auth>	<pass1>	<priv>	<pass2>
				: user - username 1 to 31 characters : access - read/write access - (ro,rw) : oid - string 1 to 127 chars - E.g. 1.3.6.1 : sec - security - (none,auth,auth/priv) : auth - algorithm - (md5,sha1) : *(required only if sec is - auth,auth/priv)* : pass1 - auth password - 8 to 31 chars : *(required only if sec is 'auth,auth/priv')* : priv - algorithm - (des, aes) : *(required only if sec is 'auth/priv')* : pass2 - privacy password - 8 to 31 chars : (required only if sec is '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 90.

BR7131>admin(system.snmp.access)> delete

Description

Deletes SNMP access entries for specific v1v2 and v3 user definitions.

Syntax

delete	**acl**	<idx>	Deletes entry <idx> (1-10) from the access control list.
		all	Deletes all entries from the access control list.
	v1v2c	<idx>	Deletes entry <idx> (1-10) from the v1/v2 configuration list.
		all	Deletes all entries from the v1/v2 configuration list.
	v3	<idx>	Deletes entry <idx> (1-10) from the v3 user definition list.
		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 90.

BR7131>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 by index <idx> (1-10).
		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 v1v2c
-----------------------------------------------------------------
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                              : 2
username                           : judy
access permission                  : read/write
object identifier                  : 1.3.6.1
security level                     : auth/priv
auth algorithm                     : md5
auth password                      : ********
privacy algorithm                  : des
privacy password                   : *******
```

For information on configuring SNMP access settings using the applet (GUI), see "Configuring SNMP access control" on page 90.

System SNMP traps commands

BR7131>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.

BR7131>admin(system.snmp.traps)> show

Description

Shows SNMP trap parameters.

Syntax

show	**trap**	Shows SNMP trap parameter settings.
	rate-trap	Shows SNMP rate-trap parameter settings.

Example

```
admin(system.snmp.traps)>show trap

SNMP Client Traps
     Client associated                    : enable
     Client unassociated                  : disable
     Client denied association            : disable
     Client denied authentication         : disable

SNMP Traps
     snmp authentication 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 seconds

SNMP System Traps
     system cold start                 : disable
     system config changed             : disable
     rogue ap detection                : disable
     ap radar detection                : disable
     wpa counter measure               : disable
     Client hotspot status                : disable
     vlan                              : disable
     lan monitor                       : disable
     DynDNS Update                     : enable
     wlan kerb auth failed             : disable
     wwan event                        : disable
```

For information on configuring SNMP traps using the applet (GUI), see "Enabling SNMP traps" on page 92.

BR7131>admin(system.snmp.traps)> set

Description

Sets SNMP trap parameters.

Syntax

set	**Client-assoc**	**enable/disable**			Enables/disables the Client associated trap.
	Client-unassoc	**enable/disable**			Enables/disables the Client unassociated trap.
	Client-deny-assoc	**enable/disable**			Enables/disables the Client association denied trap.
	Client-deny-auth	**enable/disable**			Enables/disables the Client authentication denied trap.
	snmp-auth	**enable/disable**			Enables/disables the authentication failure trap.
	snmp-acl	**enable/disable**			Enables/disables the SNMP ACL violation trap.
	port	**enable/disable**			Enables/disables the physical port status trap.
	dos-attack	**enable/disable**			Enables/disables the denial of service trap.
	dyndns-update	**enable/disable**			Enables/disables dyndns update trap.
	interval	**<rate>**			Sets denial of service trap interval.
	cold	**enable/disable**			Enables/disables the system cold start trap.
	cfg	**enable/disable**			Enables/disables a configuration changes trap.
	rogue-ap	**enable/disable**			Enables/disables a trap when a rogue-ap is detected.
	ap-radar	**enable/disable**			Enables/disables the AP Radar Detection trap.
	wpa-counter	**enable/disable**			Enables/disables the WPA counter measure trap.
	hotspot-Client-status	**enable/disable**			Enables/disables the hotspot Client status trap.
	vlan	**enable/disable**			Enables/disables VLAN traps.
	lan-monitor	**enable/disable**			Enables/disables LAN monitor traps.
	rate	<rate>	<scope>	<value>	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>.
	min-pkt	<pkt>			Sets the minimum number of packets required for rate traps to fire (**1**-**65535**).
	dyndns-update	**enable/disable**			Enables/disables dyndns update trap.
	wlan-kerb-auth-fail	**enable/disable**			Enables/disables the WLAN Kerberos authentication trap.

wwan-event	**enable/disable**	Enables/disables the WWAN event trap.
all	**enable/disable**	Enables/disables each trap.

For information on configuring SNMP traps using the applet (GUI), see "Configuring specific SNMP traps" on page 94.

BR7131>admin(system.snmp.traps)> add

Description

Adds SNMP trap entries.

Syntax

add	**v1v2**	<ip>	<port>	<comm>	<ver>			
		Adds 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>
		Adds 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/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)						

Example

```
admin(system.snmp.traps)>add v1v2 203.223.24.2 333 mycomm v1
admin(system.snmp.traps)>list v1v2c
-------------------------------------------------------------------------
index   dest ip          dest port      community        version
-------------------------------------------------------------------------
1       203.223.24.2     333            mycomm           v1

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 96.

BR7131>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 86.

BR7131>admin(system.snmp.traps)> list

Description

Lists SNMP trap entries.

Syntax

list	**v1v2c**		Lists SNMP v1/v2c access entries.
	v3	<idx>	Lists SNMP v3 access entry <idx>.
		all	Lists all SNMP v3 access entries.

Example

```
admin(system.snmp.traps)>add v1v2 203.223.24.2 162 mycomm v1
admin(system.snmp.traps)>list v1v2c
-------------------------------------------------------------------------
index   dest ip          dest port      community        version
-------------------------------------------------------------------------
1       203.223.24.2     162            mycomm           v1

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 96.

System user database commands

BR7131>admin(system)> userdb

Description

Goes to the user database submenu.

Syntax

user	Goes to the user submenu.
group	Goes to the group submenu.
save	Saves the configuration to system flash.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

8.4.5.1 adding and removing users from the user databse

BR7131>admin(system.userdb)> user

Description

Adds and remvoves users from the user database and defines user passwords.

Syntax

add	Adds a new user.
delete	Deletes a new user.
clearall	Removes all existing user IDs from the system.
set	Sets a password for a user.
show	Displays the current user database configuration.
save	Saves the configuration to system flash.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.user)> add

Description

Adds a new user to the user database.

Syntax

add	Adds a new user ID <userid> and password <passwd> string to the user database.

Example

```
admin(system.userdb.user>add george password

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.user)> delete

Description

Removes a new user to the user database.

Syntax

delete	Removes a new user to the user database.

Example

```
admin(system.userdb.user>delete george

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.user)>clearall

Description

Removes all existing user IDs from the system.

Syntax

clearall	Removes all existing user IDs from the system.

Example

```
admin(system.userdb.user>clearall

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.user)>set

Description

Sets a password for a user..

Syntax

set	<user> <passwd>	Sets user <userid> and password <passwd> string for a specific user.

Example

```
admin(system.userdb.user>set george password

admin(system.userdb.user>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

Adding and removing groups from the user database

BR7131>admin(system.userdb)> group

Description

Adds and remvoves groups from the user database.

Syntax

create	Creates a group name.
delete	Deletes a group name.
clearall	Removes all existing group names from the system.
add	Adds a user to an existing group.
remove	Removes a user from an existing group.
show	Displays existing groups.
save	Saves the configuration to system flash.
..	Goes to the parent menu.
/	Moves back to root menu.

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.group)> create

Description

Creates a group name. Once defined, users can be added to the group.

Syntax

create	Creates a group name. Once defined, users can be added to the group.

Example

```
admin(system.userdb.group)>create 2

admin(system.userdb.group)>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.group)> delete

Description

Deletes an existing group.

Syntax

delete	Deletes an existing group.

Example

```
admin(system.userdb.group)>delete 2

admin(system.userdb.group)>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.group)> clearall

Description

Removes all existing group names from the system.

Syntax

clearall	Removes all existing group names from the system.

Example

```
admin(system.userdb.group)>clearall

admin(system.userdb.group)>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.group)> add

Description

Adds a user to an existing group.

Syntax

add	<userid> <group>	Adds a user <userid> to an existing group <group>.

Example

```
admin(system.userdb.group)>add lucy group x

admin(system.userdb.group)>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

BR7131>admin(system.userdb.group)> remove

Description

Removes a user from an existing group.

Syntax

remove	<userid> <group>	Removes a user <userid> from an existing group<group> .

Example

```
admin(system.userdb.group)>remove lucy group x

admin(system.userdb.group)>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254

BR7131>admin(system.userdb.group)> show

Description

Displays existing groups.

Syntax

show		Displays existing groups and users,
	users	Displays configured user IDs for a group.
	groups	Displays configured groups.

Example

```
admin(system.userdb.group)>show groups

List of Group Names
                        : engineering
                        : marketing
                        : demo room

admin(system.userdb.group)>
```

For information on configuring User Database permissions using the applet (GUI), see "Defining user access permissions by group" on page 254.

System Radius commands

BR7131>admin(system)> radius

Description

Goes to the Radius system submenu.

Syntax

eap	Goes to the EAP submenu.
policy	Goes to the access policy submenu.
ldap	Goes to the LDAP submenu.
proxy	Goes to the proxy submenu.
client	Goes to the client submenu.
set	Sets Radius parameters.
show	Displays Radius parameters.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring Radius using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius)> set/show

Description

Sets or displays the Radius user database.

Syntax

set	Sets the Radius user database.
show all	Displays the Radius user database.

Example

```
admin(system.radius)>set database local
admin(system.radius)>show all

Database                : local

admin(system.radius)>
```

For information on configuring Radius using the applet (GUI), see "Configuring user authentication" on page 245.

8.4.6.1 BR7131>admin(system.radius)> eap

Description

Goes to the EAP submenu.

Syntax

peap	Goes to the Peap submenu.
ttls	Goes to the TTLS submenu.
import	Imports the requested EAP certificates.
set	Defines EAP parameters.
show	Displays the EAP configuration.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring EAP Radius using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.eap)> peap

Description

Goes to the Peap submenu.

Syntax

set	Defines Peap parameters.
show	Displays the Peap configuration.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring PEAP Radius using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.eap.peap)> set/show

Description

Defines and displays Peap parameters

Syntax

set	Sets the Peap authentication <peap type> (to either gtc or mschapv2).
show	Displays the Peap authentication type.

Example

```
admin(system.radius.eap.peap)>set auth gtc
admin(system.radius.eap.peap)>show

PEAP Auth Type                    : gtc
```

For information on configuring EAP PEAP Radius values using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.eap)> ttls

Description

Goes to the TTLS submenu.

Syntax

set	Defines TTLS parameters.
show	Displays the TTLS configuration.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring EAP TTLS Radius values using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.eap.ttls)> set/show

Description

Defines and displays TTLS parameters

Syntax

set	Sets the default TTLS authentication <ttls type> (to either pap, md5 or mschapv2).
show	Displays the TTLS authentication <type>.

Example

```
admin(system.radius.eap.ttls)>set auth pap
admin(system.radius.eap.ttls)>show

TTLS Auth Type                    : pap
```

For information on configuring EAP TTLS Radius values using the applet (GUI), see "Configuring user authentication" on page 245.

8.4.6.2 BR7131>admin(system.radius)> policy

Description

Goes to the access policy submenu.

Syntax

set	Sets a group's WLAN access policy.
access-time	Goes to the time based login submenu.
show	Displays the group's access policy.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring Radius access policies using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.policy)> set

Description

Defines the group's WLAN access policy.

Syntax

set	<group name> <wlan name>	Defines a group's <group> WLAN access policy (defined as a string) delimited by a space.

Example

```
admin(system.radius.policy)>set engineering 16

admin(system.radius.policy)>
```

For information on configuring Radius WLAN policy values using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.policy)> access-time

Description

Goes to the time-based login submenu.

Syntax

set	<group> <access-time>	Defines a target group's access time permissions. Access time is in DayDDDD-DDDD format.
show		Displays the group's access time rule.
save		Saves the configuration to system flash.
quit		Quits the CLI.
..		Goes to the parent menu.
/		Goes to the root menu.

Example

```
admin(system.radius.policy.access-time)>show

List of Access Policies

1                    : Tue0830-2200, We2000-2300, Th1100-1930
2                    : Any0000-2359
10                   : Any0000-2359
12                   : Any0000-2359
```

Context	Command	Description
system>radius>policy>access-time	set start-time <group> <value>	group = Valid group name.. value = 4 digit value representing HHMM (0000-2359 allowed).
system>radius>policy>access-time	set end-time <group> <value>	group = Valid group name.. value = 4 digit value representing HHMM (0000-2359 allowed). The end time should be greater than the start time.
system>radius>policy>access-time	set access-days <group> <day-selector-keyword>	group = Valid group name. day-selector-keyword = The allowed values are: Mo, Tu, We, Th, Fr, Sa, Su, Weekdays, Weekends, all.

For information on configuring Radius WLAN policy values using the applet (GUI), see "Configuring user authentication" on page 245.

BR7131>admin(system.radius.policy)> show

Description

Displays a group's access policy.

Syntax

show	Displays a group's access policy.

Example

```
admin(system.radius.policy)>show

List of Access Policies

engineering                    : 16
marketing                      : 10
demo room                      : 3
test demo                      : No Wlans

admin(system.radius.policy)>
```

For information on configuring Radius WLAN policy values using the applet (GUI), see "Configuring user authentication" on page 245

8.4.6.3 BR7131>admin(system.radius)> ldap

Description

Goes to the LDAP submenu.

Syntax

set	Defines the LDAP parameters.
show all	Displays existing LDAP parameters.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring a Radius LDAP server using the applet (GUI), see "Configuring LDAP authentication" on page 248.

BR7131>admin(system.radius.ldap)> set

Description

Defines the LDAP parameters.

Syntax

set		Defines the LDAP parameters.
	ipadr	Sets LDAP IP address.
	port	Sets LDAP server port.
	binddn	Sets LDAP bind distinguished name.
	basedn	Sets LDAP base distinguished name.
	passwd	Sets LDAP server password.
	login	Sets LDAP login attribute.
	pass_attr	Sets LDAP password attribute.
	groupname	Sets LDAP group name attribute.
	filter	Sets LDAP group membership filter.
	membership	Sets LDAP group membership attribute.

Example

```
admin(system.radius.ldap)>set ipadr 157.235.121.12
admin(system.radius.ldap)>set port 1812
admin(system.radius.ldap)>set binddn 123
admin(system.radius.ldap)>set basedn 123
admin(system.radius.ldap)>set passwd mudskipper
admin(system.radius.ldap)>set login muddy
admin(system.radius.ldap)>set pass_attr 123
admin(system.radius.ldap)>set groupname 0.0.0.0
admin(system.radius.ldap)>set filter 123
admin(system.radius.ldap)>set membership radiusGroupName

admin(system.radius.ldap)>
```

For information on configuring a Radius LDAP server using the applet (GUI), see “Configuring LDAP authentication” on page 248.

BR7131>admin(system.radius.ldap)> show all

Description

Displays existing LDAP parameters.

Syntax

show all	Displays existing LDAP parameters.

Example

```
admin(system.radius.ldap)>show all

LDAP Server IP                    : 0.0.0.0
LDAP Server Port                  : 389
LDAP Bind DN                      : cn=manager, o=trion
LDAP Base DN                      : 0=trion
LDAP Login Attribute              : (uid=%{Stripped-User-Name:-%{User-Name}})
LDAP Password attribute           : userPassword
LDAP Group Name Attribue          : cn
LDAP Group Membership Filter      :
(|(&(objectClass=GroupOfNames)(member=%{Ldap-objectClass=GroupOfUniqueNames)(
uniquemember=%{Ldap-UserDn})))
LDAP Group Membership Attribute   : radiusGroupName

admin(system.radius.ldap)>
```

For information on configuring a Radius LDAP server using the applet (GUI), see "Configuring LDAP authentication" on page 248.

8.4.6.4 BR7131>admin(system.radius)> proxy

Description

Goes to the Radius proxy server submenu.

Syntax

add	Adds a proxy realm.
delete	Deletes a proxy realm.
clearall	Removes all proxy server records.
set	Sets proxy server parameters.
show	Displays current Radius proxy server parameters.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring Radius proxy server values using the applet (GUI), see "Configuring a proxy Radius server" on page 250.

BR7131>admin(system.radius.proxy)> add

Description

Adds a proxy.

Syntax

add			Adds a proxy realm.
	name	<name>	Realm name.
	ip1	<ip1>	Authentication server IP address.
	port	<port>	Authentication server port.
	sec	<sec>	Shared secret password.

Example

```
admin(system.radius.proxy)>add lancelot 157.235.241.22 1812 muddy

admin(system.radius.proxy)>
```

For information on configuring Radius proxy server values using the applet (GUI), see "Configuring a proxy Radius server" on page 250.

BR7131>admin(system.radius.proxy)> delete

Description

Adds a proxy.

Syntax

delete	<realm>	Deletes a realm name.

Example

```
admin(system.radius.proxy)>delete lancelot

admin(system.radius.proxy)>
```

For information on configuring Radius proxy server values using the applet (GUI), see "Configuring a proxy Radius server" on page 250.

BR7131>admin(system.radius.proxy)> clearall

Description

Removes all proxy server records from the system.

Syntax

clearall	Removes all proxy server records from the system.

Example

```
admin(system.radius.proxy)>clearall

admin(system.radius.proxy)>
```

For information on configuring Radius proxy server values using the applet (GUI), see "Configuring a proxy Radius server" on page 250.

BR7131>admin(system.radius.proxy)> set

Description

Sets Radius proxy server parameters.

Syntax

set		Sets Radius proxy server parameters.
	delay	Defines retry delay time (in seconds) for the proxy server.
	count	Defines retry count value for the proxy server.

Example

```
admin(system.radius.proxy)>set delay 10
admin(system.radius.proxy)>set count 5

admin(system.radius.proxy)>
```

For information on configuring Radius proxy server values using the applet (GUI), see "Configuring a proxy Radius server" on page 250.

8.4.6.5 BR7131>admin(system.radius)> client

Description

Goes to the Radius client submenu.

Syntax

add	Adds a Radius client to list of available clients.
delete	Deletes a Radius client from list of available clients.
show	Displays a list of configured clients.
save	Saves the configuration to system flash.
quit	Quits the CLI.
..	Goes to the parent menu.
/	Goes to the root menu.

For information on configuring Radius client values using the applet (GUI), see "Configuring the Radius Server" on page 245.

BR7131>admin(system.radius.client)> add

Description

Adds a Radius client to those available to the Radius server.

Syntax

add			Adds a proxy.
	ip	<ip>	Client's IP address.
	mask	<ip1>	Network mask address of the client.
	secret	<sec>	Shared secret password.

Example

```
admin(system.radius.client)>add 157.235.132.11 255.255.255.225 muddy

admin(system.radius.client)>
```

For information on configuring Radius client values using the applet (GUI), see "Configuring the Radius Server" on page 245.

BR7131>admin(system.radius.client)> delete

Description

Removes a specified Radius client from those available to the Radius server.

Syntax

delete	**ip**	Removes a specified Radius client <ipadr> from those available to the Radius server

Example

```
admin(system.radius.client)>delete 157.235.132.11

admin(system.radius.client)>
```

For information on configuring Radius client values using the applet (GUI), see "Configuring the Radius Server" on page 245.

BR7131>admin(system.radius.client)> show

Description

Displays a list of configured Radius clients.

Syntax

show	Removes a specified Radius client from those available to the Radius server.

Example

```
admin(system.radius.client)>show
-------------------------------------------------------------------------------
Idx     Subnet/Host      Netmask            SharedSecret
-------------------------------------------------------------------------------
1       157.235.132.11   255.255.255.225    *****

admin(system.radius.client)>
```

For information on configuring Radius client values using the applet (GUI), see "Configuring the Radius Server" on page 245.

System Network Time Protocol (NTP) commands

BR7131>admin(system)> ntp

Description

Displays the NTP menu. The correct network time is required for numerous functions to be configured accurately on the Brocade Mobility 7131 Series Access Point.

Syntax

show	Shows NTP parameters settings.
date-zone	Show date, time and time zone.
zone-list	Displays list of time zones.
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.

For information on configuring NTP using the applet (GUI), see “Configuring network time protocol (NTP)” on page 99.

BR7131>admin(system.ntp)> show

Description

Displays the NTP server configuration.

Syntax

show	Shows all NTP server settings.

Example

```
admin(system.ntp)>show

current time                        : 2010-03-29 14:35:20

time zone:                          : UTC

ntp mode                            : enable
```

For information on configuring NTP using the applet (GUI), see "Configuring network time protocol (NTP)" on page 99.

BR7131>admin(system.ntp)> date-zone

Description

Show date, time and time zone.

Syntax

date-zone	Show date, time and time zone.

Example

```
admin(system.ntp)>date-zone

Date/Time          : Sat 1970-Jan-03 20:06:22 +0000 UTC

Time Zone          : UTC
```

For information on configuring NTP using the applet (GUI), see "Configuring network time protocol (NTP)" on page 99.

BR7131>admin(system.ntp)> zone-list

Description

Displays an extensive list of time zones for countries around the world.

Syntax

zone-list	Displays list of time zone indexes for every known zone.

Example

```
admin(system.ntp)> zone-list
```

For information on configuring NTP using the applet (GUI), see "Configuring network time protocol (NTP)" on page 99.

BR7131>admin(system.ntp)> set

Description

Sets NTP parameters for Brocade Mobility 7131 Series Access Point clock synchronization.

Syntax

set	**mode**	<ntp-mode>	Enables or disables NTP.
	server	<idx> <ip>	Sets the NTP sever IP address.
	port	<idx> <port>	Defines the port number.
	intrvl	<period>	Defines the clock synchronization interval used between the Brocade Mobility 7131 Series Access Point and the NTP server in minutes (15 - 65535).
	time	<time>	Sets the current system time. [yyyy] - year, [mm] - month, [dd] - day of the month, [hh] - hour of the day, [mm] - minute, [ss] second, [zone -idx] Index of the zone.
	zone	<zone>	Defines the time zone (by index) for the target country.

Example

```
admin(system.ntp)>set mode enable
admin(system.ntp)>set server 1 203.21.37.18
admin(system.ntp)>set port 1 123
admin(system.ntp)>set intrvl 15
admin(system.ntp)>set zone 1
```

For information on configuring NTP using the applet (GUI), see “Configuring network time protocol (NTP)” on page 99.

System log commands

BR7131>admin(system)> logs

Description

Displays the Brocade Mobility 7131 Series Access Point 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.

BR7131>admin(system.logs)> show

Description

Displays the current Brocade Mobility 7131 Series Access Point logging settings.

Syntax

show	Displays the current access point logging configuration.

Example

```
admin(system.logs)>show

log level                          : L6 Info
syslog server logging              : enable
syslog server ip address           : 192.168.0.102
```

For information on configuring logging settings using the applet (GUI), see "Logging configuration" on page 102.

BR7131>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>	Enables or disables syslog server logging.
	ipadr	<ip>	Sets the external syslog server IP address to <ip> (a.b.c.d).

```
admin(system.logs)>set mode enable
admin(system.logs)>set level L4
admin(system.logs)>set ipadr 157.235.112.11
```

For information on configuring logging settings using the applet (GUI), see "Logging configuration" on page 102.

>admin(system.logs)> view

Description

Displays the Brocade Mobility 7131 Series Access Point system log file.

Syntax

view	Displays the entire Brocade Mobility 7131 Series Access Point system log file.

Example

```
admin(system.logs)>view

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 16:14:41 (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
    0            0
Jan  7 16:16:01 (none) CC: 0000077e  0012e95b 0000d843 00000000 00000003
0000121
e 00000000 00000000  0037ebf7 000034dc 00000000 00000000 00000000
Jan  7 16:16:13 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:16:44 (none) klogd: :ps log:fc: queue maintenance
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 102.

BR7131>admin(system.logs)> delete

Description

Deletes the log files.

Syntax

delete	Deletes the Brocade Mobility 7131 Series Access Point system log file.

Example

```
admin(system.logs)>delete
```

For information on configuring logging settings using the applet (GUI), see “Logging configuration” on page 102.

BR7131>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. Refer to the command set under the BR7131>admin(fw update) command for information on setting up an FTP server and login 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 102.

System configuration-update commands

BR7131>admin(system.config)>

Description

Displays the Brocade Mobility 7131 Series Access Point configuration update submenu.

Syntax

default	Restores the default Brocade Mobility 7131 Series Access Point configuration.
partial	Restores a partial default Brocade Mobility 7131 Series Access Point configuration.
show	Shows import/export parameters.
set	Sets import/export Brocade Mobility 7131 Series Access Point configuration parameters.
export	Exports Brocade Mobility 7131 Series Access Point configuration to a designated system.
import	Imports configuration to the access point.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the configuration to Brocade Mobility 7131 Series Access Point system flash.
quit	Quits the CLI.

BR7131>admin(system.config)> default

Description

Restores the full Brocade Mobility 7131 Series Access Point factory default configuration.

Syntax

default	Restores the Brocade Mobility 7131 Series Access Point to the original (factory) configuration.

Example

```
admin(system.config)>default

Are you sure you want to default the configuration? <yes/no>:
```

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/exporting configurations" on page 103.

BR7131>admin(system.config)> partial

Description

Restores a partial factory default configuration. The Brocade Mobility 7131 Series Access Point's LAN, WAN and SNMP settings are uneffected by the partial restore.

Syntax

default	Restores a partial access point configuration.

Example

```
admin(system.config)>partial

Are you sure you want to partially default AP-713X? <yes/no>:
```

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/exporting configurations" on page 103.

BR7131>admin(system.config)> show

Description

Displays import/export parameters for the Brocade Mobility 7131 Series Access Point configuration file.

Syntax

show	Shows all import/export parameters.

Example

```
admin(system.config)>show

cfg filename                      : cfg.txt
cfg filepath                      :
ftp/tftp server ip address        : 192.168.0.101
ftp user name                     : myadmin
ftp password                      : ********
```

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/exporting configurations" on page 103.

BR7131>admin(system.config)> set

Description

Sets the import/export parameters.

Syntax

set	**file**	<filename>	Sets the configuration file name (1 to 39 characters in length).
	path	<path>	Defines the path used for the configuration file upload.
	server	<ipaddress>	Sets the FTP/TFTP server IP address.
	user	<username>	Sets the FTP user name (1 to 39 characters in length).
	passwd	<pswd>	Sets the FTP password (1 to 39 characters in length).

Example

```
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config>set passwd georges

admin(system.config)>show

cfg filename                        : cfg.txt
cfg filepath                        :
ftp/tftp server ip address          : 192.168.22.12
ftp user name                       : myadmin
ftp password                        : *******
```

For configuration file creation and export, only the set radio-config is supported. Therefore, when configuration files for export are created, a line such as `set rf-function X wips / wlan` (where X is 1 or 2) is never be generated.

For configuration file import, the legacy command `set rf-function X wips / wlan` is processed as it has historically.

There is no CLI menu allowing the user to enter `set rf-function X wips/wlan` (where X is 1 or 2).

Instead, the command `set radio-configX` (where X is 1,2,3,4,5,6,7, or 8) is created in the configuration files for export.

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/exporting configurations" on page 103.

BR7131>admin(system.config)> export

Description

Exports the configuration from the system.

Syntax

export	**ftp**	Exports the Brocade Mobility 7131 Series Access Point configuration to the FTP server. Use the set command to set the server, user, password, and file name before using this command.
	tftp	Exports the Brocade Mobility 7131 Series Access Point configuration to the TFTP server. Use the set command to set the IP address for the TFTP server before using the command.
	terminal	Exports the Brocade Mobility 7131 Series Access Point configuration to a terminal.
	sftp	Exports the access point configuration to the SFTP server. Use the set command to set the server, user, password, and file name before using this command.

Example

Export FTP or SFTP Example:

```
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config)>set file config.txt
admin(system.config)>set passwd

admin(system.config)>export ftp/export sftp

Export operation                 : [ Started ]
Building configuration file      : [ Done ]
File transfer                    : [ In progress ]
File transfer                    : [ Done ]
Export Operation                 : [ Done ]
```

Export TFTP Example:

```
admin(system.config)>set server 192.168.0.101
admin(system.config)>set file config.txt
admin(system.config)>export tftp

Export operation                  : [ Started ]
Building configuration file       : [ Done ]
File transfer                     : [ In progress ]
File transfer                     : [ Done ]
Export Operation                  : [ Done ]
```

CAUTION

Make sure a copy of the Brocade Mobility 7131 Series Access Point's current configuration is exported (to a secure location) before exporting the access point's configuration, as you will want a valid version available in case errors are encountered with the configuration export.

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/exporting configurations" on page 103.

BR7131>admin(system.config)> import

Description

Imports the Brocade Mobility 7131 Series Access Point configuration to the access point. Errors could display as a result of invaid configuration parameters. Correct the sepcified lines and import the file again until the import operation is error free.

Syntax

import	**ftp**	Imports the Brocade Mobility 7131 Series Access Point configuration file from the FTP server. Use the set command to set the server, user, password, and file.
	tftp	Imports the Brocade Mobility 7131 Series Access Point configuration from the TFTP server. Use the set command to set the server and file.
	sftp	Imports the access point configuration from the SFTP server. Use the set command to set the server and file.

Example

Import FTP Example

```
admin(system.config>set server 192.168.22.12
admin(system.config>set user myadmin
admin(system.config)>set file config.txt
admin(system.config)>set passwd mysecret
admin(system.config)>import ftp
Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
```

Import TFTP Example

```
admin(system.config)>set server 192.168.0.101
admin(system.config)>set file config.txt
admin(system.config)>import tftp
Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
```

CAUTION

A single-radio model access point cannot import/export its configuration to a dual-radio model access point. In turn, a dual-radio model access point cannot import/export its configuration to a single-radio access point.

For information on importing/exporting access point configurations using the applet (GUI), see "Importing/exporting configurations" on page 103.

Firmware update commands

BR7131>admin(system)>fw-update

Description

Displays the firmware update submenu. The items available under this command are shown below.

NOTE
The access point must complete the reboot process to successfully update the device firmware, regardless of whether the reboot is conducted uing the GUI or CLI interfaces.

show	Displays the current Brocade Mobility 7131 Series Access Point firmware update settings.
set	Defines the Brocade Mobility 7131 Series Access Point firmware update parameters.
update	Executes the firmware update.
..	Goes to the parent menu.
/	Goes to the root menu.
save	Saves the current configuration to the Brocade Mobility 7131 Series Access Point system flash.
quit	Quits the CLI and exits the current session.

BR7131>admin(system.fw-update)>show

Description

Displays the current Brocade Mobility 7131 Series Access Point firmware update settings.

Syntax

show	Shows the current system firmware update settings for the Brocade Mobility 7131 Series Access Point.

Example

```
admin(system.fw-update)>show

automatic firmware upgrade                : enable
automatic config upgrade                  : enable

firmware filename                         : apn.bin
firmware path                             : /tftpboot/
ftp/tftp server ip address                : 168.197.2.2
ftp user name                             : jsmith
ftp password                            : *******
```

For information on updating access point device firmware using the applet (GUI), see “Updating device firmware” on page 108.

BR7131>admin(system.fw-update)>set

Description

Defines Brocade Mobility 7131 Series Access Point 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 Brocade Mobility 7131 Series Access Point and the specified firmware on the remote system.
	cfg-auto	<mode>	When enabled, updates device configuration file each time the confif file versions are found to be different between the Brocade Mobility 7131 Series Access Point and the specified LAN or WAN interface.
	file	<name>	Defines the firmware file name (1 to 39 characters).
	path	<path>	Specifies a path for the file (1 to 39 characters)..
	server	<ip>	The IP address for the FTP/TFTP server used for the firmware and/or config file update.
	user	<name>	Specifies a username for FTP server login (1 to 39 characters)..
	passwd	<password>	Specifies a password for FTP server login (1 to 39 characters).. Default is admin.

```
admin(system.fw-update)>set fw-auto enable
admin(system.fw-update)>set cfg-auto enable
admin(system.fw-update)>set file 3.0.0.0-29D
admin(system.fw-update)>set path c:/fw
admin(system.fw-update)>set server 157.235.111.22
admin(system.fw-update)>set user mudskipper
admin(system.fw-update)>set passwd muddy
```

For information on updating access point device firmware using the applet (GUI), see “Updating device firmware” on page 108.

BR7131>admin(system.fw-update)>update

Description

Executes the Brocade Mobility 7131 Series Access Point firmware update over the WAN or LAN port using either FTP or TFTP or SFTP.

Syntax

update	<mode><iface>	Defines the FTP ot TFTP mode used to conduct the firmware update. Specifies whether the update is executed over the Brocade Mobility 7131 Series Access Point's WAN, LAN1 or LAN2 interface <iface>.

NOTE
The access point must complete the reboot process to successfully update the device firmware, regardless of whether the reboot is conducted uing the GUI or CLI interfaces.

```
admin(system.fw-update)>update ftp
```

For information on updating access point device firmware using the applet (GUI), see "Updating device firmware" on page 108.

Statistics commands

BR7131>admin(stats)

Description

Displays the Brocade Mobility 7131 Series Access Point statistics submenu. The items available under this command are:

show	Displays Brocade Mobility 7131 Series Access Point WLAN, Client, LAN and WAN statistics.
send-cfg-ap	Sends a config file to another access point within the known AP table.
send-cfg-all	Sends a config file to all access points within the known AP table.
clear	Clears all statistic counters to zero.
flash-all-leds	Starts and stops the flashing of all Brocade Mobility 7131 Series Access Point LEDs.
echo	Defines the parameters for pinging a designated station.
ping	Iniates 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.

BR7131>admin(stats)> show

Description

Displays Brocade Mobility 7131 Series Access Point system information.

Syntax

show	**wan**	Displays stats for the Brocade Mobility 7131 Series Access Point WAN port.
	lan	Displays stats for the Brocade Mobility 7131 Series Access Point LAN port
	stp	Displays LAN Spanning Tree Status
	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.
	s-radio	Displays radio statistics for a single radio
	retry-hgram	Displays a radio's retry histogram statistics.
	Client	Displays all client status.
	s-Client	Displays status and statistics for an individual Client.
	auth-Client	Displays single Client Authentication statistics.
	mesh	Displays Wireless Bridge Statistics statistics summary.
	s-mesh	Displays single Wirless Bridge statistics.
	known-ap	Displays a Known AP summary.
	packets_per_legacy_rate	Displays packets for legacy rates for a defined index.
	packets_per_mcs_rate	Displays packets for mcs rates for a defined index.

For information on displaying WAN port statistics using the applet (GUI), see "Viewing WAN statistics" on page 259.

For information on displaying LAN port statistics using the applet (GUI), see "Viewing LAN statistics" on page 263.

For information on displaying Wireless statistics using the applet (GUI), see "Viewing a LAN's IP filter statistics" on page 267.

For information on displaying individual WLAN statistics using the applet (GUI), see "Viewing WLAN statistics" on page 270.

For information on displaying Radio statistics using the applet (GUI), see "Viewing radio statistics summary" on page 275.

For information on displaying Client statistics using the applet (GUI), see "Viewing client statistics summary" on page 280.

For information on displaying Mesh statistics using the applet (GUI), see "Viewing the mesh statistics summary" on page 284.

For information on displaying Known AP statistics using the applet (GUI), see “Viewing known access point statistics” on page 286.

BR7131>admin(stats)> send-cfg-ap

Description

Copies the Brocade Mobility 7131 Series Access Point's configuration to another Brocade Mobility 7131 Series Access Point within the known AP table.

Syntax

send-cfg-ap	<index>	Copies the Brocade Mobility 7131 Series Access Point's configuration to the Brocade Mobility 7131 Series Access Points within the known AP table. Mesh configuration attributes do not get copied using this command and must be configured manually.

Example

```
admin(stats)>send-cfg-ap 2
admin(stats)>
```

NOTE
The send-cfg-ap command copies all existing configuration parameters except Mesh settings, LAN IP data, WAN IP data and DHCP Server parameter information.

For information on copying the access point config to another access point using the applet (GUI), see "Viewing known access point statistics" on page 286.

BR7131>admin(stats)> send-cfg-all

Description

Copies the Brocade Mobility 7131 Series Access Point's configuration to all of the Brocade Mobility 7131 Series Access Points within the known AP table.

Syntax

send-cfg-all	Copies the Brocade Mobility 7131 Series Access Point's configuration to all of the Brocade Mobility 7131 Series Access Points within the known AP table.

Example

```
admin(stats)>send-cfg-all
admin(stats)>
```

NOTE
The send-cfg-all command copies all existing configuration parameters except Mesh settings, LAN IP data, WAN IP data and DHCP Server parameter information.

For information on copying the access point config to another access point using the applet (GUI), see "Viewing known access point statistics" on page 286.

BR7131>admin(stats)> clear

Description

Clears the specified statistics counters to zero to begin new data calculations.

Syntax

clear	**wan**	Clears WAN statistics counters.
	lan	Clears LAN statistics counters for specified LAN index (either clear lan 1 or clear lan 2).
	all-rf	Clears all RF data.
	all-wlan	Clears all WLAN summary information.
	wlan	Clears individual WLAN statistic counters.
	all-radio	Clears Brocade Mobility 7131 Series Access Point radio summary information.
	radio1	Clears statistics counters specific to radio1.
	radio2	Clears statistics counters specific to radio2.
	all-Client	Clears all Client statistic counters.
	Client	Clears Client statistics counters.
	known-ap	Clears Known AP statistic counters.

BR7131>admin(stats)> flash-all-leds

Description

Starts and stops the illumination of a specified access point's LEDs.

Syntax

flash-all-leds	<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 access point LEDs using the applet (GUI), see "Viewing known access point statistics" on page 286.

BR7131>admin(stats)> echo

Description

Defines the echo test values used to conduct a ping test to an associated Client.

Syntax

show	Shows the Client Statistics Summary.
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.

BR7131>admin(stats.echo)> show

Description

Shows Client Statistics Summary.

Syntax

show	Shows Client Statistics Summary.

Example

```
admin(stats.echo)>show

--------------------------------------------------------------------------------
Idx    IP Address    MAC
Address      WLAN    Radio    T-put    ABS    Retries
--------------------------------------------------------------------------------
1      192.168.2.0   00:A0F8:72:57:83 demo    11a
```

BR7131>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

admin(stats.echo)>
```

BR7131>admin(stats.echo)>set

Description

Defines the parameters of the echo test.

Syntax

set	**station**	<mac>	Defines Client target MAC address.
	request	<num>	Sets number of echo packets to transmit (1-539).
	length	<num>	Determines echo packet length in bytes (1-539).
	data	<hex>	Defines the particular packet data.

BR7131>admin(stats.echo)> start

Description

Initiates the echo test.

Syntax

start	Initiates the echo test.

Example

```
admin(stats.echo)>start

admin(stats.echo)>list

Station Address             : 00A0F843AABB
Number of Pings             : 10
Packet Length               : 100
Packet Data (in HEX)        : 1

Number of Client Responses      : 2
```

BR7131>admin(stats)> ping

Description

Defines the ping test values used to conduct a ping test to an AP with the same ESSID.

Syntax

ping	**show**	Shows Known AP Summary details.
	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.

BR7131>admin(stats.ping)> show

Description

Shows Known AP Summary Details.

Syntax

show	Shows Known AP Summary Details.

Example

```
admin(stats.ping)>show
-------------------------------------------------------------------------------
Idx    IP Address    MAC Address        clients      KBIOS      Unit Name
-------------------------------------------------------------------------------
1      192.168.2.0   00:A0F8:72:57:83   3        0          access point
```

BR7131>admin(stats.ping)> list

Description

Lists ping test parameters and results.

Syntax

list	Lists ping test parameters and results.

Example

```
admin(stats.ping)>list

Station Address             : 00A0F8213434
Number of Pings             : 10
Packet Length               : 10
Packet Data (in HEX)        : 55

admin(stats.ping)>
```

BR7131>admin(stats.ping)> set

Description

Defines the parameters of the ping test.

Syntax

set	**station**	Defines the AP target MAC address.
	request	Sets number of ping packets to transmit (1-539).
	length	Determines ping packet length in bytes (1-539).
	data	Defines the particular packet data.

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

admin(stats.ping)>
```

BR7131>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
```

Chapter

Configuring Mesh Networking 9

In this chapter

- Mesh networking overview 583
- Configuring mesh networking support 587
- Mesh network deployment - quick setup 597
- Mesh networking frequently asked questions 610

Mesh networking overview

A Brocade Mobility 7131 Series Access Point can be configured in two modes to support the new mesh networking functionality. The access point can be set to a client bridge mode and/or a base bridge mode (which accepts connections from client bridges). Base bridge and client bridge mode can be used at the same time by an individual access point to optimally bridge traffic to other members of the mesh network and service associated clients.

An access point in client bridge mode scans to locate other access points using the WLAP client's ESSID. Then it is required to go through the association and authentication process to establish wireless connections with the located devices. This association process is identical to the access point's current Client association process. Once the association and authentication process is complete, the wireless client adds the connection as a port on its bridge module. This causes the client bridge to begin forwarding packets to the base bridge node. The base bridge realizes it is talking to a wireless client bridge. It then adds that connection as a port on its own bridge module. The two bridges at that point are communicating using the *Spanning Tree Protocol* (STP).

access points configured as both a base and a client bridge function as *repeaters* to transmit data with associated clients in their coverage area (client bridge mode) as well as forward traffic to other access points in the mesh network (base bridge mode). The number of access points and their intended function within the mesh network dictate whether they should be configured as base bridges, client bridges or both (repeaters).

The spanning tree determines the path to the root and detects if the current connection is part of a network loop with another connection in the system. Each bridge can be configurable so the administrator can control the spanning tree to define the root bridge and what the forwarding paths are. Once the spanning tree converges, both access points begin learning which destinations reside on which side of the network. This allows them to forward traffic intelligently.

After the client bridge establishes at least one wireless connection (if configured to support mobile users), it begins beaconing and accepting wireless connections. If configured as both a client bridge and a base bridge, it begin accepting client bridge connections. Therefore, the mesh network could connect simultaneously to different networks in a manner whereby a network loop is not created and then the connection is not blocked. Once the client bridge establishes at least one wireless connection, it begins establishing other wireless connections as it finds them available. Thus, the client bridge is able to establish simultaneous redundant links.

A mesh network must use one of the two access point LANs. If intending to use the access point for mesh networking support, Brocade recommends configuring at least one WLAN (of the 16 WLANs available) specifically for mesh networking support.

The client bridge creates up to three connections if it can find base bridges for connection. If the connections are redundant (on the same network), then one connection will be forwarding and the others blocked. However, if each of the connections links to a different wired network, then none are redundant and all are forwarding. Thus, the bridge automatically detects and disables redundant connections, but leaves non-redundant connections forwarding. This gives the user the freedom to configure their topology in a variety of ways without limitations. This is important when configuring multiple access points for base bridge support in areas like a shipping yard where a large radio coverage area is required. For more information on configuring the access point in respect to specific usage scenarios, see “Mesh network deployment - quick setup” on page 597.

NOTE
Since each access point can establish up to 3 simultaneous wireless connections, some of these connections could be redundant. If this is the case, the STP algorithm defines which links are the redundant links and disables those links from forwarding.

If an access point is configured as a base bridge (but not as a client bridge) it operates normally at boot time. The base bridge supports connections made by other client bridges.

The dual-radio model access point affords users better optimization of the mesh networking feature by enabling the access point to transmit to other mesh network members using one independent radio and transmit with associated clients using the second independent radio. A single-radio access point has its channel utilization and throughput degraded in a mesh network, as the AP’s single radio must process both mesh network traffic with other access points and Client traffic with its associated devices.

CAUTION

Only Brocade Brocade Mobility 7131 Series Access Points or Mobility 5181 model access points can be used as base bridges, client bridges or repeaters within an access point supported mesh network. If utilizing a mesh network, Brocade recommends considering a dual-radio model to optimize channel utilization and throughput.

The Brocade Mobility 7131 Series Access Point client bridge association process

An access point in client bridge mode performs an active scan to quickly create a table of the access points nearby. The table contains the access points matching the ESS of the client bridge AP’s WLAN. The table is used to determine the best access point to connect to (based on signal strength, load and the user's configured preferred connection list).

The association and authentication process is identical to the Client association process. The client access point sends 802.11 authentication and association frames to the base access point. The base access point responds as if the client is an actual client. Depending on the security policy, the two access point’s engage in the normal handshake mechanism to establish keys.

After device association, the two access points are connected and the system can establish the bridge and run the spanning tree algorithm. In the meantime, the access point in client bridge mode continues to scan in the background attempts to establish an association with other access points using the same ESS on the same channel.

CAUTION

An access point is Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the access point's WAN connection. If this situation is experienced, log-in to the access point again.

The access point in client bridge mode attempts to establish up to 3 simultaneous wireless connections. The second and third connections are established in the background while the system is running. The first connection needs to be established before the system starts bridging traffic.

The dual-radio model access point affords users better optimization of the mesh networking feature by allowing the access point to transmit to other access points (in base or client bridge mode) using one independent radio and transmit with its associated clients using the second independent radio. A single-radio access point has its channel utilization and throughput degraded in a mesh network, as the access point's single radio must process both mesh network traffic with other access points and Client traffic with its associated devices.

Client bridge configuration process example

In this example, two access points are described with the following configurations:

- AP #1 base bridge
- AP #2 repeater (both a base and client bridge)

In the case of a mesh enabled radio, the client bridge configuration always takes precedence over the base bridge configuration. Therefore, when a radio is configured as a repeater (AP #2), the base bridge configuration takes effect only after the client bridge connection to AP #1 is established. Thus, AP #2 keeps scanning to find the base bridge, form the uplink and start beaconing as a base bridge for downstream client bridge connection. This is by design, as there is no reason to use a partially broken connection with no uplink to a base bridge.

Spanning tree protocol (STP)

The access point performs mesh networking using STP as defined in the 802.1d standard.

Once device association is complete, the client and base bridge exchange *Configuration Bridge Protocol Data Units* (BPDUs) to determine the path to the root. STP also determines whether a given port is a redundant connection or not.

Defining the mesh topology

When a user wants to control how the spanning tree determines client bridge connections, they need to control the mesh configuration. The user must be able to define one node as the root. Assigning a base bridge the lowest bridge priority defines it as the root.

NOTE
Brocade recommends using the *Mesh STP Configuration* screen to define a base bridge as a root. Only advanced users should use the Advanced Client Bridge Settings screen's Preferred List to define the mesh topology, as omitting a bridge from the preferred list could break connections within the mesh network.

The access point can manipulate the path cost assigned to a bridge connection based on that connection's RSSI. This results in the spanning tree selecting the optimal path for forwarding data when redundant paths exist. However, this can be overridden using the preferred list. When using the preferred list, the user enters a priority for each bridge, resulting in the selection of the forwarding link.

Limit the wireless client's connections to reduce the number of hops required to get to the wired network. Use each radio's "preferred" base bridge list to define which access points the client bridge connects to. For more information, see "Configuring mesh networking support" on page 587.

Mesh networking and the Brocade Mobility 7131 Series Access Point's two subnets

The access point now has a second subnet on the LAN side of the system. This means wireless clients communicating through the same radio can reside on different subnets. The addition of this feature adds another layer of complexity to the access point's mesh networking functionality.

With a second LAN introduced, the LAN's Ethernet port (and any of the 16 WLANs) could be assigned to one of two different subnets. From a layer 2 perspective, the system has two different bridge functionalities, each with its own STP. The WLAN assignment controls the subnet (LAN1 or 2) upon which a given connection resides. If WLAN2 is assigned to LAN1, and WLAN2 is used to establish a client bridge connection, then the mesh network connection resides on LAN1.

Therefore, (depending upon the WLAN-to-LAN mapping), the access point could have multiple mesh connections on either LAN1 or LAN2.

Normal operation

Once the mesh network is defined, all normal access point operations are still allowed. Clients are still allowed to associate with the access point as usual. The user can create WLANs, security polices and VLANs as with any other access point. DHCP services function normally and all layer 3 communications are allowed.

WNMP is used to send information about each mesh network so information can be displayed to the user from any access point on the system. WNMP messages are AP-AP info messages used to send system status.

Impact of importing/exporting configurations to a mesh network

When using the access point's Configuration Import/Export screen to migrate an access point's configuration to other access points, mesh network configuration parameters will get sent or saved to other access points. However, if using the Known AP Statistics screen's Send Cfg to APs functionality, "auto-select" and preferred list" settings do not get imported.

CAUTION

When using the Import/Export screen to import a mesh supported configuration, do not import a base bridge configuration into an existing client bridge, as this could cause the mesh configuration to break.

Configuring mesh networking support

Configuring the access point for Mesh Bridging support entails:

- *Setting the LAN configuration for mesh networking support*
- *Configuring a WLAN for mesh networking support*
- *Configuring the access point radio for mesh support*.

Setting the LAN configuration for mesh networking support

At least one of the two access point LANs needs to be enabled and have a mesh configuration defined to correctly function as a base or client bridge within a mesh network. This section describes the configuration activities required to define a mesh network's LAN configuration.

As the *Spanning Tree Protocol* (STP) mentions, each mesh network maintains hello, forward delay and max age timers. The base bridge defined as the root imposes these settings within the mesh network. The user does not necessarily have to change these settings, as the default settings will work. However, Brocade encourages the user to define an access point as a base bridge and root (using the base bridge priority settings within the Bridge STP Configuration screen). Members of the mesh network can be configured as client bridges or additional base bridges with a higher priority value.

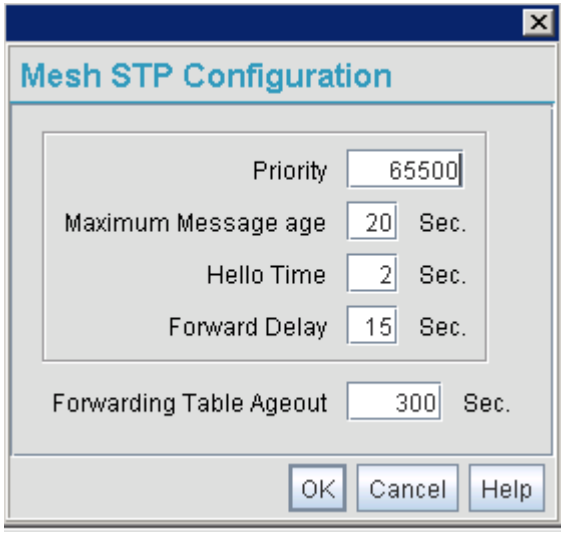
NOTE

For an overview on mesh networking and some of the implications on using the feature with the access point, see "Configuring Mesh Networking" on page 583.

To define a LAN's Mesh STP Configuration:

1. Select *Network Configuration -> LAN* from the Brocade Mobility 7131 Series Access Point menu tree.
2. Enable the LAN used to support the mesh network.

   Verify the enabled LAN is named appropriately in respect to its intended function in supporting the mesh network.
3. Select *Network Configuration -> LAN -> LAN1 or LAN2* from the Brocade Mobility 7131 Series Access Point menu tree.
4. Click the *Mesh STP Configuration* button on the bottom off the screen.
5. Define the properties for the following parameters within the mesh network:



CAUTION

If you have imported a Server or CA certificate, the certificate will not be saved when updating the access point's firmware. Export your certificates before upgrading the access point's firmware. From the access point CLI, use the *admin(system.cmgr)> expcert* command to export the certificate to a secure location.

6. Click *OK* to return to either the LAN1 or LAN2 screen where updates to the Mesh STP Configuration can be saved by clicking the *Apply* button.
7. Click *Cancel* to discard the changes made to the Mesh STP Configuration and return to the LAN1 or LAN2 screen. Once the Mesh STP Configuration is defined, the access point's radio can be configured for base and/or client bridge support.

Configuring a WLAN for mesh networking support

Each access point comprising a particular mesh network is required to be a member of the same WLAN. Therefore, each base bridge, client bridge or repeater within the mesh network must use the same WLAN in order to share the same ESSID, radio designation, security policy, Client ACL and Quality of Service policy. If intending to use the access point for mesh networking support, Brocade recommends configuring at least one WLAN (of the 16 WLANs available) specifically for mesh networking support.

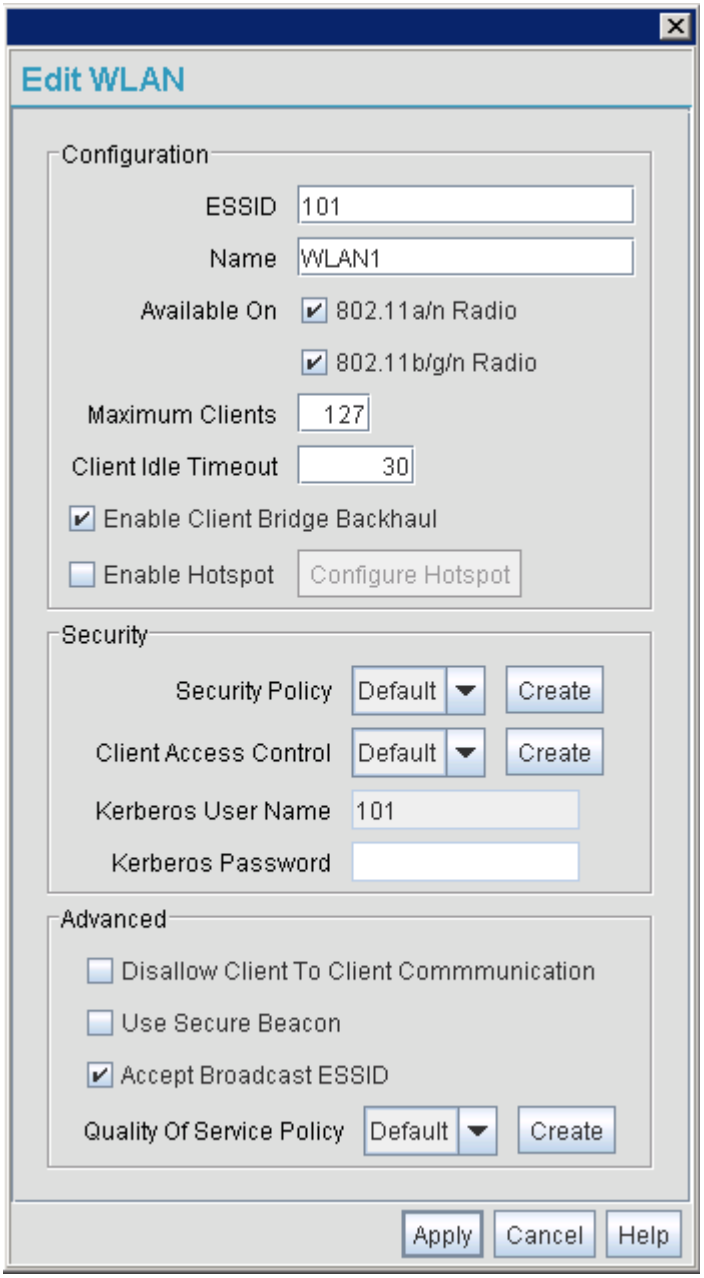
To define the attributes of the WLAN shared by the members of the mesh network:

1. Select *Network Configuration -> Wireless* from the Brocade Mobility 7131 Series Access Point menu tree.

   The *Wireless Configuration* screen displays with those existing WLANs displayed within the table.

2. Select the *Create* button to configure a new WLAN specifically to support mesh networking.

   An existing WLAN can be modified (or used as is) for mesh networking support by selecting it from the list of available WLANs and clicking the *Edit* button.



3. Assign an *ESSID* and *Name* to the WLAN that each access point will share when using this WLAN within their mesh network.

   Brocade recommends assigning a unique name to a WLAN supporting a mesh network to differentiate it from WLANs defined for non mesh support. The name assigned to the WLAN is what is selected from the *Radio Configuration* screen for use within the mesh network.

NOTE
It is possible to have different ESSID and WLAN assignments within a single mesh network (one set between the Base Bridge and repeater and another between the repeater and Client Bridge). However, for ease of management and to not waste network bandwidth, Brocade recommends using the same ESSID across the entire mesh network.

4. Use the *Available On* checkboxes to specify the access point radio(s) used with the target WLAN within the mesh network.

   The Available On checkboxes are for making this WLAN available for base bridges or repeaters to connect to. The Available On checkbox should only be selected for a mesh WLAN if this target access point is to be configured as a base bridge or repeater on the radio. If the WLAN is to be defined for client bridge support only, the Available On checkbox should not be selected. Instead, it only needs to have the Enable Client Bridge Backhaul option selected.

5. Use the *Maximum clients* field to define the number of clients allowed to associate with this WLAN. This number should be defined based on the number of client bridge and repeaters within this mesh network. This value can be increased as the mesh network grows and devices are added.

   Only advanced users should define the number of devices allowed to associate with the WLAN, as setting the value too low could restrict devices from joining an expanding mesh network, and setting it too high could prohibit other WLANs from granting access to the all the devices needed.

6. Select the *Enable Client Bridge Backhaul* checkbox to make this WLAN available in the *Mesh Network Name* drop-down menu within the *Radio Configuration* screen. Only WLANs defined for mesh networking support should have this checkbox selected, in order to keep the list of WLANs available (within the Radio Configuration screen) restricted to just WLANs configured specifically with mesh attributes.

7. Refer to the *Security Policy* drop-down menu to select the security policy used within this WLAN and mesh network.

   A security policy for a mesh network should be configured carefully since the data protection requirements within a mesh network differ somewhat compared to a typical wireless LAN. *No Encryption* is a bad idea in a mesh network, since mesh networks are typically not guest networks, wherein public assess is more important than data protection. Brocade also discourages user-based authentication schemes such as Kerberos and 802.1x EAP, as these authentication schemes are not supported within a mesh network.

   If none of the existing policies are suitable, select the *Create* button to the right of the *Security Policy* drop-down menu and configure a policy suitable for the mesh network. For information on configuring a security using the authentication and encryption techniques available to the access point, see “Enabling authentication and encryption schemes” on page 194.

8. ACL policies should be configured to allow or deny a range of MAC addresses from interoperating with the WLAN used with the mesh network. ACLs should be defined based on the client bridge and repeater (an access point defined as both a base and client bridge) association requirements within the mesh network.

   For information on defining an ACL for use with the WLAN assigned to the mesh network, see “Configuring a WLAN Access Control List (ACL)” on page 144.

NOTE
The *Kerberos User Name* and *Kerberos Password* fields can be ignored, as Kerberos is not supported as a viable authentication scheme within a mesh network.

9. Select the *Disallow Client to Client Communication* checkbox to restrict clients from interacting with each other both within this WLAN, as well as other WLANs.

   Selecting this option could be a good idea, if restricting device “chatter” improves mesh network performance. If base bridges and client bridges are added at any given time to extent the coverage are of a mesh network, the data going back and forth amongst just those radios could be compromised by network interference. Adding mesh device traffic could jeopardize network throughput. If however, Client to Client communication is central to the organization (for example, scanners sharing data entry information) then this checkbox should remain unselected.

10. Select the *Use Secure Beacon* checkbox to not transmit the ESSID amongst the access points and devices within the mesh network. If a hacker tries to find an ESSID via an Client, the access point’s ESSID does not display since the ESSID is not in the beacon. Brocade recommends keeping the option enabled to reduce the likelihood of hacking into the WLAN.

11. Select the *Accept Broadcast ESSID* checkbox to associate an Client that has a blank ESSID (regardless of which ESSID the access point is currently using). Traffic within a mesh network probably consists of known devices, so you may want to leave the checkbox unselected and configure each Client with an ESSID. The default is selected. However, for WLANs used within a mesh network, Brocade recommends unselecting this option as it would prevent the AP from answering to blank ESSID probes from other wireless clients.

12. If there are certain requirements for the types of data proliferating the mesh network, select an existing policy or configure a new QoS policy best suiting the requirements of the mesh network. To define a new QoS policy, select the *Create* button to the right of the Quality Of Service Policy drop-down menu.

    For detailed information on configuring a QoS policy, see “Setting the WLAN Quality of Service (QoS) policy” on page 147.

13. Click *Apply* to save the changes made to the mesh network configured WLAN.

    An access point radio is now ready to be configured for use with this newly created mesh WLAN.

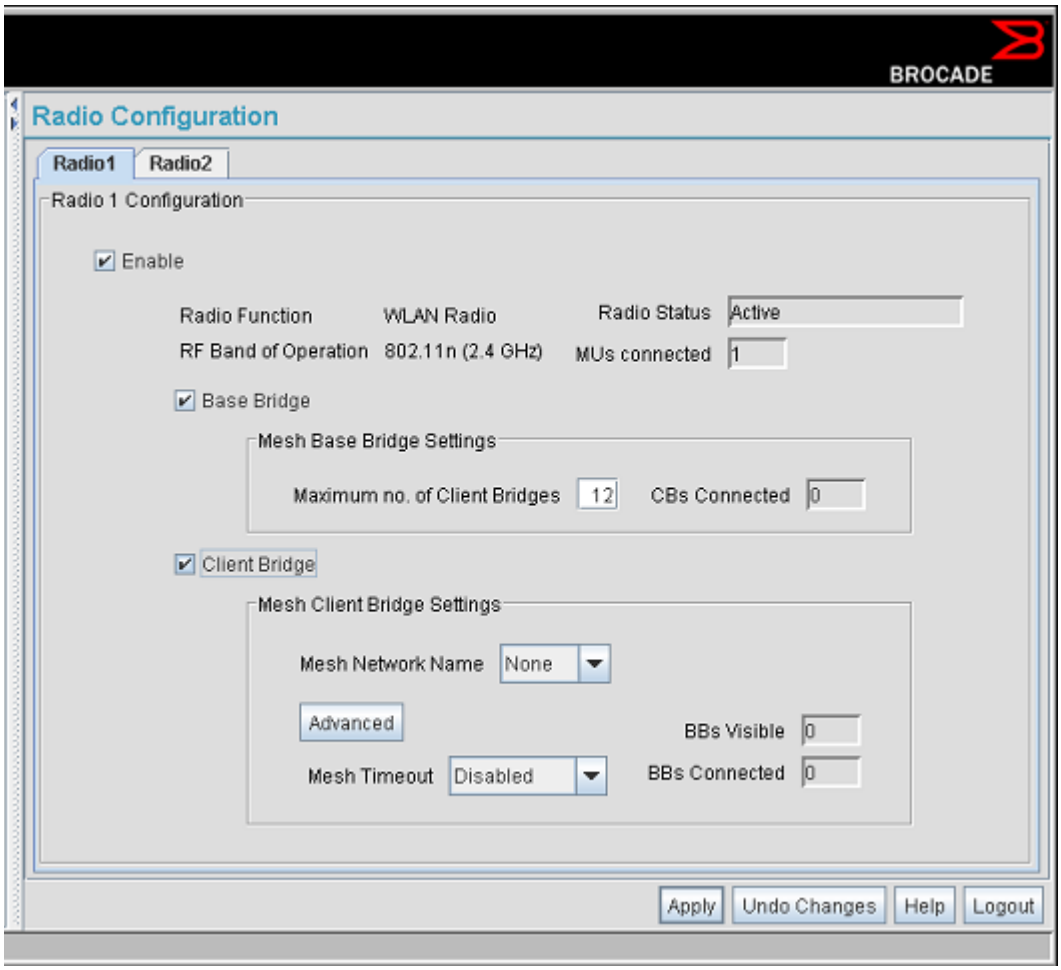
Configuring the access point radio for mesh support

An access point radio intended for use within a mesh network requires configuration attributes unique from a radio intended for non-mesh support.This section describes how to configure an access point radio for mesh network support.

To configure the access point radio for mesh networking support:

NOTE
The dual-radio model access point affords users better optimization of the mesh network feature by allowing the access point to transmit to other access points (in base or client bridge mode) using one independent radio and transmit with its associated devices using the second independent radio. A single-radio access point has its channel utilization and throughput degraded in a mesh network, as the AP’s single radio must process both mesh network traffic with other access points and Client traffic with its associated devices.

1. Select *Network Configuration -> Wireless -> Radio Configuration* from the Brocade Mobility 7131 Series Access Point menu tree.



2. Enable the radio(s) using the *Enable* checkbox(es) for both Radio 1 and Radio 2.

   Refer to *RF Band of Operation* parameter to ensure you are enabling the correct 802.11a/n or 802.11b/g/n radio. After the settings are applied within this Radio Configuration screen, the *Radio Status* and *clients connected* values update. If this is an existing radio within a mesh network, these values update in real-time.

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. Select the *Base Bridge* checkbox to allow the access point radio to accept client bridge connections from other access points in client bridge mode. The base bridge is the acceptor of mesh network data from those client bridges within the mesh network and never the initiator.

CAUTION

A problem could arise if a Base Bridge's Indoor channel is not available on an Outdoor Client Bridge's list of available channels. As long as an Outdoor Client Bridge has the Indoor Base Bridge channel in its available list of channels, it can associate to the Base Bridge.

4. If the Base Bridge checkbox has been selected, use the *Max# Client Bridge*s parameter to define the client bridge load on a particular base bridge.

   The maximum number of client bridge connections per access point radio is 12, with 24 representing the maximum for dual-radio models.

CAUTION

An access point in Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the access point's WAN connection. If this situation is experienced, log-in to the access point again.

   Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of client bridge connections for this specific radio displays within the *CBs Connected* field. If this is an existing radio within a mesh network, this value updates in real-time.

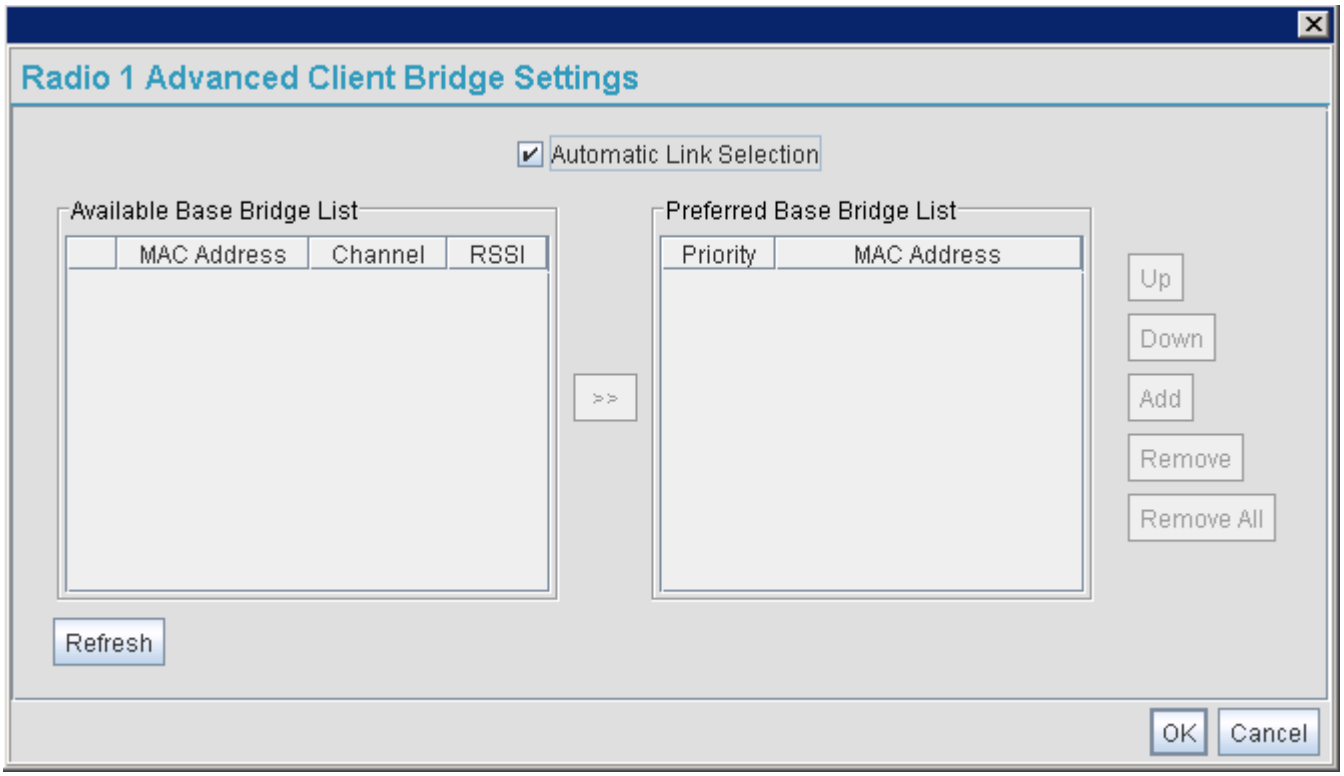
5. Select the *Client Bridge* checkbox to enable the access point radio to initiate client bridge connections with other mesh network supported access points radios on the same WLAN.

   If the Client Bridge checkbox has been selected, use the *Mesh Network Name* drop-down menu to select the WLAN (ESS) the client bridge uses to establish a wireless link. The default setting, is (WLAN1). Brocade recommends creating (and naming) a WLAN specifically for mesh networking support to differentiate the Mesh supported WLAN from non-Mesh supported WLANs. For more information, see *"Configuring a WLAN for mesh networking support"* on page 588

   Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of base bridges visible to the radio displays within the *BBs Visible* field, and the number of base bridges currently connected to the radio displays within the *BBs Connected* field. If this is an existing radio within a mesh network, these values update in real-time.

NOTE
Ensure you have verified the radio configuration for both Radio 1 and Radio 2 before saving the existing settings and exiting the Radio Configuration screen.v

6. Click the *Advanced* button to define a prioritized list of access points to define mesh connection links.



7. Select the *Automatic Link Selection* checkbox to allow the access point to select the links used by the client bridge to populate the mesh network. Selecting this checkbox prohibits the user from selecting the order base bridges are added to the mesh network when one of the three associated base bridges becomes unavailable.

NOTE
Auto link selection is based on the RSSI and load. The client bridge will select the best available link when the *Automatic Link Selection* checkbox is selected. Brocade recommends you do not disable this option, as (when enabled) the access point will select the best base bridge for connection.

8. Refer to the *Available Base Bridge List* to view devices located by the access point using the WLAN selected from the Radio Configuration screen. Refer the following for information on located base bridges:

MAC	The MAC field displays the factory set hard-coded MAC address that serves as a device identifier.
RSSI	The *Relative Signal Strength Indicator* (RSSI) displays the located device's signal strength with the associated access point in client bridge mode. Use this information as criteria on whether to move a particular device from the available list to the preferred list.

CHANN	The CHANN displays the name of the channel that both the access point and base bridge use. A client bridge can only connect to access points (Base Bridges) on the same channel. If the user selects multiple base bridges on different channels, the access point will only be able to connect to those bridges on the same channel and the others will not be able to join this particular mesh network.

9. Click *Refresh* at any time to update the list of available Base Bridge devices available to the access point.
10. Use the >> button to move a selected base bridge MAC address from Available Base Bridge List
11. Refer to the *Preferred Base Bridge List* for a prioritized list of base bridges the mesh network's client bridge uses to extend the mesh network's coverage area and potentially provide redundant links. If a device does not appear on the Available Base Bridge List, there is no" way it can be moved to Preferred Base Bridge List as the device has not yet been "seen." However, if you know the MAC Address corresponding to that Base Bridge, you can add that to the Preferred List using the add button.
12. Highlight a MAC address from the Preferred Base Bridge List and click the *Up* button to assign that device's MAC address a higher priority and a greater likelihood of joining the mesh network if an association with another device is lost.

    If a MAC address is not desirable as others but still worthy of being on the preferred list, select it, and click the *Down* button to decrease its likelihood of being selected as a member of the mesh network.
13. If a device MAC address is on the Preferred Base Bridge List and constitutes a threat as a potential member of the mesh network (poor RSSI etc.), select it and click the *Remove* button to exclude it from the preferred list.

    If all of the members of the Preferred Base Bridge List constitute a risk as a member of the mesh network, click the *Remove All* button. This is not recommended unless the preferred list can be re-populated with more desirable device MAC addresses from the Available Base Bridge List.
14. Click *Ok* to return to the Radio Configuration screen. Within the Radio Configuration screen, click *Apply* to save any changes made within the Advanced Client Bridge Settings screen.
15. Click *Cancel* to undo any changes made within the Advanced Client Bridge Settings screen. This reverts all settings for the screen to the last saved configuration.
16. If using a dual-radio model access point, refer to the *Mesh Timeout* drop-down menu (from within the Radio Configuration screen) to define whether one of the access point's radio's beacons on an existing WLAN or if a client bridge radio uses an uplink connection. The Mesh Timeout value is not available on a single-radio access point, since the radio would have to stop beaconing and go into scan mode to determine if a base bridge uplink is lost. The following drop-down menu options are available:

Disabled	When disabled, both radios are up at boot time and beaconing. If one radio (radio 1) does not have a mesh connection, the other radio (radio 2) is not affected. Radio 2 continues to beacon and associate clients, but Client's can only communicate amongst themselves using the access point. Disabled is the default value.
Upload Detect	When Uplink Detect is selected, the access point only boots up the radio configured as a client bridge. The access point boots up the second radio as soon as the first mesh connection is established. However, if the client bridge radio loses its uplink connection, the second radio shuts down immediately.
Enabled	If the mesh connection is down on one radio (radio 1), the other radio (radio 2) is brought down and stops beaconing after the timeout period (45 seconds). This allows the client bridge (radio 1) to roam without dropping the Client's associated to radio 2. The disadvantage is that radio 2 may beacon for the 45 second timeout period and have to drop associated Client's because radio 1 could not establish its uplink.

NOTE
The Mesh Time Out variable overrides the *Ethernet Port Time Out* (EPTO) setting on the LAN page when the access point is in bridge mode. As long as the mesh is down, the access point acts in accordance to the Mesh Time Out setting regardless of the state of the Ethernet. However, if the Ethernet goes down and the mesh link is still up, the EPTO takes effect.

17. 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.

CAUTION

When defining a Mesh configuration and changes are saved, the mesh network temporarily goes down. The mesh network is unavailable because the access point radio goes down when applying the changes. This can be problematic for users making changes within a deployed mesh network. If updating the mesh network using a LAN connection, the access point applet loses connection and the connection must be re-instated. If updating the mesh network using a WAN connection, the applet does not lose connection, but the mesh network is unavailable until the changes have been applied.

18. 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.
19. Click *Logout* to securely exit the 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 Brocade Mobility 7131 Series Access Point menu tree.

For additional information on configuring the access point's radio, see "Configuring the 802.11a/n or 802.11b/g/n radio" on page 167. For two fictional deployment scenarios, see "Mesh network deployment - quick setup" on page 597.

Mesh network deployment - quick setup

This section provides instructions on how to quickly setup and demonstrate mesh functionality using three access points. Two following two deployment scenarios will be addressed:

- *Scenario 1* - Two base bridges (redundant) and one client bridge
- *Scenario 2* - A two hop mesh network with a base bridge, repeater (combined base bridge and client bridge mode) and a client bridge.

Scenario 1 - two base bridges and one client bridge

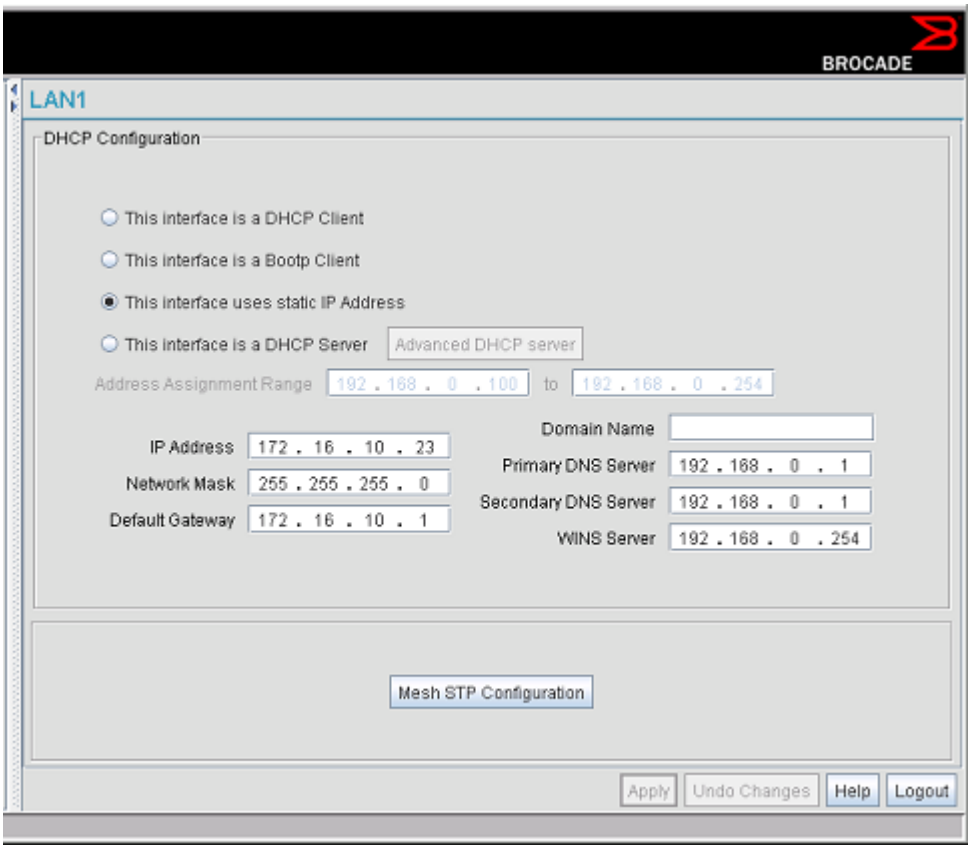
In scenario 1, the following three access point configurations will be deployed within the mesh network:

- AP#1 - An active base bridge
- AP#2 - A redundant base bridge
- AP#3 - A client bridge connecting to both AP#1 and AP#2 simultaneously.

AP#1 and AP#2 will be configured somewhat the same. However there are some important (yet subtle) differences. Therefore, the configuration of each access point will be described separately.

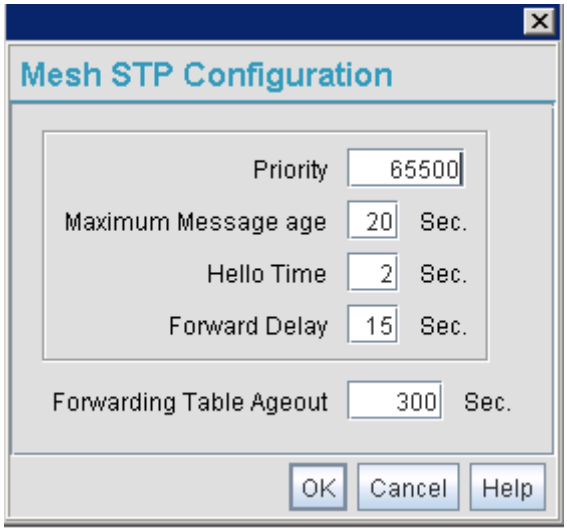
Configuring AP#1

1. Provide a known IP address for the LAN1 interface.

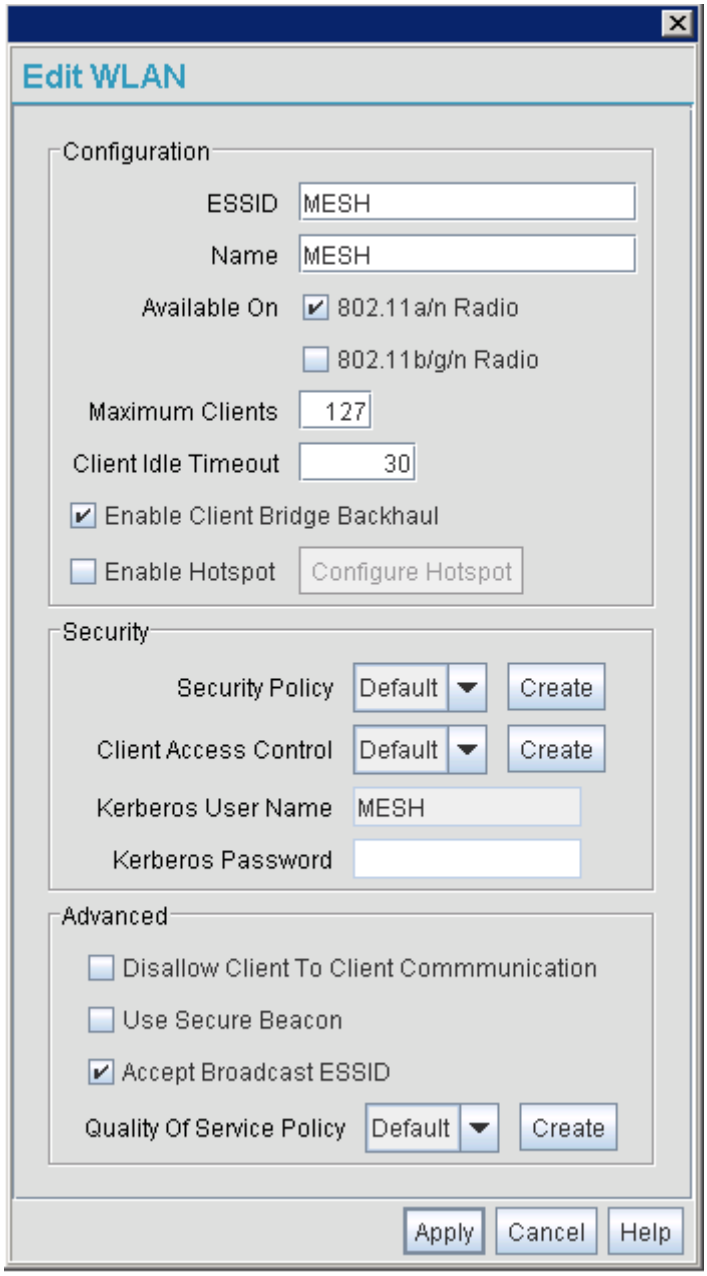


NOTE
Enable the LAN1 Interface of AP#1 as a DHCP Server if you intend to associate clients and require them to obtain an IP address via DHCP.

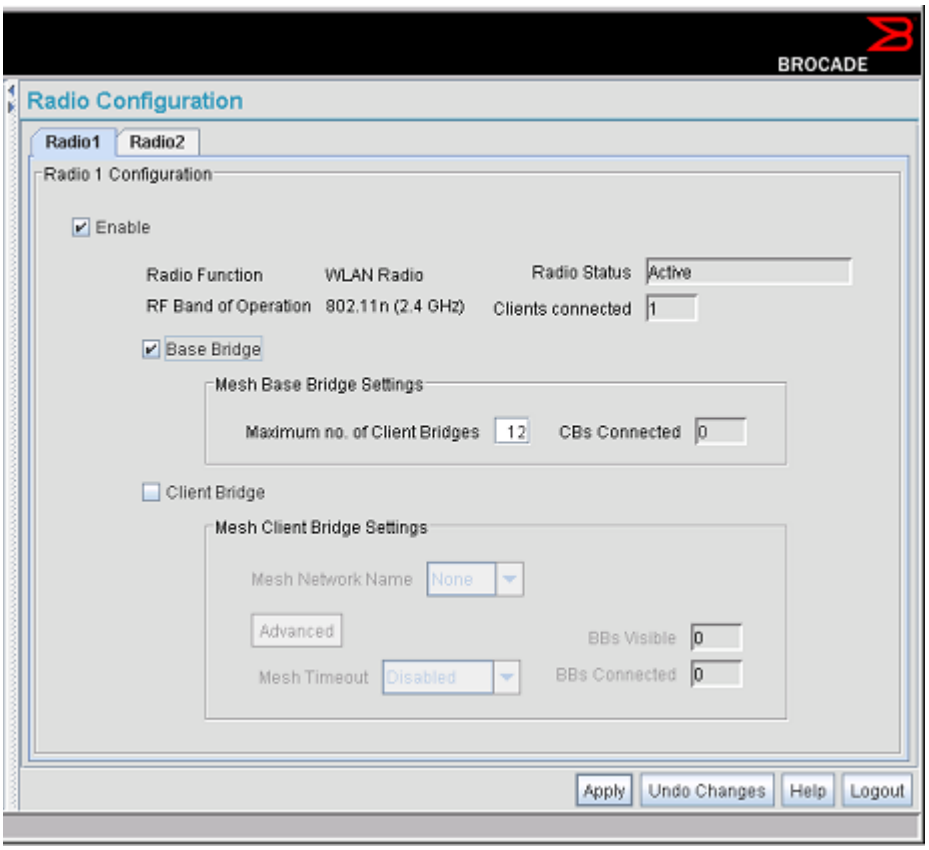
2. Assign a Mesh STP Priority of 40000 to LAN1 Interface.



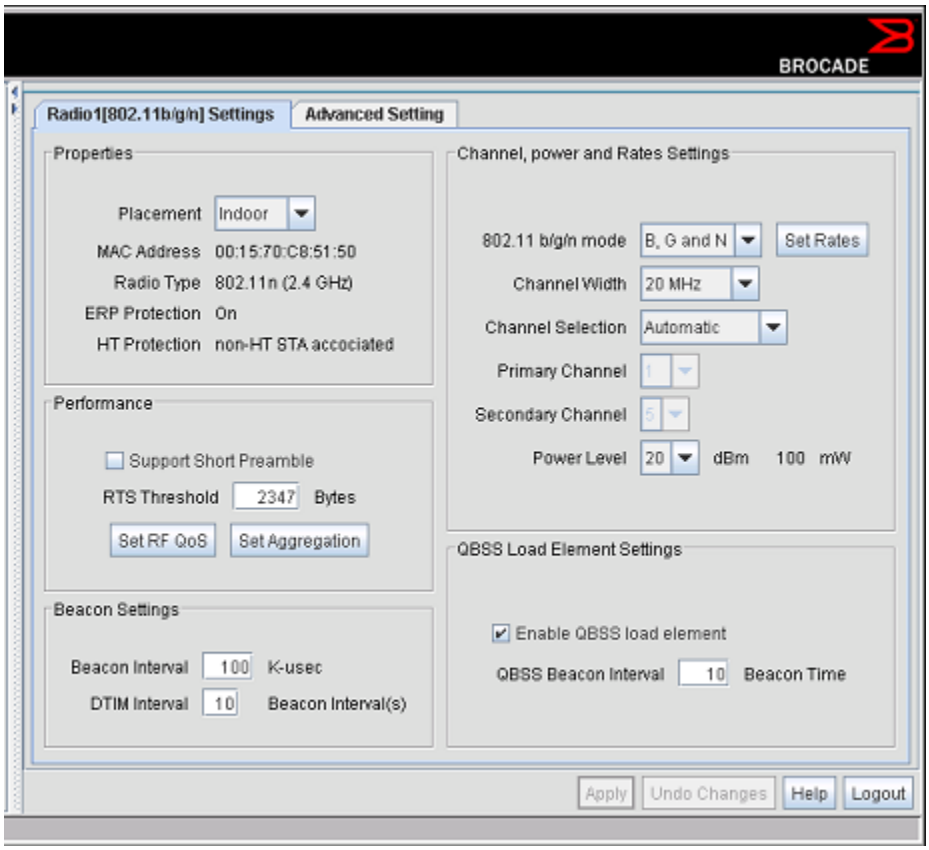
3. Define a mesh supported WLAN.



4. Enable base bridge functionality on the 802.11a/n radio (Radio 2).



5. Define a channel of operation for the 802.11a/n radio.



6. If needed, create another WLAN mapped to the 802.11b/g/n radio if 802.11b/g/n support is required for clients on that 802.11 band.

Configuring AP#2

AP#2 can be configured the same as AP#1 with the following exceptions:

- Assign an IP Address to the LAN1 Interface different than that of AP#1
- Assign a higher Mesh STP Priority 50000 to the AP#2 LAN1 Interface.

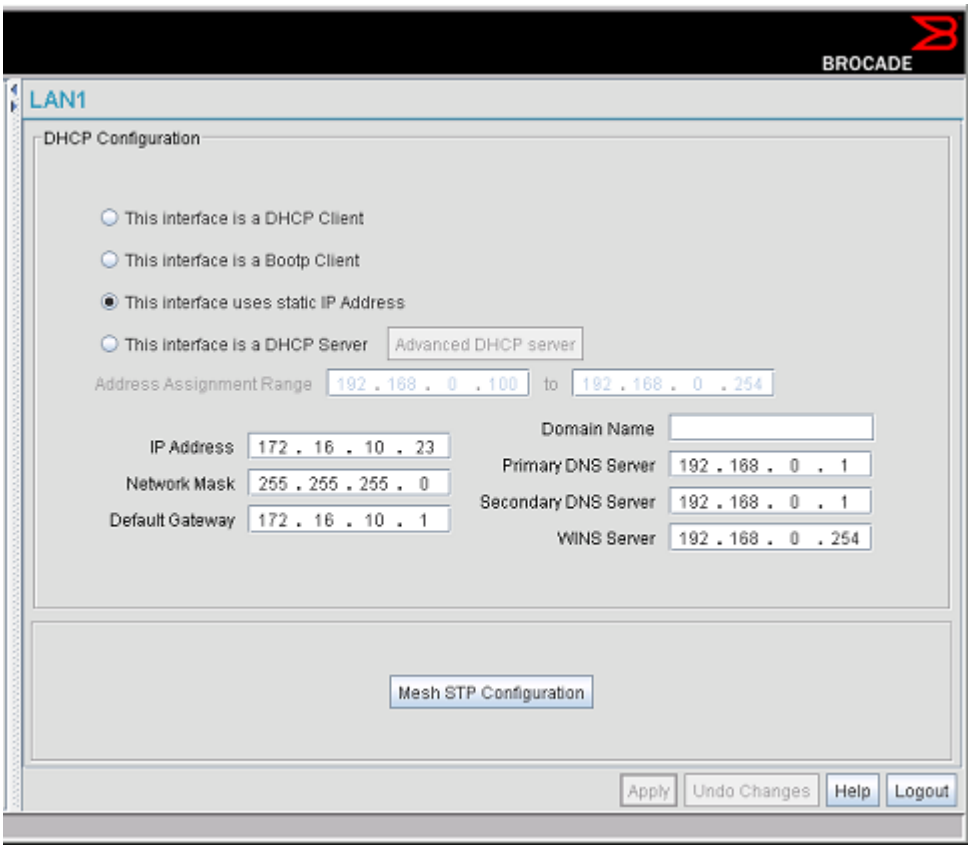
NOTE
In a typical deployment, each base bridge can be configured for a Mesh STP Priority of 50000. In this example, different values are used to force AP#1 to be the forwarding link since it's a small mesh network (of only three APs) with AP within close proximity of one another.

NOTE
Ensure AP#1 and AP#2 use the same channel for each 802.11a/n radio, or the APs will not be able to “hear” each other over different channels.

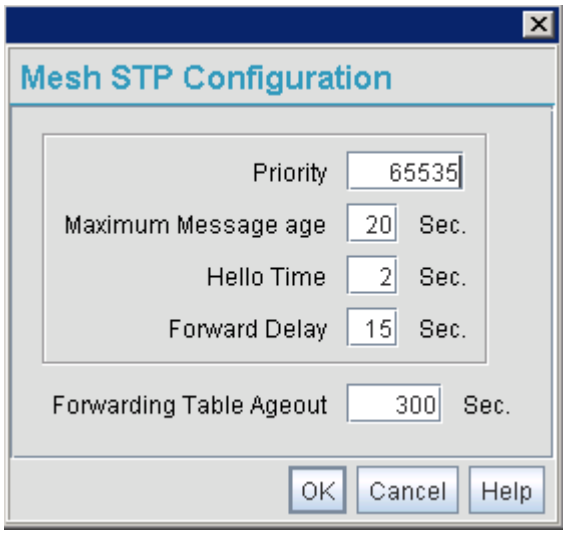
Configuring AP#3

To define the configuration for AP#3 (a client bridge connecting to both AP#1 and AP#2 simultaneously):

1. Provide a known IP address for the LAN1 interface.



2. Assign the maximum value (65535) for the Mesh STP Priority.

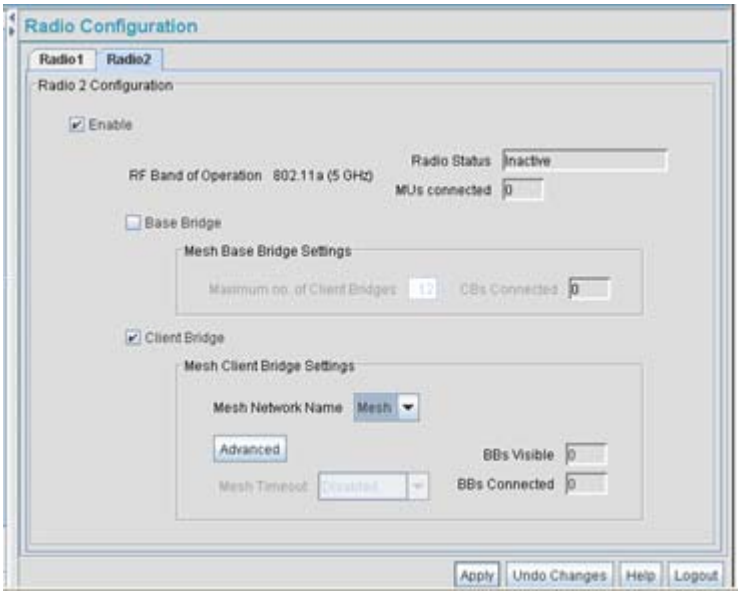


3. Create a mesh supported WLAN with the *Enable Client Bridge Backhaul* option selected.

NOTE
This WLAN should not be mapped to any radio. Therefore, leave both of the “Available On” radio options unselected.

4. Select the *Client Bridge* checkbox to enable client bridge functionality on the 802.11a/n radio. Use the *Mesh Network Name* drop-down menu to select the name of the WLAN created in step 3.

NOTE
You don't need to configure channel settings on the client bridge (AP#3). It automatically finds the base bridges (AP#1 and AP#2) and uses the channel assigned to them.



5. If needed, create another WLAN mapped to the 802.11b/g/n radio if 802.11b/g/n support is required for clients on that 802.11 band.

Verifying mesh network functionality for scenario #1

You now have a three AP mesh network ready to demonstrate. Associate a single Client on each AP WLAN configured for 802.11b/g/n radio support. Once completed, pass traffic among the three APs comprising the mesh network.

Scenario 2 - two hop mesh network with a base bridge repeater and a client bridge

By default, the mesh algorithm runs an automatic link selection algorithm to determine the best possible active and redundant links. If member APs are not far apart (in physical distance), the algorithm intelligently chooses a single hop link to forward data. To force APs to use multiple hops for demonstrations, use manual links.

In scenario 2, the following three AP configurations comprise the mesh network:

- AP#1 is a base bridge
- AP#2 is a repeater (client bridge/base bridge combination)
- AP#3 is a client b ridge

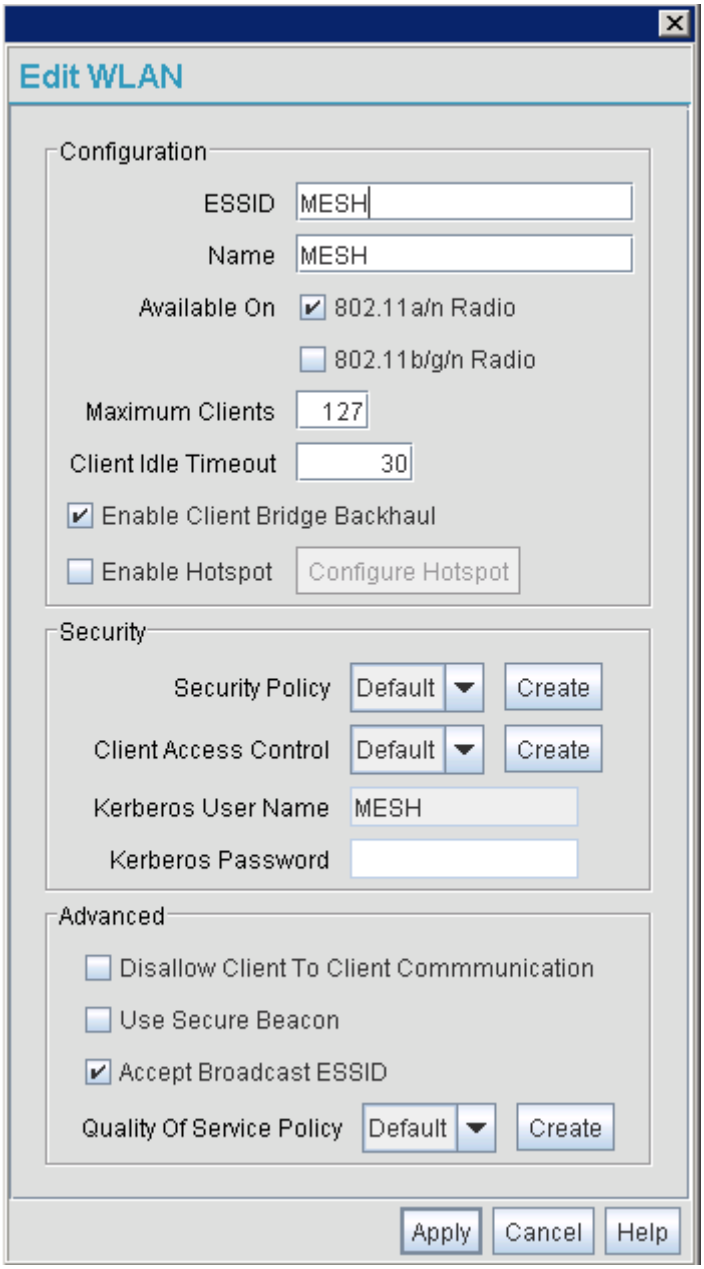
Configuring AP#1

The setup of AP#1 within this usage scenario is exactly the same as the AP#1 configuration within *Scenario 1 - two base bridges and one client bridge* for step by step instructions for configuring AP#1, see "Configuring AP#1" on page 598. Once completed, return to "Configuring AP#2" on page 606 within this section.

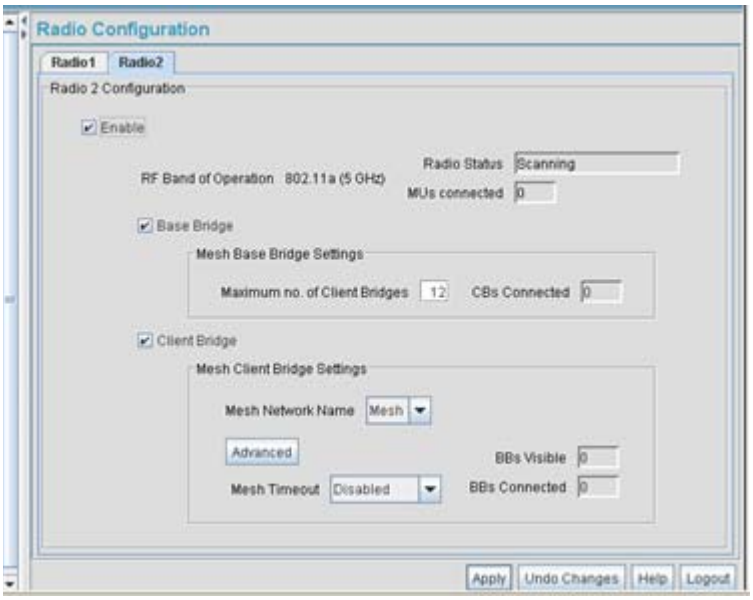
Configuring AP#2

AP#2 requires the following modifications from AP#2 in the previous scenario to function in base bridge/client bridge repeater mode.

1. Enable client bridge backhaul on the mesh supported WLAN.



2. Enable client and base bridge functionality on the 802.11a/n radio

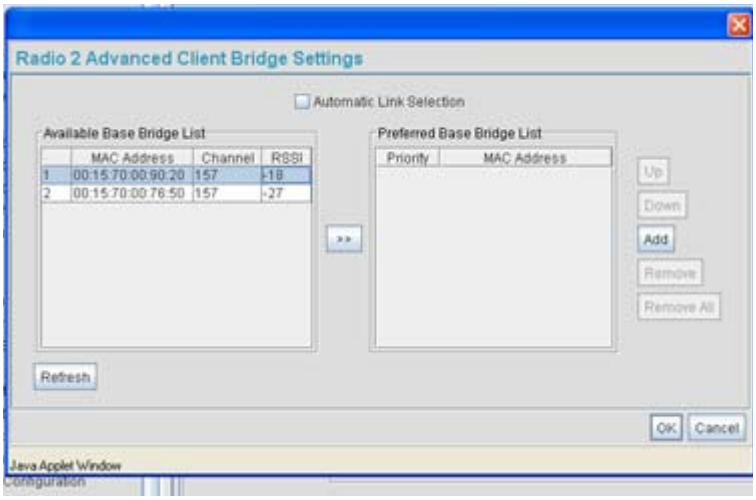


Configuring AP#3

To define AP #3's configuration:

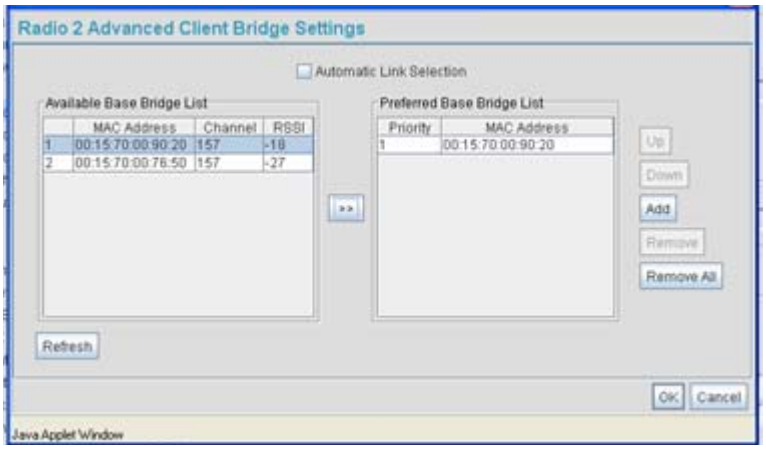
1. The only change needed on AP#3 (with respect to the configuration used in scenario #1), is to disable the *Auto Link Selection* option.

   Click the *Advanced* button within the *Mesh Client Bridge Settings* field.

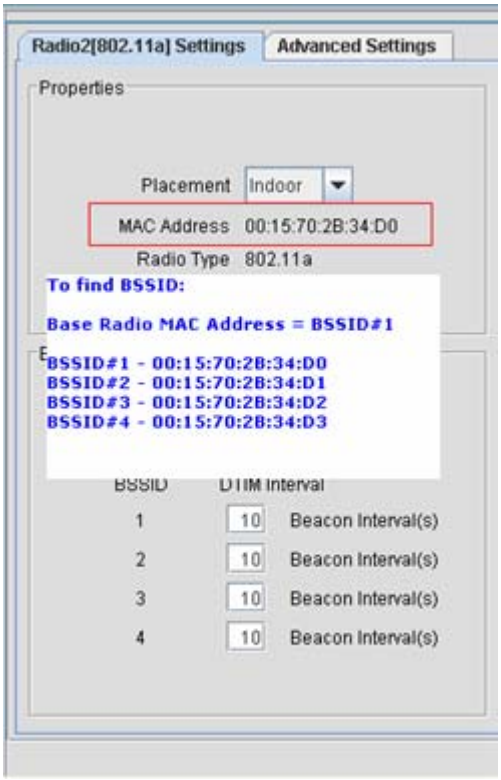


2. Add the 802.11a/n Radio MAC Address.

   In scenario #2, the mesh WLAN is mapped to BSS1 on the 802.11a/n radio if each AP. The Radio MAC Address (the BSSID#1 MAC Address) is used for the AP#2 Preferred Base Bridge List. Ensure both the AP#1 and AP#2 Radio MAC Addresses are in the Available Base Bridge List. Add the AP#2 MAC Address into the Preferred Base Bridge List.



3. Determine the Radio MAC Address and BSSID MAC Addresses.



Verifying Mesh Network Functionality for Scenario #2

You now have a three AP demo multi-hop mesh network ready to demonstrate. Associate an Client on the WLANs configured on the 802.11b/g/n radio for each AP and pass traffic among the members of the mesh network.

Mesh networking frequently asked questions

The following scenarios represent issues that could be encountered and resolved when defining a Brocade Mobility 7131 Series Access Point supported mesh configuration:

Mesh deployment issue 1 - client bridge can only connect to one of two base bridges

You have two access points configured as base bridges (AP1, AP2) and one access point defined as a as a client bridge (AP3). However, the client bridge is able to connect to only one of the base bridges.

Resolution

Check the mesh backhaul radio channel configuration on both base bridges (AP1, AP2). They need to use the same channel so the client bridge can connect to both simultaneously.

Mesh deployment issue 2 - faulty client bridge connectivity

You have configured three access points in mesh mode; one base bridge (AP1), one client bridge/base bridge (AP2) and one client bridge (AP3). However, the client bridge (AP3) is connecting to both AP1 and AP2 and using its link to base bridge (AP1) to forward traffic.

Resolution

This is valid behavior, you see this when your mesh APs are close enough (in proximity) so the client bridge can see both the base bridges (AP1, AP2), in which case it forms two links, one each to AP1 and AP2. Since the link to AP1 is the shortest path in terms of number of hops, AP3 uses that link to forward traffic.

Mesh deployment issue 3 - cannot select a WLAN name for a client bridge

You created a WLAN for mesh backhaul on an AP needed as a client bridge, but you don't get to select the WLAN name in the *Mesh Network Name* drop down menu. Why?

Resolution

Check the WLAN configuration to ensure you have enabled the *Enable Client Bridge Backhaul* option.

Mesh deployment issue 4 - Do I need to map a WLAN to a radio when configuring mesh backhaul on a client bridge?

When creating a mesh backhaul WLAN on a client bridge only AP, do you need to map the WLAN on a radio?

Resolution

No, a client bridge only AP behaves just like an Client! It scans for base bridges and forms connections to them. It doesn't need to beacon on that WLAN. Therefore, while creating a mesh backhaul WLAN on a client bridge only AP, just enable the *Enable Client Bridge Backhaul* option.

Mesh deployment issue 5 - Do I need to use secure beacons on a mesh backhaul supported WLAN?

Can I use secure beacons on the mesh backhaul supported WLAN?

Resolution

Yes, you can enable a secure beacon on a mesh backhaul supported WLAN. In fact, it is a Brocade recommended practice.

Mesh deployment Issue 6 - Is my mesh topology complete?

How can I determine if all my mesh APs are connected and the mesh topology is complete?

Resolution

Each mesh AP has a *Known AP Table* (available in the applet, CLI and SNMP). All APs (whether they are supporting mesh or not) periodically exchange ID messages notifying their presence to one another. Review the Known AP Table on any mesh supported AP to determine if you have all required APs connected to the mesh topology.

Mesh deployment Issue 7 - can clients roam within a mesh topology?

Can clients connected to a mesh AP roam seemlessly among other clients and wired access points?

Resolution

Yes, clients on a mesh APs can roam seemlessly throughout the mesh network as well as with non-mesh access points on the wired network.

Mesh deployment Issue 8 - can I mesh between a Brocade Mobility 7131 Series Access Point and a Brocade Mobility 5181 Access Point?

Can I mesh between these three models?

Resolution

Yes, the access points are fairly close from a software deployment standpoint. So it is a supported configuration for three models to exist in a single topology.

Mesh deployment issue 9 - Can I mesh between and a Brocade Mobility 7131 Series Access Point and a Brocade Mobiltiy 300 Access Point?

Can I mesh between a Brocade Mobility 7131 Series Access Point, Mobility 5181 Access Point and a Brocade Mobility 300 Access Point?

Resolution

No, a Brocade Mobility 300 Access Point does not support mesh networking, so you won't be able to mesh between two Brocade Mobility 300 Access Points or between a Brocade Mobility 300 Access Point and a Brocade Mobility 7131 Series Access Point or Mobility 5181.

Mesh deployment Issue 11 - can I update firmware/configuration files across a mesh backhaul?

Can I update device firmware over the mesh backhaul on a client bridge or repeater AP with no wired connectivity?

Resolution

Yes, a Brocade Mobility 7131 Series Access Point and a Brocade Mobility 5181 Access Point both support wireless firmware updates.

Mesh deployment issue 12 - can I perform firmware/configuration file updates with DHCP options?

Can I use the AP’s Automatic Firmware/Configuration update functionalities with DHCP Options on the AP for mesh nodes as well?

Resolution

Yes, mesh nodes also support Automatic Firmware/Configuration updates using DHCP Options. Make sure you create DHCP reservations for each mesh node and add an appropriate configuration file to each one of them. If you don't, the base bridge configuration file could get applied on a client bridge or repeater and you will loose connectivity to that AP.

Mesh deployment issue 13 - why do I lose connectivity when updating configurations?

When I make a configuration change and apply the changes on a client bridge or repeater, I momentarily loose connectivity to that AP, why?

Resolution

That is expected behavior, when you make a configuration change on a mesh supported AP, it brings the radio driver down and then back up again. Consequently, the AP needs to re-establish its mesh connection after saving the configuration.

Mesh deployment issue 14 - will an existing client bridge see a new base bridge or repeater?

If I add a new base bridge or repeater to an existing mesh topology, will my current client bridges see it and connect to it?

Resolution

Yes, all client bridges perform periodic background scanning - both passively (by sniffing the air for beacons) and actively (by sending Probe Requests). Therefore, a client bridge automatically detects the presence of a new base bridge or repeater added to the mesh network topology and forms a seam less connection without affecting current operation.

Mesh deployment issue 15 - Can a mesh supported AP react to changing RF conditions?

If RF conditions change, will a mesh supported AP automatically detect and re-route traffic on its backup link or look for new links if all current links are exhausted?

Resolution

Yes, all mesh nodes have built in dynamic link switching and auto-recovery mechanisms that ensure they adapt to changing RF conditions.

Chapter

Adaptive AP

10

In this chapter

- Adaptive AP overview. 613
- Supported adaptive AP topologies 618
- How the AP receives its adaptive configuration 619
- Establishing basic adaptive AP connectivity 620

Adaptive AP overview

An *adaptive AP* (AAP) is a Brocade Mobility 7131 Series Access Point access point that can adopt like a Brocade Mobility 300 Access Point. The management of an AAP is conducted by the controller, once the access point connects to a Brocade Mobility RFS6000 Controller or Mobility RFS7000 Controller and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- the tunneling of centralized traffic to the wireless controller

An AAP's controller connection can be secured using IP/UDP or IPSec depending on whether a secure WAN link from a remote site to the central site already exists.

The controller can be discovered using one of the following mechanisms:

- DHCP
- Controller *fully qualified domain name* (FQDN)
- Static IP addresses

The benefits of an AAP deployment include:

- *Centralized Configuration Management & Compliance* - Wireless configurations across distributed sites can be centrally managed by the wireless controller or cluster.
- *WAN Survivability* - Local WLAN services at a remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLAN's to stores for corporate visitors* - Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location.
- *Maintain local WLAN's for in store applications* - WLANs created and supported locally can be concurrently supported with your existing infrastructure.

Where to go from here

Refer to the following for a further understanding of AAP operation:

- *Adaptive AP management*
- *Licensing*
- *Controller discovery*
- *Securing a configuration channel between controller and AP*
- *Adaptive AP WLAN topology*
- *Configuration updates*
- *Securing data tunnels between the controller and AAP*
- *Adaptive AP controller failure*
- *Remote site survivability (RSS)*
- *Adaptive mesh support*

For an understanding of how AAP support should be configured for the access point and its connected controller, see "How the AP receives its adaptive configuration" on page 619.

For an overview of how to configure both the access point and controller for basic AAP connectivity and operation, see "Establishing basic adaptive AP connectivity" on page 620.

To configure the access point's controller discovery method and connection medium, see "Adaptive AP setup" on page 72.

Adaptive AP management

An AAP can be adopted, configured and managed like a thin access point from the wireless controller.

NOTE
An AAP cannot support a firmware download from the wireless controller.

Once an access point connects to a controller and receives its AAP configuration, its WLAN and radio configuration is similar to a thin access point. An AAP's radio mesh configuration can also be configured from the controller. However, non-wireless features (DHCP, NAT, Firewall etc.) cannot be configured from the controller and must be defined using the access point's resident interfaces before its conversion to an AAP.

Licensing

An AAP uses the same licensing scheme as a thin access point. This implies an existing license purchased with a controller can be used for an AAP deployment. Regardless of how many Mobility 300 and/or AAPs are deployed, you must ensure the license used by the controller supports the number of radio ports (both Mobility 300s and AAPs) you intend to adopt.

Controller discovery

For a Brocade Mobility 7131 Series Access Point to function as an AAP (regardless of mode), it needs to connect to a controller to receive its configuration. There are two methods of controller discovery:

- *Auto discovery using DHCP*
- *Manual adoption configuration*v

Auto discovery using DHCP

Extended Global Options 189, 190, 191, 192 can be used or Embedded Option 43 - Vendor Specific options can be embedded in Option 43 using the vendor class identifier: *BrocadeAP.71xx.*

	Code	Data Type
List of Controller IP addresses *(separate by comma, semi-colon, or space delimited)*	188	String
Controller FQDN	190	String
Brocade Mobility 7131 Series Access Point Encryption IPSec Passphrase (Hashed) **	191	String
Brocade Mobility 7131 Series Access Point controller discovery mode 1 = auto discovery enable 2 = auto discover enabled (using IPSec)	192	String

** The Brocade Mobility 7131 Series Access Point uses an encryption key to hash passphrases and security keys. To obtain the encryption passphrase, configure a Brocade Mobility 7131 Series Access Point with the passphrase and export the configuration file.

```
/
enc-admin-passwd d2
/
// System Configuration
/
system
set name AP-51xx
set loc \0
set email \0
set cc us
/
system
aap-setup
// Adaptive AP menu
set auto-discovery disable
set interface lan1
set name \0
set port 24576
delete all
set enc-passphrase bf0819993a702c39
set ac-keepalive 5
set tunnel-to-switch enable
/
// System-Access menu
system
access
set applet lan 1 enable
set applet slan 1 enable
set cli lan 1 enable
```

Encrypted Passphrase to be used in DHCP Option

Manual adoption configuration

A manual controller adoption of an AAP can be conducted using:

- *Static FQDN* - A controller fully qualified domain name can be specified to perform a DNS lookup and controller discovery.

- *Static IP addresses* - Up to 12 controller IP addresses can be manually specified in an ordered list the AP can choose from. When providing a list, the AAP tries to adopt based on the order in which they are listed (from 1-12).

NOTE
An AAP can use it's LAN or WAN Ethernet interface to adopt. The LAN is PoE and DHCP enabled by default.

The WAN has no PoE support and has a default static AP address of 10.1.1.1/8.

Securing a configuration channel between controller and AP

Once an access point obtains a list of available controllers, it begins connecting to each. The controller can be either on the LAN or WAN side of the access point to provide flexibility in the deployment of the network. If the controller is on the access point's LAN, ensure the LAN subnet is on a secure channel. The AP will connect to the controller and request a configuration.

Adaptive AP WLAN topology

An AAP can be deployed in the following WLAN topologies:

- *Extended WLANs* - Extended WLANs are the centralized WLANs created on the controller
- *Independent WLANs* - Independent WLANs are local to an AAP and can be configured from the controller. You must specify a WLAN as independent to stop traffic from being forwarded to the controller. Independent WLANs behave like WLANs on a standalone access point.
- *Both* - Extended and independent WLANs are configured from the controller and operate simultaneously.

NOTE
For a review of some important considerations impacting the use of extended and independent WLANs within an AAP deployment, see "Adaptive AP deployment considerations" on page 625.

Configuration updates

An AAP receives its configuration from the controller initially as part of its adoption sequence. Subsequent configuration changes on the controller are reflected on an AAP when applicable.

An AAP applies the configuration changes it receives from the controller after 30 seconds from the last received controller configuration message. When the configuration is applied on the AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds) forcing associated clients to be deauthenticated. Clients are quickly able to associate.

Securing data tunnels between the controller and AAP

If a secure link (site-to-site VPN) from a remote site to the central location already exists, the AAP does not require IPSec be configured for adoption.

For sites with no secure link to the central location, an AAP can be configured to use an IPSec tunnel (with AES 256 encryption) for adoption. The tunnel configuration is automatic on the AAP side and requires no manual VPN policy be configured. On the controller side, configuration updates are required to adopt the AAP using an IPSec tunnel.

To review a sample AAP configuration, see "Sample controller configuration file for IPSec and independent WLAN" on page 625.

Adaptive AP controller failure

In the event of a controller failure, an AAP's independent WLAN continues to operate without disruption. The AAP attempts to connect to other controllers (if available) in background. Extended WLANs are disabled once controller adoption is lost. When a new controller is discovered and a connection is secured, an extended WLAN can be enabled.

If a new controller is located, the AAP synchronizes its configuration with the located controller once adopted. If *Remote Site Survivability* (RSS) is disabled, the independent WLAN is also disabled in the event of a controller failure.

Remote site survivability (RSS)

RSS can be used to turn off RF activity on an AAP if it loses adoption (connection) to the controller.

RSS State	Independent WLANs	Extended WLANs
RSS Enabled	WLAN continues beaconing	WLAN continues beaconing but AP does allow clients to associate on that WLAN
RSS Disabled	WLAN stops beaconing	WLAN stops beaconing

NOTE
For a dependant AAP, independent WLANs continue to beacon for three days in the absence of a controller.

Adaptive mesh support

An AAP can extend existing mesh functionality to a controller managed network. All mesh APs are configured and managed through the wireless controller. APs without a wired connection form a mesh backhaul to a repeater or a wired mesh node and then get adopted to the controller. Mesh nodes with existing wired access get adopted to the controller like a wired AAP.

Mesh AAPs apply configuration changes 300 seconds after the last received controller configuration message. When the configuration is applied on the Mesh AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds), forcing associated clients to be deauthenticated and the Mesh link will go down. Clients are able to quickly associate, but the Mesh link will need to be re-established before clients can pass traffic. This typically takes about 90 to 180 seconds depending on the size of the mesh topology.

NOTE
When mesh is used with AAPs, the "ap-timeout" value needs to be set to a higher value (for example, 180 seconds) so Mesh AAPs remain adopted to the controller during the period when the configuration is applied and mesh links are re-established.

For an overview of mesh networking and how to configure a Brocade Mobility 7131 Series Access Point to support mesh, see "Configuring Mesh Networking" on page 583.

Supported adaptive AP topologies

For this version of the access point firmware, the following AAP topologies are supported:

- *Extended WLANs only*
- *Independent WLANs Only*
- *Extended WLANs with independent WLANs*
- *Extended WLAN with mesh networking*

Topology deployment considerations

When reviewing the AAP topologies describes in the section, be cognizant of the following considerations to optimize the effectiveness of the deployment:

- An AAP firmware upgrade will not be performed at the time of adoption from the wireless controller. Instead, the firmware is upgraded using the firmware update procedure (manually or using the DHCP Auto Update feature).
- An AAP can use its LAN1 interface or WAN interface for adoption. The default gateway interface is set to LAN1. If the WAN Interface is used, explicitly configure WAN as the default gateway interface.
- Brocade recommends using the LAN1 interface for adoption in multi-cell deployments.
- If you have multiple independent WLANs mapped to different VLANs, the AAP's LAN1 interface requires trunking be enabled with the correct management and native VLAN IDs configured. Additionally, the AAP needs to be connected to a 802.1q trunk port on the wired controller.
- Be aware IPSec Mode supports NAT Traversal (NAT-T).

Extended WLANs only

An extended WLAN configuration forces all Client traffic through the controller. No wireless traffic is locally bridged by the AAP.

Each extended WLAN is mapped to the access point's virtual LAN2 subnet. By default, the access point's LAN2 is not enabled and the default configuration is set to static with IP addresses defined as all zeros. If the extended VLAN option is configured on the controller, the following configuration updates are made automatically:

- The AAP’s LAN2 subnet becomes enabled
- All extended VLANs are mapped to LAN2.

NOTE
clients on the same WLAN associated to the AAP can communicate locally at the AP Level without going through the controller. If this scenario is undesirable, the access point's Client-to-Client disallow option should be enabled. To enable the access point’s Client-to-Client disallow option, see “Creating/editing individual WLANs” on page 139.

Independent WLANs Only

An independent WLAN configuration forces all Client traffic be bridged locally by the AAP. No wireless traffic is tunneled back to the controller. Each extended WLAN is mapped to the access point's LAN1 interface. The only traffic between the controller and the AAP are control messages (for example, heartbeats, statistics and configuration updates).

Extended WLANs with independent WLANs

An AAP can have both extended WLANs and independent WLANs operating in conjunction. When used together, Client traffic from extended WLANs go back to the controller and traffic from independent WLANs is bridged locally by the AP.

All local WLANs are mapped to LAN1, and all extended WLANs are mapped to LAN2.

Extended WLAN with mesh networking

Mesh networking is an extension of the existing wired network. There is no special configuration required, with the exceptions of setting the mesh and using it within one of the two extended VLAN configurations and defining an access point radio as a preferred base bridge.

NOTE
The mesh backhaul WLAN must be an independent WLAN mapped to LAN1. The controller enforces the WLAN be defined as an independent WLAN by automatically setting the WLAN to independent when backhaul is selected. The AP ensures the backhaul WLAN be put on LAN1.

How the AP receives its adaptive configuration

An AAP does not require a separate "local" or "running" configuration. Once enabled as an AAP, the AP obtains its configuration from the controller. If the AP's WAN link fails, it continues to operate using the last valid configuration until its link is re-established and a new configuration is pushed down from the controller. There is no separate file-based configuration stored on the controller.

Only WLAN, VLAN extension and radio configuration items are defined for the AAP by its connected controller. None of the other access point configuration items (RADIUS, DHCP, NAT, Firewall etc.) are configurable from the connected controller.

After the AP downloads a configuration file from the controller, it obtains the version number of the image it should be running. The controller does not have the capacity to hold the access point's firmware image and configuration. The access point image must be downloaded using a means outside the controller. If there is still an image version mismatch between what the controller expects and what the AAP is running, the controller will deny adoption.

Adaptive AP pre-requisites

Converting a Brocade Mobility 7131 Series Access Point model access point into an AAP requires:

- A Brocade Mobility RFS6000 Controller or Mobility RFS7000 Controller.
- The appropriate controller licenses providing AAP functionality on the controller.
- The correct password to authenticate and connect the adaptive to the controller.

Configuring the adaptive AP for adoption by the controller

1. An AAP needs to find and connect to the controller. To ensure this connection:
   - Configure the controller's IP address on the AAP
   - Provide the controller IP address using DHCP option 189 on a DHCP server. The IP address is a comma delimited string of IP addresses. For example "157.235.94.91, 10.10.10.19". There can be a maximum of 12 IP addresses.
   - Configure the controller's FQDN on the AAP. The AAP can use this to resolve the IP address of the controller.
2. Use the controller's secret password on the AAP for the controller to authenticate it.

   For additional information on defining the connection medium used by the access point t to receive an AAP configuration, see "Adaptive AP setup" on page 72.

   To avoid a lengthy broken connection with the controller, Brocade recommends generating an SNMP trap when the AAP loses adoption with the controller.

NOTE
For additional information (in greater detail) on the AP configuration activities described above, see "Adaptive AP configuration" on page 621.

Configuring the controller for adaptive AP adoption

The tasks described below are configured on a Brocade Mobility RFS6000 Controller or a RFS7000 Controller. For information on configuring the controller for AAP support, see *http://www.brocade.com*.

To adopt an AAP on a controller:

1. Ensure enough licenses are available on the controller to adopt the required number of AAPs.
2. As soon as the AAP displays in the adopted list:

   Adjust each AAP's radio configuration as required. This includes WLAN-radio mappings and radio parameters. WLAN-VLAN mappings and WLAN parameters are global and cannot be defined on a per radio basis. WLANs can be assigned to a radio as done today for a Brocade Mobility 300 model access point. Optionally, configure WLANs as independent and assign to AAPs as needed.
3. Configure each VPN tunnel with the VLANs to be extended to it.

   If you do not attach the target VLAN, no data will be forwarded to the AAP, only control traffic required to adopt and configure the AP.

NOTE
For additional information (in greater detail) on the controller configuration activities described above, see "Controller configuration" on page 623.

Establishing basic adaptive AP connectivity

This section defines the activities required to configure basic AAP connectivity with a Brocade Mobility RFS6000 Controller or Mobility RFS7000 Controller. In establishing a basic AAP connection, both the access point and controller require modifications to their respective default configurations. For more information, see:

- *Adaptive AP configuration*
- *Controller configuration*

NOTE
Refer to *"Adaptive AP deployment considerations"* on page 625 for usage and deployment caveats that should be considered before defining the AAP configuration. Refer to *"Sample controller configuration file for IPSec and independent WLAN"* on page 625 if planning to deploy an AAP configuration using IPSec VPN and an extended WLAN.

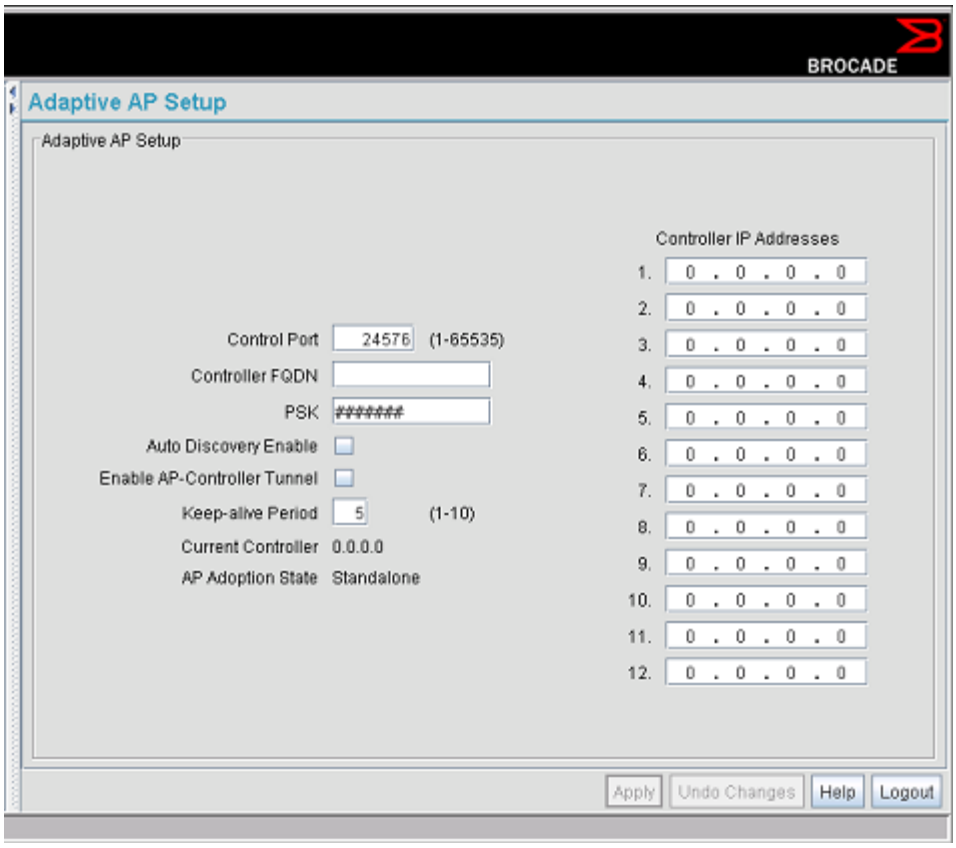
Adaptive AP configuration

An AAP can be manually adopted by the controller, adopted using a configuration file (consisting of the adaptive parameters) pushed to the access point or adopted using DHCP options. Each of these adoption techniques is described in the sections that follow.

Adopting an adaptive AP manually

To manually enable the access point's controller discovery method and connection medium required for adoption:

1. Select *System Configuration -> Adaptive AP Setup* from the access point's menu tree.



2. Select the *Auto Discovery Enable* checkbox.

Enabling auto discovery will allow the AAP to be detected by a controller once its connectivity medium has been configured (by completing steps 3-6)

3. Enter up to 12 *controller IP Addresses* constituting the target switches available for AAP connection.

   The AAP will begin establishing a connection with the first addresses in the list. If unsuccessful, the AP will continue down the list (in order) until a connection is established.

4. If a numerical IP address is unknown, but you know a controller's *fully qualified domain name* (FQDN), enter the name as the *controller FQDN* value.

5. Select the *Enable AP-Controller Tunnel* option to allow AAP configuration data to reach a controller using a secure VPN tunnel.

6. If using IPSec as the tunnel resource, enter the IPSec *Passkey* to ensure IPSec connectivity.

7. Click *Apply* to save the changes to the AAP setup.

NOTE
The manual AAP adoption described above can also be conducted using the access point's CLI interface using the *admin(system.aapsetup)>* command.

Adopting an adaptive AP using a configuration file

To adopt an AAP using a configuration file:

1. Refer to *Adopting an adaptive AP manually* and define the AAP controller connection parameters.

2. Export the AAP's configuration to a secure location.

   Either import the configuration manually to other APs or the same AP later (if you elect to default its configuration). Use DHCP option 186 and 187 to force a download of the configuration file during startup (when it receives a DHCP offer).

   For instruction on how to use the access point's configuration import/export functionality, see "Importing/exporting configurations" on page 103.

   For information on updating the access point's firmware, see "Updating device firmware" on page 108.

Adopting an adaptive AP using DHCP options

An AAP can be adopted to a wireless controller by providing the following options in the DHCP Offer:

Option	Data Type	Value
189	String	<Controller IP Address or Range of IP addresses separated by [, ; <space>]>
190	String	<Fully qualified Domain Name for the Wireless Controller>
191	String	<Hashed IPSec Passkey - configure on 1 AP and export to get hashed key>
192	String	<Value of "1" denotes Non-IPSec Mode and "2" denotes IPSec Mode>

NOTE
Options 189 and 192 are mandatory to trigger adoption using DHCP options. Unlike a Brocade Mobility 300, option 189 alone won't work. These options can be embedded in Vendor Specific Option 43 and sent in the DHCP Offer.

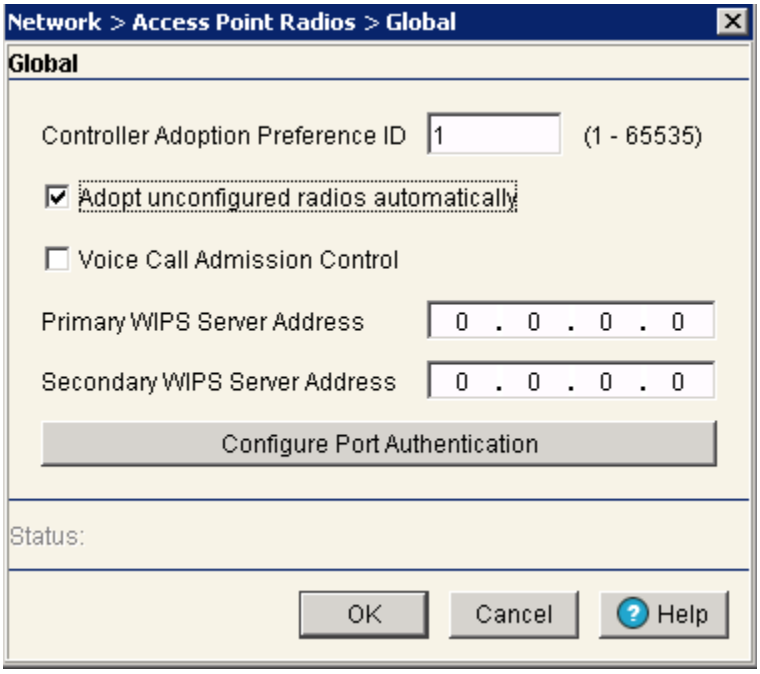
Controller configuration

Both a Brocade Mobility RFS6000 Controller and a Brocade Mobility RFS7000 Controller require an explicit adaptive configuration to adopt an access point (if IPSec is not being used for adoption). The same licenses currently used for Mobility 300 adoption can be used for an AAP.

Disable the controller's *Adopt unconfigured radios automatically* option and manually add AAPs requiring adoption, or leave as default. In default mode, any AAP adoption request is honored until the current controller license limit is reached.

To disable automatic adoption on the controller:

1. Select *Network* > *Access Point Radios* from the controller main menu tree.
2. Select the *Configuration* tab (should be displayed be default) and click the *Global Settings* button.



3. Ensure the *Adopt unconfigured radios automatically* option is NOT selected.

   When disabled, there is no automatic adoption of non-configured radios on the network. Additionally, default radio settings will NOT be applied to access points when automatically adopted.

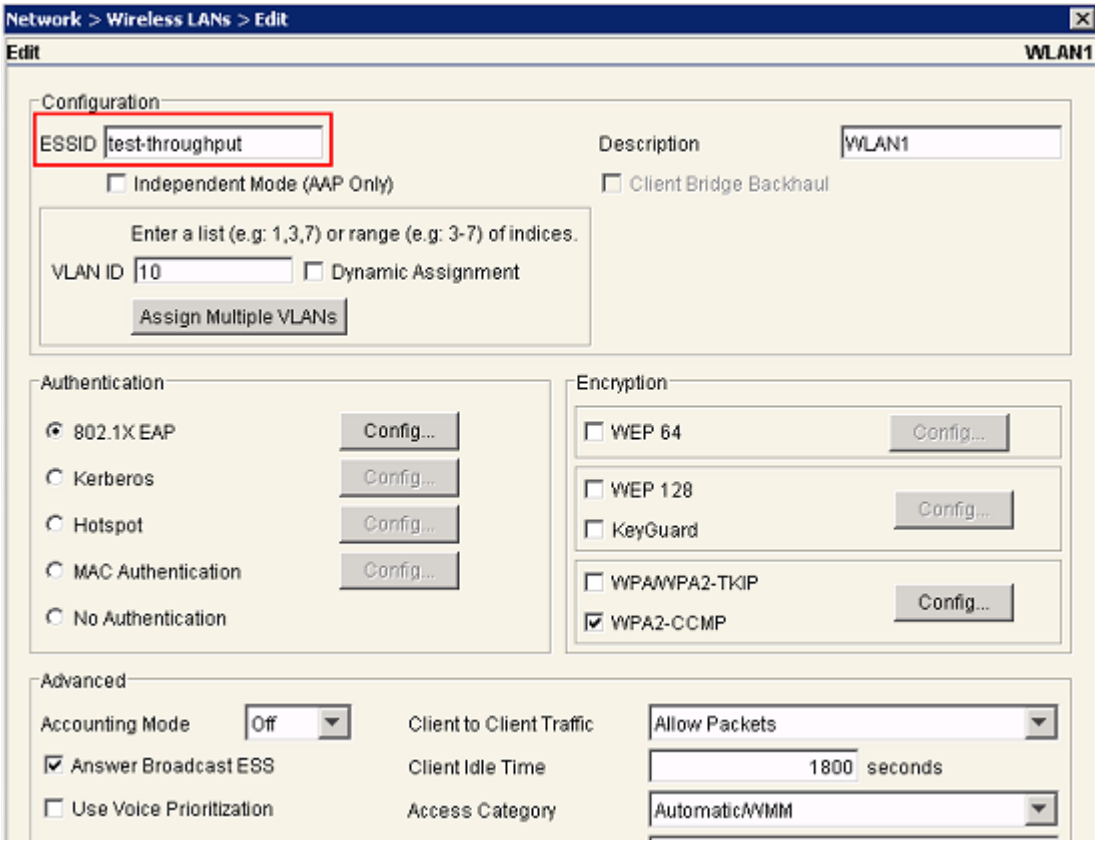
NOTE
For IPSec deployments, refer to "Sample controller configuration file for IPSec and independent WLAN" on page 625 and take note of the CLI commands in red and associated comments in green.

   Any WLAN configured on the controller becomes an extended WLAN by default for an AAP.

4. Select *Network* > *Wireless LANs* from the controller main menu tree.
5. Select the target WLAN you would like to use for AAP support from those displayed and click the *Edit* button.

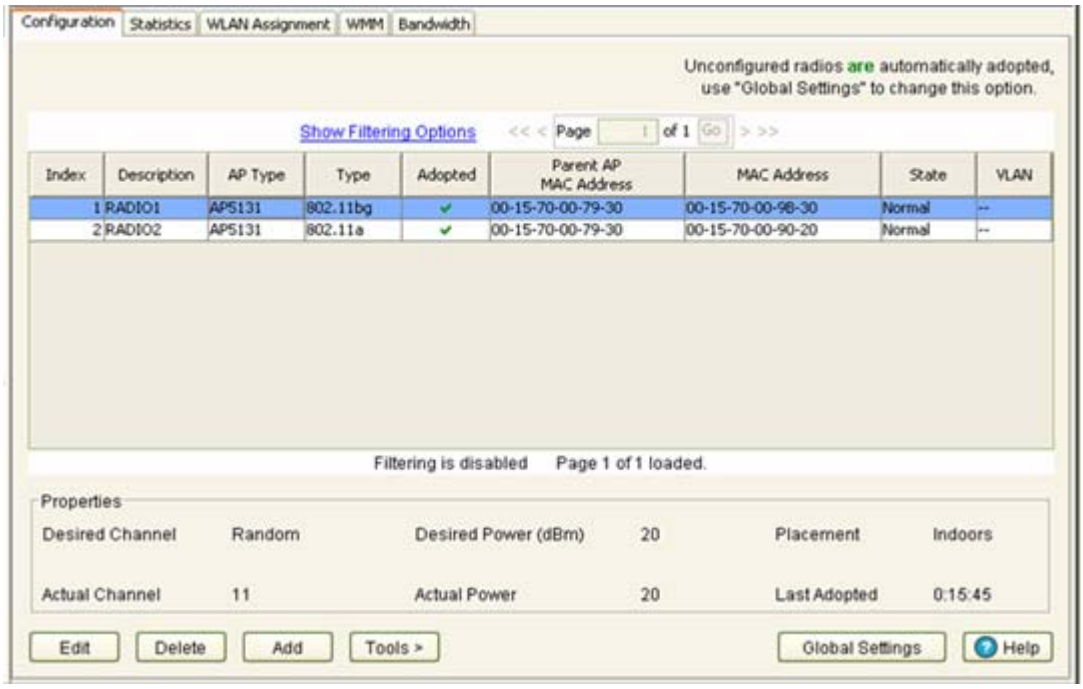
6. Select the *Independent Mode (AAP Only)* checkbox.

   Selecting the checkbox designates the WLAN as independent and prevents traffic from being forwarded to the controller. Independent WLANs behave like WLANs as used on a a standalone access point. Leave this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the controller).



NOTE
Additionally, a WLAN can be defined as independent using the "*wlan <index> independent*" command from the config-wireless context.

Once an AAP is adopted by the controller, it displays within the controller *Access Point Radios* screen (under the Network parent menu item) as a Brocade Mobility 7131 Series Access Point within the *AP Type* column.



Adaptive AP deployment considerations

Before deploying your controller/AAP configuration, refer to the following usage caveats to optimize its effectiveness:

- Extended WLANs are mapped to the AP's LAN2 interface and all independent WLANs are mapped to the AP's LAN1 Interface.
- If deploying multiple independent WLANs mapped to different VLANs, ensure the AP's LAN1 interface is connected to a trunk port on the L2/L3 controller and appropriate management and native VLANs are configured.
- The WLAN used for mesh backhaul must always be an independent WLAN.
- The controller configures an AAP. If manually changing wireless settings on the AP, they are not updated on the controller. It's a one way configuration, from the controller to the AP.
- An AAP always requires a router between the AP and the controller.
- An AAP can be used behind a NAT.
- An AAP uses UDP port 24576 for control frames and UDP port 24577 for data frames.
- Multiple VLANs per WLAN, L3 mobility, dynamic VLAN assignment, NAC, self healing, rogue AP, Client locationing, hotspot on extended WLAN are some of the important wireless features not supported in an AAP supported deployment.

Sample controller configuration file for IPSec and independent WLAN

The following constitutes a sample Mobility RFS7000 Controller configuration file supporting an AAP IPSec with Independent WLAN configuration. Please note new AAP specific CLI commands in red and relevant comments in blue.

The sample output is as follows:

```
!
! configuration of RFS7000 RFS7000-1 version 3.2.2.0
!
version 1.0
!
!
aaa authentication login default none
service prompt crash-info
!
hostname RFS7000-1
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
To configure the ACL to be used in the CRYPTO MAP
!
ip access-list extended AAP-ACL permit ip host 10.10.10.250 any rule-precedence 20
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst config
name My Name
!
country-code us
logging buffered 4
logging console 7
logging host 157.235.92.97
logging syslog 7
snmp-server sysname RFS7000-1
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
!
To configure the passkey for a Remote VPN Peer - 255.255.255.255 denotes all AAPs. 12345678
is the default passkey. If you change on the AAP, change here as well.
!
crypto isakmp key 0 12345678 address 255.255.255.255
!
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
no service pm sys-restart
timezone America/Los_Angeles
license AP
xyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyx
!
```

```
wireless
no adopt-unconf-radio enable
manual-wlan-mapping enable
wlan 1 enable
wlan 1 ssid qs5-ccmp
wlan 1 vlan 200
wlan 1 encryption-type ccmp
wlan 1 dot11i phrase 0 Brocade123
wlan 2 enable
wlan 2 ssid qs5-tkip
wlan 2 vlan 210
wlan 2 encryption-type tkip
wlan 2 dot11i phrase 0 Brocade123
wlan 3 enable
wlan 3 ssid qs5-wep128
wlan 3 vlan 220
wlan 3 encryption-type wep128
wlan 4 enable
wlan 4 ssid qs5-open
wlan 4 vlan 230
wlan 5 enable
wlan 5 ssid Mesh
wlan 5 vlan 111
wlan 5 encryption-type ccmp
wlan 5 dot11i phrase 0 Brocade123
!
To configure a WLAN as an independent WLAN
!
wlan 5 independent
wlan 5 client-bridge-backhaul enable
wlan 6 enable
wlan 6 ssid test-mesh
wlan 6 vlan 250
radio add 1 00-15-70-00-79-30 11bg aap7131
radio 1 bss 1 3
radio 1 bss 2 4
radio 1 bss 3 2
radio 1 channel-power indoor 11 8
radio 1 rss enable
radio add 2 00-15-70-00-79-30 11a aap7131
radio 2 bss 1 5
radio 2 bss 2 1
radio 2 bss 3 2
radio 2 channel-power indoor 48 8
radio 2 rss enable
radio 2 base-bridge max-clients 12
radio 2 base-bridge enable
radio add 3 00-15-70-00-79-12 11bg aap7131
radio 3 bss 1 3
radio 3 bss 2 4
radio 3 bss 3 2
radio 3 channel-power indoor 6 8
```

```
radio 3 rss enable
radio add 4 00-15-70-00-79-12 11a aap7131
radio 4 bss 1 5
radio 4 bss 2 6
radio 4 channel-power indoor 48 4
radio 4 rss enable
radio 4 client-bridge bridge-select-mode auto
radio 4 client-bridge ssid Mesh
radio 4 client-bridge mesh-timeout 0
radio 4 client-bridge enable
radio default-11a rss enable
radio default-11bg rss enable
radio default-11b rss enable
no ap-ip default-ap switch-ip
!
radius-server local
!
To create an IPSEC Transform Set
!
crypto ipsec transform-set AAP-TFSET esp-aes-256 esp-sha-hmac mode tunnel
!
To create a Crypto Map, add a remote peer, set the mode, add a ACL rule to match and transform
and set to the Crypto Map
!
crypto map AAP-CRYPTOMAP 10 ipsec-isakmp
set peer 255.255.255.255
set mode aggressive
match address AAP-ACL
set transform-set AAP-TFSET
!
interface ge1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge2
switchport access vlan 1
!
interface ge3
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge4
switchport access vlan 1
!
```

```
interface me1
ip address dhcp
!
interface sa1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
!
!
!
!
interface vlan1
ip address dhcp
!
To attach a Crypto Map to a VLAN Interface
!
crypto map AAP-CRYPTOMAP
!
sole
!
ip route 157.235.0.0/16 157.235.92.2
ip route 172.0.0.0/8 157.235.92.2
!
ntp server 10.10.10.100 prefer version 3

line con 0
line vty 0 24
!
end
```

Appendix

Technical Specifications

A

In this chapter

- Mobility 7131 physical characteristics 631
- Mobility 7131N physical characteristics 631
- Electrical characteristics 632
- Radio characteristics 632
- Antenna specifications 633
- Country codes 634

Mobility 7131 physical characteristics

A Brocade Mobility 7131 Access Point has the following physical characteristics:

Dimensions	5.50 in. L x 8.00 in. W x 1.10 in. H 13.97 cm L x 20.32 cm W x 2.79 cm H
Housing	Metal, plenum-rated housing (UL2043)
Weight	2.22 lbs/9.98 kg
Operating Temperature	-4°F to 122°F/-20°C to 50°C
Storage Temperature	-40°F to 158°F/-40°C to 70°C
Altitude	8000 ft./2438 m @ 82°F/28°C (Operating) 15000 ft./4572 m @ 53°F/12°C (Storage)
Humidity	5 to 95% RH non-condensing
Electrostatic Discharge	15kV air, 8kV contact

Mobility 7131N physical characteristics

A Brocade Mobility 7131N Access Point has the following physical characteristics:

Dimensions	5.50 in. Depth x 7.88 in. Width x 1.38 in. Height 14 cm Depth x 20.32 cm Width x 3.5 cm Height
Housing	Metal, plenum-rated housing (UL2043)
Weight	2.7 lbs
Operating Temperature	-4°F to 122°F/-20°C to 50°C
Storage Temperature	-40°F to 158°F/-40°C to 70°C

Altitude	8000 ft./2438 m @ 82°F/28°C (Operating) 15000 ft./4572 m @ 53°F/12°C (Storage)
Humidity	5 to 95% RH non-condensing
Electrostatic Discharge	15kV air, 8kV contact

Electrical characteristics

The Brocade Mobility 7131 Series Access Point has the following electrical characteristics:

Operating Voltage	38-54V DC
Operating Current	Not to exceed 600mA @ 48VDC

Radio characteristics

A Brocade Mobility 7131 Access Point has the following radio characteristics:

Operating Channels	All channels from 4920 MHz to 5825 MHz except channel 52 -64 Channels 1-13 (EU), Channels 1-11 (US/Canada) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory
Data Rates Supported	802.11g: 1,2,5.5,11,6,9,12,18,24,36,48, and 54Mbps 802.11a: 6,9,12,18,24,36,48, and 54Mbps 802.11n: MCS 0-15 up to 300Mbps
Wireless Medium	*Direct Sequence Spread Spectrum* (DSSS), *Orthogonal Frequency Division Multiplexing* (OFDM) *Spatial multiplexing* (MIMO)
Network Standards	802.11a, 802.11b, 802.11g, 802.3, 802.11n (Draft 2.0)
Maximum Available Transmit Power	20dBm
Transmit Power Adjustment	1dB increments
Antenna Configuration	2x3 or 3x3

A Brocade Mobility 7131N Access Point has the following radio characteristics:

Operating Channels	All channels from 4920 MHz to 5825 MHz except channel 52 -64 Channels 1-13 (EU), Channels 1-11 (US/Canada) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory
Data Rates Supported	802.11g: 1,2,5.5,11,6,9,12,18,24,36,48, and 54Mbps 802.11a: 6,9,12,18,24,36,48, and 54Mbps 802.11n: MCS 0-15 up to 300Mbps

Wireless Medium	*Direct Sequence Spread Spectrum* (DSSS), *Orthogonal Frequency Division Multiplexing* (OFDM) *Spatial multiplexing* (MIMO)
Network Standards	802.11a, 802.11b, 802.11g, 802.3, 802.11n (Draft 2.0)
Maximum Available Transmit Power	Maximum available conducted transmit power per chain: 2.4Ghz: + 23dBm Maximum available conducted transmit power all chains: 2.4GHz: + 27.7dBm Maximum available conducted transmit power per chain: 5.2Ghz: + 20 dBm Maximum available conducted transmit power all chains: 5.2GHz: + 24.7dBm
Transmit Power Adjustment	1dB increments
Antenna Configuration	2x3 or 3x3

Antenna specifications

CAUTION

Using an antenna other than the Dual-Band Antenna (Part No. ML-2452-APA2-01) could render the Brocade Mobility 7131 Series Access Point's Rogue AP Detector Mode feature inoperable. Contact your Brocade sales associate for specific information.

2.4 GHz antenna matrix

The following table describes each 2.4 GHz antenna approved for use with the Brocade Mobility 7131 Series Access Point.

Part Number	Antenna Type	Nominal Net Gain (dBi)
ML-2499-11PNA2-01R	Wide Angle Directional	8.5
ML-2499-HPA3-01R	Omni-Directional Antenna	3.3
ML-2499-BYGA2-01R	Yagi Antenna	13.9
ML-2452-APA2-01	Dual-Band	3.0
ML-2452-PTA2M3X3-2	Facade with 6 Element Antenna Module	2.0
ML-2452-PTA3M3-036	3 Port MIMO Antenna	3.0

5 GHz antenna matrix

The following table describes each 5 GHz antenna approved for use with the Brocade Mobility 7131 Series Access Point.

Part Number	Antenna Type	Nominal Net Gain (dBi)
ML-5299-WPNA1-01R	Panel Antenna	13.0
ML-5299-HPA1-01R	Wide-Band Omni-Directional Antenna	5.0

Part Number	Antenna Type	Nominal Net Gain (dBi)
ML-2452-APA2-01	Dual-Band	4.0
ML-2452-PTA2M3X3-2	Facade with 6 Element Antenna Module	2.0
ML-2452-PTA3M3-036	3 Port MIMO Antenna	3.0

Brocade Mobility 7131 Series Access Point additional antenna components

The following table lists the Brocade part number for various antenna accessories. This table also includes the loss for each accessory at both 2.4 and 5 GHz.

Item	Part Number	Description	Loss (db) @ 2.4 GHz	Loss (db) @ 5 GHz
72PJ	ML-1499-72PJ-01R	Cable Extension	2.5	
LAK1	ML-1499-LAK1-01R	Lightning Arrestor+	0.75	
LAK2	ML-1499-LAK2-01R	Lightning Arrestor	0.25	
10JK	ML-1499-10JK-01R	Jumper Kit	0.75	1.6
25JK	ML-1499-25JK-01R	Jumper Kit	1.9	3.5
50JK	ML-1499-50JK-01R	Jumper Kit	3.75	6.6
100JK	ML-1499-100JK-01R	Jumper Kit	7.5	12.8

Brocade Mobility 7131 Series Access Point antenna accessory connectors, cable type and length

The following table describes each antenna accessory's connector and cable type, plus the length.

Item	Connector1	Connector2	Length (meters)	Cable Type
72PJ	RPBNC-F	RPBNC-M	1.83	RG-58
LAK1	RPBNC-F	N-F	0.305	RG-58
LAK2	N-F	N-M		
10JK	N-M	N-M	3.05	RG-8
25JK	N-M	N-M	7.62	RG-8
50JK	N-M	N-M	15.24	RG-8
100JK	N-M	N-M	30.48	RG-8

Country codes

The following list of countries and their country codes is useful when using the access point configuration file, CLI or the MIB to configure the access point:

Country	Code	Country	Code
Argentina	AR	Mexico	MX
Australia	AU	Montenegro	ME
Austria	AT	Morocco	MA
Bahamas	BS	Netherlands	NL
Bahrain	BH	Netherlands Antilles	AN
Barbados	BB	New Zealand	NZ
Belarus	BY	Nicaragua	NI
Bermuda	BM	Norfolk Island	NF
Belgium	BE	Norway	NO
Bolivia	BO	Oman	OM
Botswana	BW	Panama	PA
Botznia-Herzegovina	BA	Pakistan	PK
Brazil	BR	Paraguay	PY
Bulgaria	BG	Peru	PE
Canada	CA	Philippines	PH
Cayman Islands	KY	Poland	PL
Chile	CL	Portugal	PT
China	CN	Puerto Rico	PR
Christmas Islands	CX	Qatar	QA
Colombia	CO	Romania	RO
Costa Rica	CR	Russian Federation	RU
Croatia	HR	Saudi Arabia	SA
Cypress	CY	Serbia	RS
Czech Rep.	CZ	Singapore	SG
Denmark	DK	Slovak Republic	SK
Dominican Republic	DO	Slovenia	SI
Ecuador	EC	South Africa	ZA
El Salvador	SV	South Korea	KR
Estonia	EE	Spain	ES
Egypt	EG	Sri Lanka	LK
Falkland Islands	FK	Sweden	SE
Finland	FI	Switzerland	CH
France	FR	Taiwan	TW
Germany	DE	Thailand	TH
Greece	GR	Trinidad and Tobago	TT
Guam	GU	Turkey	TR

Guatemala	GT	Ukraine	UA
Guinea	GN	UAE	AE
Haiti	HT	United Kingdom	UK
Honduras	HN	USA	US
Hong Kong	HK	Uruguay	UY
Hungary	HU	Virgin Islands (British)	VG
Iceland	IS	Virgin Islands (US)	VI
India	IN	Vietnam	VN
Indonesia	ID	Venezuela	VE
Ireland	IE		
Israel	IL		
Italy	IT		
Jamaica	JM		
Japan	JP		
Jordan	JO		
Kazakhstan	KZ		
Kuwait	KW		
Latvia	LV		
Lebanon	LB		
Liechtenstein	LI		
Lithuania	LT		
Luxembourg	LU		
Macedonia	MK		
Malaysia	MY		
Malta	MT		
Martinique	MQ		

Appendix

Usage Scenarios

B

In this chapter

- Configuring automatic updates using a DHCP or Linux BootP Server 637
- Configuring an IPSEC tunnel and VPN FAQs 643

This appendix provides practical usage scenarios for many of the access point's key features. This information should be referenced as a supplement to the information contained within this Product Reference Guide.

Configuring automatic updates using a DHCP or Linux BootP Server

This section provides specific details for configuring either a DHCP or Linux BootP Server to send firmware or configuration file updates to an access point.

The AutoUpdate feature updates the access point firmware and/or configuration automatically when the access point is reset or does a DHCP request. The update process is conducted over the LAN or WAN port depending on which server responds first to the access point's request for an automatic update.

The firmware is automatically updated each time firmware versions are found to be different between what is running on the access point and the firmware file that resides on the server. The configuration file is automatically applied when the configuration filename is found to be different between what resides on the access point and the filename residing on the server or when the configuration version is found to be different between what resides on the access point and the configuration version residing on the server.

The configuration version can be modified in the text file to cause the configuration to be applied when required. The access point only checks the two characters after the third hyphen (01) when making a comparison. Change the last two characters to update the configuration. The two characters can be alpha-numeric.

Windows - DHCP server configuration

See the following sections for information on these DHCP server configurations in the Windows environment:

- *Embedded options - using option 43*
- *Global options - using extended/standard options*
- *DHCP priorities*

Embedded options - using option 43

This section provides instructions for automatic update of firmware and configuration file via DHCP using extended options or standard options configured globally.

The setup example described in this section includes:

- 1 Brocade Mobility 7131 Series Access Point model access point
- 1 Microsoft Windows DHCP Server
- 1 TFTP Server

Note the following caveats regarding this procedure before beginning:

- Ensure the LAN Interface is configured as a DHCP Client
- If the existing and update firmware files are the same, the firmware will not get updated.

To configure the DHCP Server for automatic updates:

1. Set the Windows DHCP Server and access point on the same Ethernet segment.
2. Configure the Windows based DHCP Server as follows:
    a. Highlight the Server Domain Name (for example, apfw.brocade.com). From the *Action* menu, select *Define Vendor Classes*.
    b. Create a new vendor class. For example, Mobility7131 Options.
    c. Enter the vendor class Identifier**.** Enter the value in ASCII format, the server converts it to hex automatically.
    d. From the *Action* menu, select *Set Predefined Options*.
    e. Add the following 3 new options under Mobility7131 Options class:

	Code	Data type
Access point TFTP Server IP Address (Note: Use any one option)	181 186	IP address String
Access point Firmware File Name	187	String
Access point Config File Name (Note: Use any one option)	129 188	String String

    f. Highlight *Scope Options* from the tree and select *Configure Options*.
    g. Go to the *Advanced* tab. From under the Vendor Class Mobility7131 Options, check all three options mentioned in the table above and enter a value for each option.
3. Copy the firmware and configuration files to the appropriate directory on the TFTP Server.
4. Restart the access point.
5. While the access point boots, verify the access point:
    - Obtains and applies the expected IP Address from the DHCP Server
    - Downloads both the firmware and configuration files from the TFTP Server and updates both as needed. Verify the file versions within the *System Settings* screen.

NOTE
If the firmware files are the same, the firmware will not get updated. If the configuration file name matches the last used configuration file on the access point or if the configuration file versions are the same, the access point configuration will not get updated.

Global options - using extended/standard options

The following are instructions for automatic firmware and configuration file updates via DHCP using extended options or standard options configured globally.

The setup example described in this section includes:

- 1 Brocade Mobility 7131 Series Access Point model access point
- 1 Microsoft Windows DHCP Server
- 1 TFTP Server.

To configure Global options using extended/standard options:

1. Set the Windows DHCP Server and access point on the same Ethernet segment.
2. Configure the Windows based DHCP Server as follows:
   a. Highlight the Server Domain Name (for example, apfw.brocade.com). From the *Action* menu, select *Set Predefined Options*.
   b. Add the following 3 new options under *DHCP Standard Options* class:

Extended Options	Code	Data type
Access point TFTP Server IP Address (Note: Use any one option)	181 186	IP address String
Access point Firmware File Name	187	String
Access point Config File Name (Note: Use any one option)	129 188	String String

Standard Options	Code	Data type
Access point TFTP Server IP Address	66	String
Access point Firmware File Name	67	String

NOTE
If using Standard Options and the configuration of the access point needs to be changed, use option 129 or 188 as specified in the Extended Options table. Standard options 66 and 67 are already present in the DHCP Standard Options Class by default.

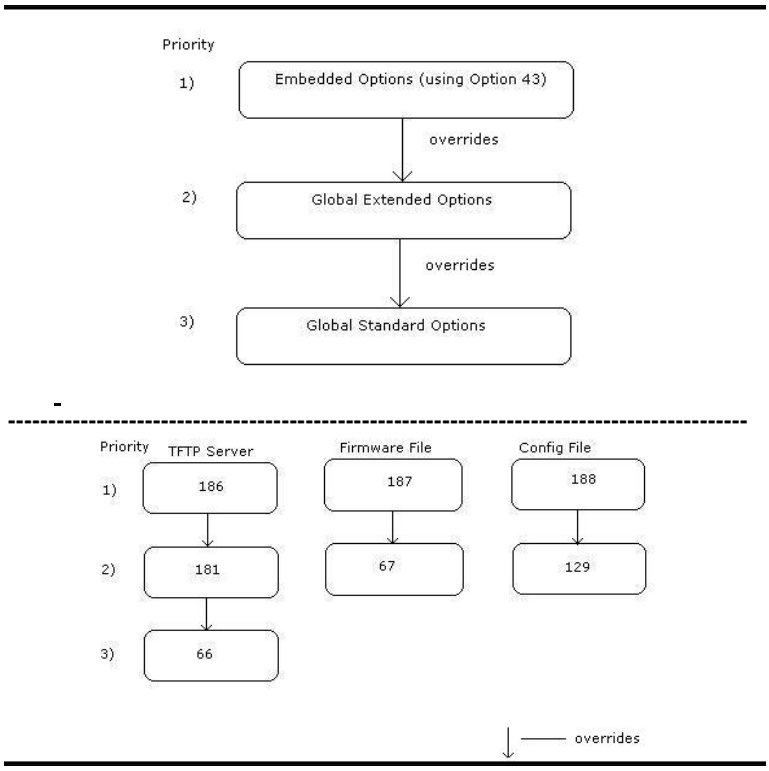
   c. Highlight *Scope Options* and select *Configure Options*.
   d. Under the *General* tab, check all 3 options mentioned within the Extended Options table and enter a value for each option.
3. Copy both the firmware and configuration files to the appropriate directory on the TFTP Server.
4. By default, auto update is enabled on the access point (since the LAN Port is a DHCP Client, out-of-the-box auto update support is on the LAN Port).
5. Restart the access point.
6. While the access point boots up, verify the access point:
   - Obtains and applies the expected IP Address from the DHCP Server
   - Downloads the firmware and configuration files from the TFTP Server and updates both as required. Verify the file versions within the *System Setting*s screen.

NOTE
If the firmware files are the same, the firmware will not get updated. If the configuration file name matches the last used configuration file on the access point or if the configuration file versions are the same, the access point configuration will not get updated.

NOTE
The update process is conducted over the LAN or WAN port depending on which Server responds first to the access point's request for an automatic update.

DHCP priorities

The following flowchart indicates the priorities used by the access point when the DHCP server is configured for multiple options.



If the DHCP Server is configured for options 186 and 66 (to assign TFTP Server IP addresses) the access point uses the IP address configured for option 186. Similarly, if the DHCP Server is configured for options 187 and 67 (for the firmware file) the access point uses the file name configured for option 187. If the DHCP Server is configured for embedded and global options, the embedded options take precedence.

Linux - BootP server configuration

See the following sections for information on these BootP server configurations in the Linux environment:

- *BootP options*
- *BootP priorities*

BootP options

This section contains instructions for the automatic update of the access point firmware and configuration file using a BootP Server.

The setup example described in this section includes:

- 1 Brocade Mobility 7131 Series Access Point model access point
- 1 Linux/Unix BOOTP Server
- 1 TFTP Server.

To configure BootP options using a Linux/Unix BootP Server:

1. Set the Linux/Unix BootP Server and access point on the same Ethernet segment.
2. Configure the bootptab file (/etc/bootptab) on the Linux/Unix BootP Server in any one of the formats that follows:

   Using options 186, 187 and 188:

```
AP-7131:ha=00a0f88aa6d8\          < LAN MAC Address>
        :sm=255.255.255.0\        <Subnet Mask>
        :ip=157.235.93.128\       <IP Address>
        :gw=157.235.93.2\         <gateway>
        :T186="157.235.93.250"\   <TFTP Server IP>
        :T187="apfw.bin"\         <Firmware file>
        :T188="cfg.txt":          <Configuration file>
```

   Using options 66, 67 and 129:

```
AP-7131:ha=00a0f88aa6d8\          < LAN MAC Address>
        :sm=255.255.255.0\        <Subnet Mask>
        :ip=157.235.93.128\       <IP Address>
        :gw=157.235.93.2\         <gateway>
        :T66="157.235.93.250"\    <TFTP Server IP>
        :T67="apfw.bin"\          <Firmware file>
        :T129="cfg.txt":          <Configuration file>
```

   Using options sa, bf and 136:

```
AP-7131:ha=00a0f88aa6d8\          < LAN MAC Address>
        :sm=255.255.255.0\        <Subnet Mask>
        :ip=157.235.93.128\       <IP Address>
        :gw=157.235.93.2\         <gateway>
        :sa=157.235.93.250\       <TFTP Server IP>
        :bf=/tftpboot/cfg.txt\    <Configuration file>
        :T136="/tftpboot/":       <TFTP root directory>
```

NOTE
The bf option prefixes a forward slash (/) to the configuration file name. The forward slash may not be supported on Windows based TFTP Servers.

3. Copy the firmware and configuration files to the appropriate directory on the TFTP Server.

   By default, auto update is enabled on the access point (since the LAN Port is a DHCP Client, out-of-the-box auto update support is on the LAN Port).

4. Restart the access point.
5. While the access point boots, verify the access point:
   - Sends a true BootP request.
   - Obtains and applies the expected IP Address from the BootP Server.
   - Downloads both the firmware and configuration files from the TFTP Server and updates them as required. Verify the file versions within the *System Settings* screen.

   Whenever a configuration file is specified, the access point will tftp the config file, parse it and use the firmware file name in the config file.

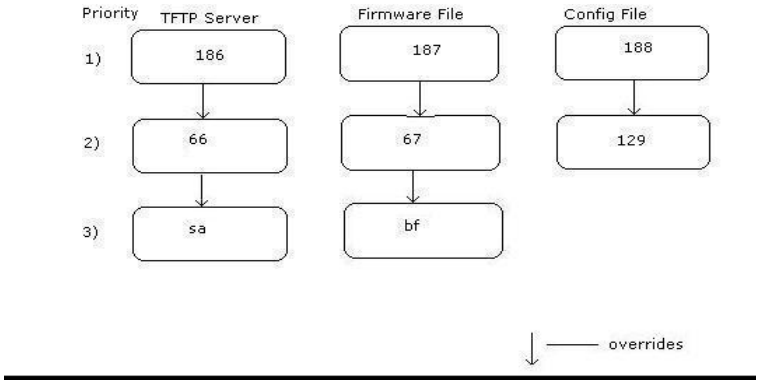
   If T136 is provided by the server, the access point strips off the TFTP root directory from the fully qualified configuration file name to obtain a relative file name. For example, if using bf=/opt/tftpdir/ftp/dist/ap.cfg and T136="/opt/tftpdir", the config file name is ftp/dist/ap.cfg. T136 is only used for this purpose. It is NOT used to append to the config file name or the firmware file name. If T136 is not specified, the access point uses the entire bf field as the config file name.

NOTE
The update process is conducted over the LAN or WAN port depending on which Server responds first to the access point's request for an automatic update.

NOTE
If the firmware files are the same, the firmware will not get updated. If the configuration file name matches the last used configuration file on the access point or if the configuration file versions are the same, the access point configuration will not get updated. The LAN Port needs to be configured as a BootP client. There's no BootP support on the WAN Port. The WAN supports only DHCP.

BootP priorities

The following flowchart displays the priorities used by the access point when the BootP server is configured for multiple options:



If the BootP Server is configured for options 186 and 66 (to assign TFTP server IP addresses) the access point uses the IP address configured for option 186. Similarly, if the BootP Server is configured for options 188 and 129 (for the configuration file) the AP uses the file name configured for option 188.

Configuring an IPSEC tunnel and VPN FAQs

The access point has the capability to create a tunnel between an access point and a VPN endpoint. The access point can also create a tunnel from one access point to another access point.

The following instruction assumes the reader is familiar with basic IPSEC and VPN terminology and technology.

- *Configuring a VPN tunnel between two access points*
- *Configuring a Cisco VPN device*
- *Frequently asked VPN questions*

Configuring a VPN tunnel between two access points

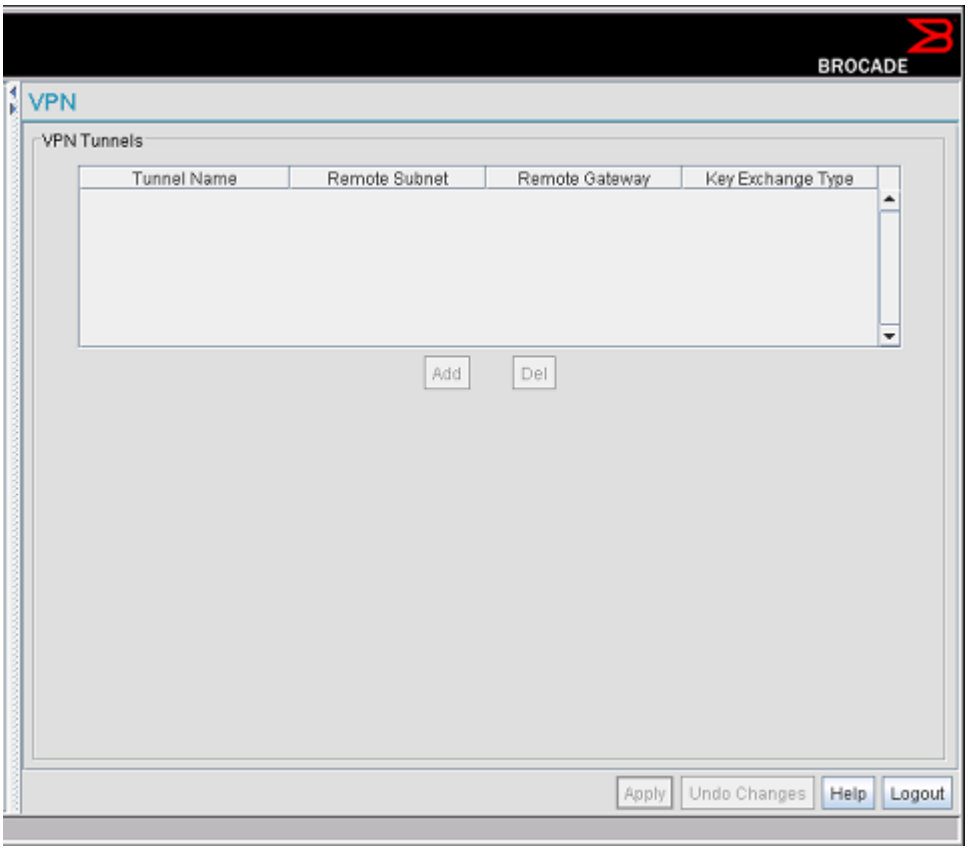
The access point can connect to a non-AP device supporting IPSec, such as a Cisco VPN device - labeled as "Device #2".

For this usage scenario, the following components are required:

- 2 access points (either Brocade Brocade Mobility 7131 Series Access Point or Mobility 5181 access points)
- 1 PC on each side of the access point's LAN.

To configure a VPN tunnel between two access points:

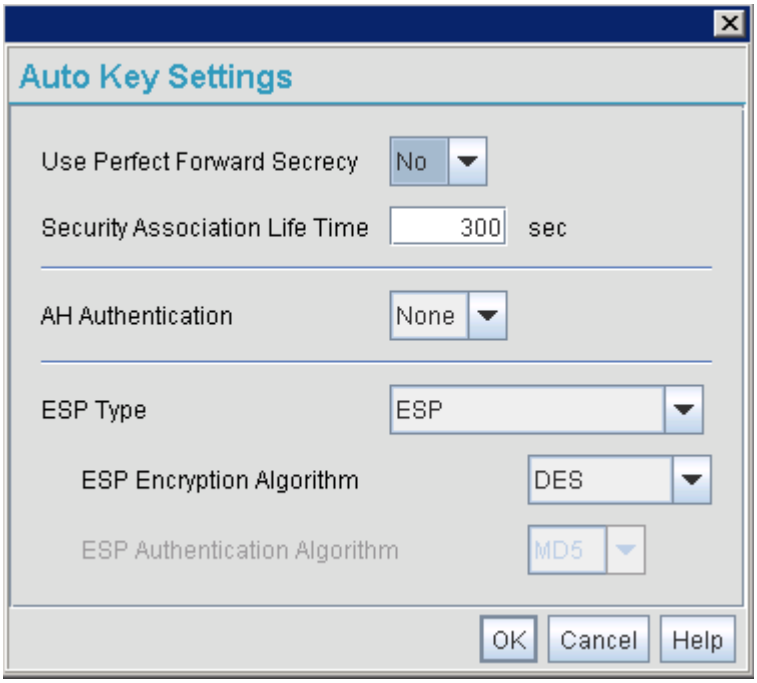
1. Ensure the WAN ports are connected via the internet.
2. On access point #1, select *WAN -> VPN* from the main menu tree.
3. Click *Add* to add the tunnel to the list.
4. Enter a tunnel name (tunnel names do not need to match).



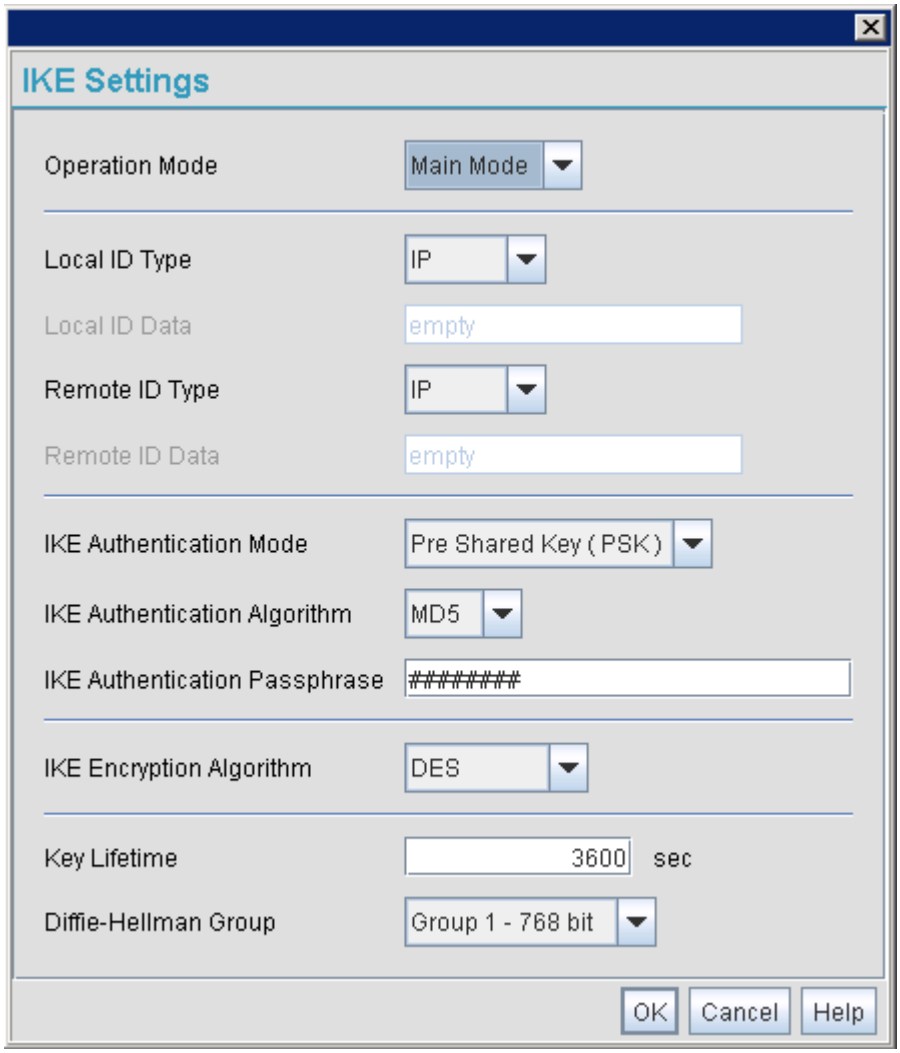
5. Enter the WAN port IP address of AP #1 for the *Local WAN IP*.
6. Within the *Remote Subnet* and *Remote Subnet Mask* fields, enter the LAN IP subnet and mask of AP #2 /Device #2.
7. Enter the WAN port IP address of AP #2/ Device #2 for a *Remote Gateway*.
8. Click *Apply* to save the changes.

NOTE
For this example, Auto IKE Key Exchange is used. Any key exchange can be used, depending on the security needed, as long as both devices on each end of the tunnel are configured exactly the same.

9. Select the *Auto (IKE) Key Exchange* radio button.
10. Select the *Auto Key Settings* button.



11. For the ESP Type, select *ESP with Authentication* and use *AES 128-bit* as the ESP encryption algorithm and *MD5* as the authentication algorithm. Click *OK*.
12. Select the *IKE Setting*s button.



13. Select *Pre Shared Key (PSK)* from the IKE Authentication Mode drop-down menu.
14. Enter a *Passphrase*. Passphrases must match on both VPN devices.

NOTE
Ensure the IKE authentication Passphrase is the same as the Pre-shared key on the Cisco PIX device.

15. Select *AES 128-bit* as the IKE Encryption Algorithm.
16. Select *Group 2* as the Diffie -Hellman Group. Click *OK*. This will take you back to the VPN screen.
17. Click *Apply* to make the changes
18. Check the *VPN Status* screen. Notice the status displays "NOT_ACTIVE". This screen automatically refreshes to get the current status of the VPN tunnel. Once the tunnel is active, the IKE_STATE changes from NOT_CONNECTED to SA_MATURE.

19. On access point #2/ Device #2, repeat the same procedure. However, replace access point #2 information with access point #1 information.
20. Once both tunnels are established, ping each side of the tunnel to ensure connectivity.

Configuring a Cisco VPN device

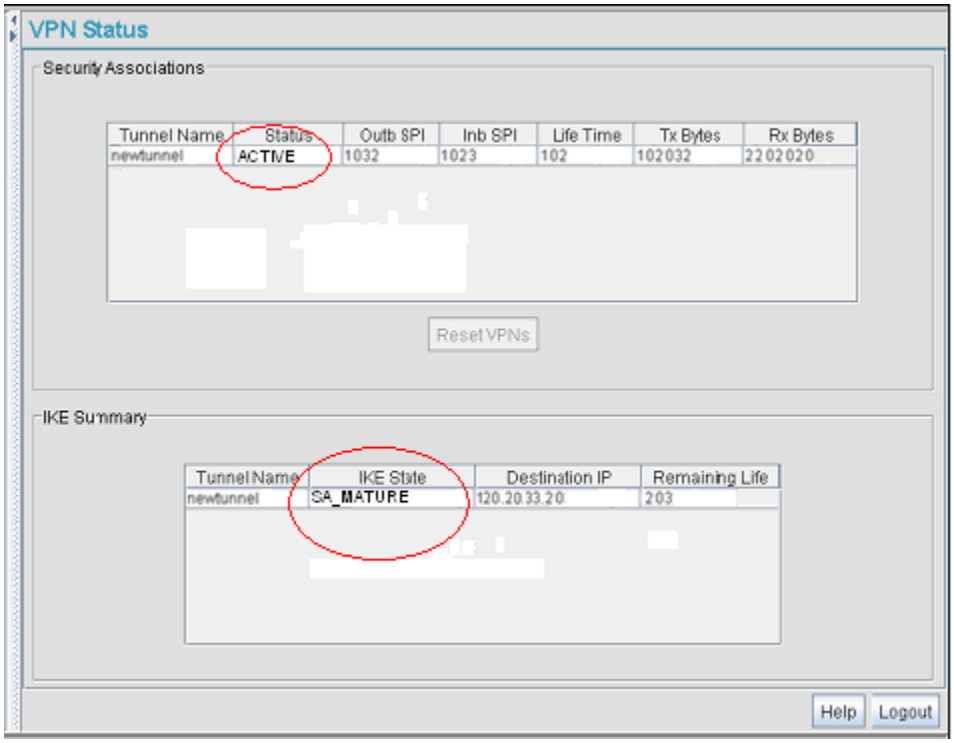
This section includes general instructions for configuring a Cisco PIX Firewall 506 series device.

For the usage scenario described in this section, you will require the following:

- 1 Cisco VPN device
- 1 PC connected to the LAN side of the access point and the Cisco PIX.

NOTE
The Cisco PIX device configuration should match the access point VPN configuration in terms of Local WAN IP (PIX WAN), Remote WAN Gateway (access point WAN IP), Remote Subnet (access point LAN Subnet), and the Remote Subnet Mask. The Auto Key Settings and the IKE Settings on the Cisco PIX should match the access point Key and IKE settings.

Below is how the access point VPN Status screen should look if the entire configuration is setup correctly once the VPN tunnel is active. The status field should display "ACTIVE".



Frequently asked VPN questions

The following are common questions that arise when configuring a VPN tunnel.

- **Question 1: Does the access point IPSec tunnel support multiple subnets on the other end of a VPN concentrator?**

  Yes. The access point can access multiple subnets on the other end of the VPN Concentrator from the access point's Local LAN Subnet by:

  - Creating multiple VPN Tunnels. The AP supports a maximum of 25 tunnels.
  - When using the Remote Subnet IP Address with an appropriate subnet mask, the AP can access multiple subnets on the remote end.

  For example: If creating a tunnel using 192.168.0.0/16 for the Remote Subnet IP address, the following subnets could be accessed:

  192.168.1.x

  192.168.2.x

  192.168.3.x, etc

- **Question 2: Even if a wildcard entry of "0.0.0.0" is entered in the Remote Subnet field in the VPN configuration page, can the AP access multiple subnets on the other end of a VPN concentrator for the APs LAN/WAN side?**

  No. Using a "0.0.0.0" wildcard is an unsupported configuration. In order to access multiple subnets, the steps in Question #1 must be followed.

- **Question 3: Can the AP be accessed via its LAN interface of AP#1 from the local subnet of AP#2 and vice versa?**

  Yes.

- **Question 4: Will the default "Manual Key Exchange" settings work without making any changes?**

  No. Changes need to be made. Enter Inbound and Outbound ESP Encryption keys on both APs. Each one should be of 16 Hex characters (depending on the encryption or authentication scheme used). The VPN tunnel can be established only when these corresponding keys match. Ensure the Inbound/Outbound SPI and ESP Authentication Keys have been properly specified.

- **Question 5: Can an IPSec tunnel over a PPPoE connection be established - such as a PPPoE enabled DSL link?**

  Yes. The access point supports tunneling when using a PPPoE username and password.

- **Question 6: Can I setup an access point so clients can access both the WAN normally and only use the VPN when talking to specific networks?**

  Yes. Only packets that match the VPN Tunnel Settings will be sent through the VPN tunnel. All other packets will be handled by whatever firewall rules are set.

- **Question 7: How do I specify which certificates to use for an IKE policy from the access point certificate manager?**

  When generating a certificate to use with IKE, use one of the following fields: *IP address*, *Domain Name*, or *Email* address. Also, make sure you are using NTP when attempting to use the certificate manager. Certificates are time sensitive.

  Configure the following on the *IKE Settings* page:

  Local ID type refers to the way that IKE selects a local certificate to use.

- *IP* - tries the match the local WAN IP to the IP addresses specified in a local certificate.
- *FQDN* - tries to match the user entered local ID data string to the domain name field of the certificate.
- *UFQDN* - tries to match the user entered local ID data string to the email address field of the certificate.

Remote ID type refers to the way you identify an incoming certificate as being associated with the remote side.

- *IP* - tries the match the remote gateway IP to the IP addresses specified in the received certificate.
- *FQDN* - tries to match the user entered remote ID data string to the domain name field of the received certificate.
- *UFQDN* - tries to match the user entered remote ID data string to the email address field of the received certificate.

- **Question 8: I am using a direct cable connection between my two VPN gateways for testing and cannot get a tunnel established, yet it works when I set them up across another network or router. Why?**

  The packet processing architecture of the access point VPN solution requires the WAN default gateway to work properly. When connecting two gateways directly, you don't need a default gateway when the two addresses are on the same subnet. As a workaround, point the access point's WAN default gateway to be the other VPN gateway and vice-versa.

- **Question 9: I have setup my tunnel and the status still says 'Not Connected'. What should I do now?**

  VPN tunnels are negotiated on an "as-needed" basis. If you have not sent any traffic between the two subnets, the tunnel will not get established. Once a packet is sent between the two subnets, the VPN tunnel setup occurs.

- **Question 10: I still can't get my tunnel to work after attempting to initiate traffic between the two subnets. What now?**

Try the following troubleshooting tips:

- Verify you can ping each of the remote Gateway IP addresses from clients on either side. Failed pings can indicate general network connection problems.
- Pinging the internal gateway address of the remote subnet should run the ping through the tunnel as well. Allowing you to test, even if there are no clients on the remote end.
- Try re-setting the shared secret password on the access point.

- **Question 11: My tunnel works fine when I use the LAN-WAN Access page to configure my firewall. Now that I use Advanced LAN Access, my VPN stops working. What am I doing wrong?**

  VPN requires certain packets to be passed through the firewall. Subnet Access automatically inserts these rules for you when you do VPN. Advanced Subnet Access requires these rules to be in effect for each tunnel.

  - An 'allow' inbound rule.

Scr	<Remote Subnet IP range>
Dst	<Local Subnet IP range>
Transport	ANY
Scr port	1:65535
Dst port	1:65535
Rev NAT	None

  - An 'allow' outbound rule.

Scr	<Local Subnet IP range>
Dst	<Remote Subnet IP range>
Transport	ANY
Scr port	1:65535
Dst port	1:65535
NAT	None

  - For IKE, an 'allow' inbound rule.

Scr	<Remote Subnet IP range>
Dst	<WAN IP address>
Transport	UDP
Scr port	1:65535
Dst port	500
Rev NAT	None

  These three rules should be configured above all other rules (default or user defined). When Advanced LAN Access is used, certain inbound/outbound rules need to be configured to control incoming/outgoing packet flow for IPSec to work properly (with Advanced LAN Access). These rules should be configured first before other rules are configured.

- **Question 12: Do I need to add any special routes on the access point to get my VPN tunnel to work?**

No. However, clients could need extra routing information. Clients on the local LAN side should either use the access point as their gateway or have a route entry tell them to use the access point as the gateway to reach the remote subnet.

B Configuring an IPSEC tunnel and VPN FAQs