Aruba Mesh Router
Web-based
Configuration Guide
v4.2
Copyright
© 2011 Aruba Networks, Inc. All rights reserved.
Aruba Networks® is a registered trademark, and Aruba The Mobile Edge Company is a trademark of Aruba Networks, Inc.
Specifications are subject to change without notice.

Trademarks
Sygate On-Demand Agent and Sygate Enforcer are trademarks of Sygate Technologies.
All other trademarks or registered trademarks are the property of their respective holders.

Legal Notice
The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks.

Warranty
This hardware product is protected by the standard Aruba warranty of one year parts/labor.
For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.
Altering this device (such as repainting it) voids the warranty.
Table of Contents

CHAPTER 1 ABOUT THIS GUIDE .................................................................................................................. 6
  1.1. SCOPE ................................................................................................................................................ 6
  1.2. AUDIENCE ......................................................................................................................................... 6
  1.3. RELATED DOCUMENTS .................................................................................................................... 6

CHAPTER 2 WEB CONFIGURATION OVERVIEW ....................................................................................... 7
  2.1. GETTING STARTED ............................................................................................................................. 7
    2.1.1. Logging into the Web-based Management Interface ................................................................. 7
    2.1.2. WMI Basics ................................................................................................................................... 8

CHAPTER 3 BASIC SETTINGS ..................................................................................................................... 9
  3.1. BASIC SETTINGS ................................................................................................................................ 9

CHAPTER 4 CONFIGURING ETHERNET INTERFACE .................................................................................. 11
  4.1. CONFIGURING ETHERNET INTERFACE BASIC .............................................................................. 11
  4.2. CONFIGURING ETHERNET INTERFACE VLAN ............................................................................. 12
  4.3. CONFIGURING ETHERNET INTERFACE IPv4 ................................................................................. 13
  4.4. CONFIGURING ETHERNET INTERFACE QoS ................................................................................. 14
  4.5. ETHERNET INTERFACE ADVANCED CONFIGURATION ................................................................. 15

CHAPTER 5 WIRELESS SETTINGS ............................................................................................................. 16
  5.1. RADIO INTERFACES CONFIGURATION ............................................................................................ 16
    5.1.1. Configuring Radio Interface Basic .............................................................................................. 16
    5.1.2. Configuring Radio Interface Backhaul ....................................................................................... 18
    5.1.3. Configuring Radio Interface Advanced Settings .................................................................. 19
  5.2. BSS INTERFACES CONFIGURATION .............................................................................................. 21
    5.2.1. Creating a New BSS/Entering an Existing BSS ........................................................................ 21
    5.2.2. Configuring a New Created BSS/an Existing BSS ................................................................ 24
    5.2.3. Configuring BSS Security ........................................................................................................... 25
    5.2.4. Configuring BSS VLAN .............................................................................................................. 29
    5.2.5. Configuring BSS IPv4 ............................................................................................................... 29
    5.2.6. Configuring BSS QoS .................................................................................................................. 30
    5.2.7. Configuring BSS Advanced Settings ....................................................................................... 31
    5.2.8. Deleting a BSS ............................................................................................................................ 33
  5.3. MESH CONFIGURATION .................................................................................................................... 33
    5.3.1. Configuring Mesh Basic .............................................................................................................. 33
    5.3.2. Configuring Mesh Security ........................................................................................................ 34
    5.3.3. Configuring Mesh ACL List ...................................................................................................... 37
    5.3.4. Configuring Preferred Links .................................................................................................... 38
    5.3.5. Configuring Mesh Advanced Settings ..................................................................................... 40
  5.4. CLIENT MODE CONNECTION CONFIGURATION ............................................................................. 41
    5.4.1. Creating a New/Entering an Existing Client-mode Connection ................................................. 42
    5.4.2. Configuring a Client-mode Connection (STA) ....................................................................... 44
    5.4.3. Configuring Client-mode Connection Security ....................................................................... 45
    5.4.4. Configuring Client-mode Connection VLAN .......................................................................... 48
    5.4.5. Configuring Client-mode Connection IPv4 ............................................................................. 49
    5.4.6. Configuring Client-mode Connection Scanning ...................................................................... 50
    5.4.7. Configuring Client-mode Connection Advanced Settings .................................................... 51

CHAPTER 6 NETWORK SETTINGS ............................................................................................................... 53
6.1. CONFIGURING ROUTING ........................................................................................................ 53
  6.1.1. Routing Table Configuration .............................................................................................. 53
  6.1.2. Adding an IPv4 Static Route ................................................................................................ 54
  6.1.3. Deleting an IPv4 Static Route ............................................................................................. 55
  6.1.4. View IPv4 System Routing Table ...................................................................................... 56
  6.1.5. OSPF Configuration Page ................................................................................................ 58
  6.1.6. Adding OSPF Network ....................................................................................................... 59
  6.1.7. Deleting OSPF Network .................................................................................................... 59
  6.1.8. Adding Summary Address ............................................................................................... 60
  6.1.9. Deleting Summary Address ............................................................................................. 61
  6.1.10. AWR Configuration Page ................................................................................................ 62
  6.1.11. Multicast Configuration Page .......................................................................................... 64
6.2. CONFIGURING DHCP ............................................................................................................. 64
  6.2.1. DHCP Server Configuration .............................................................................................. 65
  6.2.2. Adding a New DHCP Pool .................................................................................................. 65
  6.2.3. Configuring the New DHCP Pool ...................................................................................... 66
  6.2.4. Deleting an Existing DHCP Pool ...................................................................................... 66
  6.2.5. Adding an IP Address Range ............................................................................................ 68
  6.2.6. Deleting an IP Address Range .......................................................................................... 69
  6.2.7. Adding an Fixed IP Assignment ......................................................................................... 70
  6.2.8. Deleting an Existing Fixed Assignment ............................................................................ 70
  6.2.9. Deleting DHCP Option ..................................................................................................... 71
  6.2.10. DHCP Relay Configuration ............................................................................................. 72
  6.2.11. Deleting DHCP Relay ..................................................................................................... 72
6.3. CONFIGURING VLAN ............................................................................................................ 73
  6.3.1. VLAN Configuration .......................................................................................................... 73
  6.3.2. Adding VLAN Interface .................................................................................................... 74
  6.3.3. Configuring VLAN Basic Settings .................................................................................... 75
  6.3.4. Configuring VLAN Interface IPv4 ................................................................................... 76
  6.3.5. VLAN Interface Advanced Configuration .................................................................... 78
  6.3.6. Deleting a VLAN Interface ............................................................................................... 78
6.4. CONFIGURING LOOPBACK ................................................................................................... 79
  6.4.1. Loopback Configuration .................................................................................................... 79
  6.4.2. Adding a Loopback Interface ............................................................................................ 80
  6.4.3. Deleting an Existing Loopback Interface .......................................................................... 82
6.5. CONFIGURING NTP .............................................................................................................. 82
   6.5.1. NTP Configuration ............................................................................................................ 82

CHAPTER 7  CONFIGURING SERVICES .................................................................................. 84
  7.1. MOBILITY ............................................................................................................................. 84
  7.2. VPLM .................................................................................................................................... 84
  7.3. AUTO RECOVERY ................................................................................................................ 85
  7.4. AVT ....................................................................................................................................... 86
   7.4.1. Adding an Ingress IP ........................................................................................................ 87
   7.4.2. Deleting an Existing Ingress IP ....................................................................................... 87

CHAPTER 8  SNMP CONFIGURATION ..................................................................................... 89
  8.1. DEVICE INFO ....................................................................................................................... 89
  8.2. SNMP COMMUNITIES ......................................................................................................... 90
   8.2.1. Configuring SNMP Communities .................................................................................... 90
   8.2.2. Adding a New Community .............................................................................................. 90
   8.2.3. Deleting a Community .................................................................................................... 91
  8.3. SNMP TRAP RECEIVERS .................................................................................................... 91
8.3.1. Configuring SNMP Trap Receivers ................................................................. 92
8.3.2. Adding a New Receiver .................................................................................. 92
8.3.3. Deleting a Trap Receiver .............................................................................. 93
8.4. SNMP v3 USERS ............................................................................................. 93
  8.4.1. Configuring SNMPv3 Users ........................................................................ 93
  8.4.2. Adding a New v3 User ................................................................................ 94
  8.4.3. Deleting an SNMPv3 User .......................................................................... 95

CHAPTER 9  SYSLOG CONFIGURATION ................................................................... 96
  9.1. CONFIGURING SYSLOG CLIENT .................................................................... 96
  9.2. REMOTE SYSLOG SERVICE ......................................................................... 96
  9.3. ADDING A SYSLOG SERVER ......................................................................... 97
  9.4. DELETING A SYSLOG SERVER ..................................................................... 97
  9.5. ADDING FACILITY AND SEVERITY LEVEL .................................................. 98
  9.6. DELETING FACILITY AND SEVERITY ......................................................... 98

CHAPTER 10  TROUBLESHOOTING ....................................................................... 99
  10.1. TOOLS ......................................................................................................... 99
  10.2. LOGS ........................................................................................................ 101
      10.2.1. Viewing Logs ....................................................................................... 102
      10.2.2. Downloading Logs ............................................................................. 102

CHAPTER 11  MAINTENANCE ................................................................................. 104
  11.1. UPGRADE .................................................................................................. 104
  11.2. IMPORT/EXPORT CONFIGURATION ......................................................... 105
      11.2.1. Export Configuration .......................................................................... 105
      11.2.2. Import Configuration ......................................................................... 106
  11.3. REBOOT .................................................................................................... 107
  11.4. FACTORY RESET ....................................................................................... 108
  11.5. CHANGE PASSWORD .................................................................................. 109
Chapter 1 About this Guide

This chapter covers the following topics:

- Scope
- Audience
- Related Documents

1.1. Scope

This document provides instructions and examples for the configuration of Aruba wireless mesh routers through the Web-based Management Interface (WMI), and the document’s scope is limited to such. For information on wireless mesh routers’ Command Line Interface (CLI) or other subjects, please refer to the Aruba Mesh Router CLI Configuration Guide and/or related documents.

Note: All screen shots displayed in this document are captured using an MSR2000 and are for demonstration purposes only. The exact screen output may vary depending on the model of the router used as well as your browser and system settings.

1.2. Audience

This document is intended for a system/IT or network administrator who is responsible for configuring or maintaining wireless mesh routers. This guide assumes the user has knowledge of wireless, wired, Layer-2, and Layer-3 networking technologies, and is comfortable with the use of an internet browser.

1.3. Related Documents

For more information about the wireless mesh routers, please refer to the following documents:

- Aruba Mesh Router CLI Configuration Guide
Chapter 2  Web Configuration Overview

The Web-based Management Interface (WMI) allows administrators to manage wireless mesh routers from a remote location conveniently and efficiently in a graphical interface accessible from most modern internet browsers, including Microsoft Internet Explorer or Mozilla Firefox.

The basic software requirement for the web-interface is:
- Web Browser: Internet Explorer 5.5 and above with Javascript enabled
- Optimal Resolution: 1024 X 768 and above

2.1. Getting Started

This chapter introduces the basic functionality and layout of the Web-based Management Interface. It contains the following topics:
- Logging into the Web-based Management Interface
- WMI Basics

2.1.1. Logging into the Web-based Management Interface

To log in the web interface of a MESH ROUTER product, input the wireless mesh router’s IP address, such as X.X.X.X in the web browser address.

If the device is in factory default state, there are two methods to access the device using web interface. One method is to configure Management IP address on the interface vlan 1, which is configured to obtain IP address using DHCP in factory default. You need to use the USB console to set a static IP address on the interface VLAN 1. After this, the WMI can be accessed by the management IP address.

If the device is in factory default state, the wireless connection is another method of accessing the device. **Do not connect anything to the device's Ethernet port and then power it on.** The default SSID of the BSS of the device is a **hidden** SSID “ArubaDefault”. Because the default SSID is hidden and there is no DHCP service, a wireless laptop has to be manually configured to associate to this default BSS on the device using a static IP address on the 192.168.216.0/24 network. After it finishes association, the WMI should be accessible at http://192.168.216.1.

After connecting to the WMI, a pop-up dialog box would appear and request a username and password.

Enter the default username ‘root’ and password ‘public’ in the pop-up dialog box. After the successful authentication, the home page for WMI would appear.

![Figure 2-1 Logging into Web Management Interface (WMI)](image)
Note: During the log-in process, an option such as “Remember my password” may appear. If this option is enabled, one would not be required to re-enter the username or password when accessing the WMI next time. Please use this option with care.

After successfully logging into the wireless mesh router web management interface, one is lead directly to the System Information as shown in figure below.

![Web Management Interface Home Page](image)

**Figure 2-2 Web Management Interface Home Page**

**2.1.2. WMI Basics**

The WMI is composed of three components: the title banner (top), the menu tree (left), the configuration area (right), and the locale selector (bottom) as shown in figure below. The title banner shows the model name and the company Logo; the menu tree provides clear, hierarchical navigation to the various configuration areas. Clicking on one of the choices in the menu tree would cause the area on the right to display the specific configurable settings for that menu choice. The locale selector on the bottom allows users to change the current language and locale-specific style used by the WMI. Currently, US English and PRC Chinese are supported.
Chapter 3  Basic Settings

This chapter describes the basic settings to a wireless mesh router.

3.1. Basic Settings

Clicking on the menu item “Basic Settings” leads the user to the basic settings area which allows the user to retrieve and edit configuration settings which take effect across the wireless mesh router. An example screen is shown in figure below.

![Basic Configuration Screen](image)

Figure 3-1 Basic Configuration Screen

The table below describes basic settings configuration:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory domain code</td>
<td>Selects the regulatory domain code.</td>
<td>United States</td>
</tr>
<tr>
<td>Installation Type</td>
<td>Selects the installation type: Indoor or Outdoor</td>
<td>For MSR1200, the default value is Indoor; for MSR2000, MSR4000 and MST2000, the default is Outdoor</td>
</tr>
<tr>
<td>Hostname</td>
<td>Allows users to set the hostname of the MESH ROUTER product. Input a character string as the hostname. The character string shall include up to 32 characters</td>
<td>The name of MESH ROUTER product</td>
</tr>
<tr>
<td><strong>Location Info</strong></td>
<td>Enter the longitude, latitude and altitude value of the device.</td>
<td>N/A</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----</td>
</tr>
</tbody>
</table>
| **Management IP Address** | 1) Use DHCP: Enter vendor ID, configure DHCP Option 60 (up to 64 characters)  
2) Static IP/mask: manually configure static IP/mask, format A.B.C.D/M  
3) Do not configure: not configure IP address | N/A |
| **Telnet Access** | Whether enable Telnet access | Disabled |

**Saving Configuration for the Basic Settings**

After editing the values for the above fields, one may save the changes by clicking the "Apply Changes" button.
Chapter 4  Configuring Ethernet Interface

Each wireless mesh router contains one physical Ethernet interface used to connect with a wired network or device. This chapter describes how the Ethernet interface is configured using Web-based Management.

4.1. Configuring Ethernet Interface Basic

Click the “Wired Settings” button in the menu to expand the sub-menu. Then, click the “Ethernet” button in the sub-menu to enter the Ethernet interface configuration page.

Table below describes the settings for the Ethernet interface basic.
### Ethernet Interface Basic Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Describe the Ethernet interface</td>
<td>N/A</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Can be up or down. If down, this interface would be inactive (shutdown).</td>
<td>Up</td>
</tr>
</tbody>
</table>

### Saving Configuration for the Ethernet Interface Basic

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

### 4.2. Configuring Ethernet Interface VLAN

To configure the Ethernet interface VLAN, click the “VLAN” tab to enter the VLAN configuration page.

![Ethernet Interface VLAN Configuration Screen](image)

Table below describes the settings for the Ethernet interface VLAN.

### Ethernet Interface VLAN Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
</table>
| VLAN        | 1) No VLAN; 2) Access VLAN, configure the Ethernet interface as VLAN access port, and enter VLAN access ID; 3) Trunk VLAN, configure the Ethernet interface as Trunk VLAN port  
Note: VLAN configuration is mutually exclusive with IP address configuration. If want to configure VLAN, please choose “Do not configure” in the IP address configuration section. | Trunk VLAN 1 |
Native VLAN ID | When the Ethernet interface acts as Trunk port, configure its local VLAN. | 1
VPLM Site ID | Configure a manual defined Ethernet domain ID. Used by VPLM for handling loop problem. | N/A

**Saving Configuration for the Ethernet Interface VLAN**

To save the configuration after editing the above settings, click the "Apply Changes" button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**Note:** Change the VLAN setting may make the router inaccessible via Ethernet interface. Be careful to change this setting.

### 4.3. Configuring Ethernet Interface IPv4

To configure the Ethernet interface IPv4, click the “IPv4” tab to enter the IPv4 edit page.

**Table 4-3 Ethernet Interface IPv4 Configuration Fields**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
</table>
| IP Address    | 1) Use DHCP: Enter manufacturer ID, configure DHCP Option 60 (up to 64 characters)  
                 2) Static IP/mask: manually configure static IP/mask, format A.B.C.D/M  
                 3) Do not configure: not configure IP address                  | Do not configure         |
Management Interface

Yes: Configure the Ethernet interface as management interface.
No: Cancel the configuration of the Ethernet interface as management interface.

Router-ID Interface

Yes: Configure the Ethernet interface as Router-ID interface.
No: Cancel the configuration of the Ethernet interface as Router-ID interface.

Layer-3 Service

Configure the layer-3 working mode at this interface, including 4 options:
No layer-3 service: Not enable layer-3 mode;
Layer-3 access: Enable layer-3 access mode;
Layer-3 gateway: Enable layer-3 gateway mode;
Layer-3 backhaul: Enable layer-3 backhaul mode;

DHCP Server/Relay

1) Disabled
2) DHCP Server
   DHCP Pool: configure DHCP address pool
3) DHCP Relay
   Option 82 Circuit ID configuration

Saving Configuration for the Ethernet Interface IPv4

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**Note:** Change IP address from “Static” or “Use DHCP” to “Do not configure” may make the router inaccessible via Ethernet interface. Be careful to change this setting.

4.4. Configuring Ethernet Interface QoS

To configure the Ethernet interface QoS, click the “QoS” tab to enter the QoS edit page.

**Table 4-4 Ethernet Interface QoS Configuration Fields**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Category Mapping</td>
<td>Configure the mapping relations of QoS priorities</td>
<td>None</td>
</tr>
</tbody>
</table>

**Saving Configuration for the Ethernet Interface QoS**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

### 4.5. Ethernet Interface Advanced Configuration

To configure the Ethernet interface advanced features, click the “Advanced” tab to enter the Advanced edit page.

![Figure 4-6 Ethernet Interface Advanced Configuration Screen](image)

Table below describes the settings for the Ethernet interface advanced features.

**Table 4-5 Ethernet Interface Advanced Configuration Fields**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU (Maximum Transmission Unit)</td>
<td>Maximum transmission unit in bytes; controls how Layer-3 packets would be fragmented when they are sent through this interface. Range: 256-1500</td>
<td>1500</td>
</tr>
<tr>
<td>Link Auto-negotiate</td>
<td>Whether enable link auto negotiation mode at the Ethernet interface</td>
<td>Enable</td>
</tr>
<tr>
<td>Link Speed/Duplex</td>
<td>Set the Ethernet interface at force speed and duplex mode. 10/100/1000 means the Ethernet interface speed is set at 10Mbps/100Mbps/1000Mbps; full</td>
<td>half means the duplex mode of Ethernet interface is full/half duplex</td>
</tr>
</tbody>
</table>

**Saving Configuration for the Ethernet Interface Advanced**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.
Chapter 5  Wireless Settings

Dot11Radio interfaces on the wireless mesh routers are used for connecting with 802.11-compatible client devices. This chapter contains the following content:

- Radio Interface Configuration
- BSS Interface Configuration
- Mesh Configuration
- Client Mode Configuration

5.1. Radio Interfaces Configuration

Click the "Radio" item in the "Wireless Settings" sub-menu to enter the Radio interface configuration page. The resulting page displays the router’s physical radio interfaces in a list, as shown in figure below.

![Radio Interfaces Screen](image)

5.1.1. Configuring Radio Interface Basic

To view or change the configuration for a particular radio, click the name of the radio interface (i.e. "Radio 0" in Figure above). The resulting page displays the basic configuration settings and allows them to be changed.
Table below describes the settings for radio interface basic.

### Table 5-1 Radio Interface Basic Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Index</td>
<td>0, means Radio0 interface</td>
<td>For radio0, the default Mode/Channel is 802.11na 40Mhz Plus, 184 (4.92GHz, 40Mhz Bandwidth); for radio1, the default is 802.11g, 1(2.412GHz, 20Mhz Bandwidth)</td>
</tr>
<tr>
<td>Mode/Channel</td>
<td>Configure the wireless settings of this radio interface manually.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mode: a, b, g or g-only, na,ng,na-ht40plus,na-ht40minus,ng-ht40plus,ng-ht40minus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a: Use 802.11a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b: Use 802.11b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g: Use 802.11g; compatible with 802.11b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g-only: Use 802.11 g-only, don’t compatible with 802.11b;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>na: Use 802.11na and the bandwidth of each channel is 20MHz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ng: Use 802.11ng and the bandwidth of each channel is 20MHz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>na-ht40plus: Use 802.11na, combining two neighboring 20MHz channels into one 40MHz channel. The control channel is the configured channel, and the frequency of the extension channel is higher than that of the control channel.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>na-ht40minus: Use 802.11na, combining two neighboring 20MHz channels into one 40MHz channel. The control channel is the configured channel, and the frequency of the extension channel is lower than that of the master channel.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ng-ht40plus: Use 802.11ng, combining two neighboring</td>
<td></td>
</tr>
</tbody>
</table>
20MHz channels into one 40MHz channel. The control channel is the configured channel, and the frequency of the extension channel is higher than that of the control channel.

ng-ht40minus: Use 802.11ng, combining two neighboring 20MHz channels into one 40MHz channel. The control channel is the configured channel, and the frequency of the extension channel is lower than that of the control channel.

Note: g mode is compatible with 802.11b mode; g-only mode is not compatible with the 802.11b mode. ng, ng-ht40plus, ng-ht40minus mode is compatible with 802.11g; na,na-ht40plus,na-ht40minus mode is compatible with 802.11a.

By default, the MSR/MSA only support 802.11b/g, other modes need license.

Channel: Channel setting is optional. A channel number must be allowed by the device’s country/regulatory domain code. China supports Channel 1-13 in 2.4G. If not configured, the system will choose the first legal channel number of the country/regulatory domain code.

Antenna Gain: Configure antenna gain, the range of value is 0-255. This parameter is usually set at deployment time and shall be changed with caution.

Tx Power: Configure Radio’s Tx power in dbm. The maximum parameter that can be configured is determined by the Tx power of the radio interface. 0 means restore Radio’s Tx power to the default. This parameter shall be changed with caution.

Admin Status: Can be up or down. If down, this interface would be inactive (shutdown). If up, this interface would be active.

Saving Configuration for the Radio Interface Basic

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

5.1.2. Configuring Radio Interface Backhaul

Click the “Backhaul” tab to enter the Backhaul configuration page.
Table below describes the settings for Radio interface Backhaul Parameters.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Index</td>
<td>0, means Radio0 interface</td>
<td>N/A</td>
</tr>
<tr>
<td>Auto WDS Meshing</td>
<td>Enabled or disable Auto WDS Meshing</td>
<td>For radio 0, the default is Disabled; for radio 1, the default is Enabled</td>
</tr>
<tr>
<td>Max Allowed Links</td>
<td>Configure the maximum allowed links (1-6) on this radio interface</td>
<td>1</td>
</tr>
</tbody>
</table>

Saving Configuration for the Radio Interface Backhaul

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

5.1.3. Configuring Radio Interface Advanced Settings

Click the “Advanced” tab to enter the Advanced configuration page.
Table below describes the settings for Radio interface Advanced features.

**Table 5-3 Radio Interface Advanced Configuration Fields**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Index</td>
<td>0, means Radio0 interface</td>
<td>N/A</td>
</tr>
<tr>
<td>Channel Policy</td>
<td>Configure channel policy of radio interface.</td>
<td>Manual</td>
</tr>
<tr>
<td>Channel Selection Interval (m)</td>
<td>Only valid under auto channel selection mode, the valid value is 1-6000 minutes or 0 as no repeat selection.</td>
<td>0</td>
</tr>
<tr>
<td>Channel List</td>
<td>Configure the working frequency and channel list of the Radio interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>Max Neighbor Distance</td>
<td>Configure the maximum distance between two neighbor nodes, value from 1 to 50000 meters, 0 for unset.</td>
<td>0</td>
</tr>
<tr>
<td>CTS Protection</td>
<td>Enable/disable CTS protection for handling of a mix of 802.11b and 802.11g clients.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>Configure the milliseconds between each time of sending beacon from this radio interface (100-1000 milliseconds)</td>
<td>100</td>
</tr>
</tbody>
</table>

*This parameter is usually set at deployment time and rarely needs to change.*
Preamble Mode | Preamble: part of the packet head, including the information needed when AP and client receiving or sending packet. Short: to improve throughput. Long: to compatible with the client that only support long preamble. | Long
---|---|---
Short GI | This setting is used to enable the short interval feature of the radio interface under 802.11n mode (needs license). If the multipath effect is not obvious, this setting can adjust the Tx interval of signals from 800ns to 400ns, improving the throughput. Note: If the multipath effect is obvious, it's not recommended to use this setting. | Disabled

Saving Configuration for the Radio Interface Advanced

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

5.2. BSS Interfaces Configuration

Click “Wireless Settings” > “BSS” listed in the main menu tree. The resulting page shows the configuration and status of all BSSs on the device.

![Figure 5-5 BSS List Page](image)

In this page, users could create a new BSS as well as configure or delete an existing BSS.

5.2.1. Creating a New BSS/Entering an Existing BSS

To create a new BSS, click the “Create New BSS” button in the BSS list page. The “Create New BSS” page appears.
Select radio interface and BSS ID from the drop-down menu and click “Create New BSS” button to enter BSS configuration page; click “Cancel Changes” button to discard any changes and return to the previous page.

After clicking “Create New BSS” button, the BSS basic configuration page for the new created BSS will appear, as shown in figure below:

![Figure 5-6 Creating a New BSS Page](image)

To enter an existing BSS, click its BSS Name to enter the BSS configuration page.

![Figure 5-7 Basic Configuration Screen for a New Created BSS](image)

To enter an existing BSS, click its BSS Name to enter the BSS configuration page.
Figure 5-8 Entering an Existing BSS Page

Figure 5-9 Basic Configuration Screen for an Existing BSS
5.2.2. Configuring a New Created BSS/an Existing BSS

To configure a new created BSS/an existing BSS, enter the BSS configuration page as stated above.

![Figure 5-10 BSS Basic Configuration Screen](image)

Table below describes the BSS basic settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>SSID</td>
<td>The 802.11 SSID for this BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>Hide SSID</td>
<td>Enable: not broadcast SSID. Clients can't scan out the SSID. If a client needs to connect to this BSS, it needs to specify this SSID. Disable: broadcast SSID and allow this BSS's SSID broadcast to the air periodically. Clients can scan out the SSID.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Station Isolation</td>
<td>Enabled: prevent the stations under this BSS from communicating with each other. Disabled: not prevent the stations under this BSS from communicating with each other.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Max Station Allowed</td>
<td>The maximum number (1-255) of clients that would be allowed to associate with this BSS</td>
<td>255</td>
</tr>
<tr>
<td>Station Inactivity Limit</td>
<td>Configure the maximum amount of time (15-65535 seconds) a station/client is allowed to be inactive before the inactivity policy takes effect. If in the configured time, BSS doesn't receive the data from client, BSS will disassociate with the client.</td>
<td>300</td>
</tr>
</tbody>
</table>

Saving configuration for BSS Basic Configuration
To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

### 5.2.3. Configuring BSS Security

BSS supports 802.11 security standards. By clicking the “Security” tab in the BSS Configuration page, enter the Security page. Choose Open WEP, Shared WEP, WPA, WPA2 from the drop-down menu besides the “Authentication Type” to enter the security configuration page.

Note: if choose Open/None from the drop-down menu besides “Authentication Type”, no security configuration page appears.

By clicking the drop down button beside the “Authentication Type” in the BSS Configuration page, choose Open WEP to enter the security configuration page.
In WEP encryption mode, the user can configure up to 4 keys and specify one of them as default key.

Shared WEP

By clicking the drop down button beside the “Authentication Type” in the BSS Configuration page, choose Shared WEP to enter the security configuration page.

WPA

By clicking the drop down button beside the “Authentication Type” in the BSS Configuration page,
choose WPA to enter the security configuration page.

Table 5-5 WPA Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Choose WPA</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Allowed Encryption Modes | Choose WPA encryption modes:  
  1) AES Only: choose AES encryption mode;  
  2) TKIP Only: choose TKIP encryption mode;  
  3) TKIP and AES: choose TKIP and AES encryption mode | TKIP and AES  |
| WPA Type              | Choose WPA Type:  
  1) WPA-PSK, ASCII Key;  
  2) WPA-PSK, Hex Key;  
  3) WPA-RADIUS and needs to configure Radius server. | WPA-PSK, ASCII Key |
| PSK Key String        | ASCII code or hexadecimal key. The length of ASCII code is 8-63; the length of Hex is 64. | N/A           |

WPA2

By clicking the drop down button beside the “Authentication Type” in the BSS Configuration page, choose WPA2 to enter the security configuration page.
Table below describes the WPA2 settings in this page.

Table 5-6 WPA Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Choose WPA2</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Allowed Encryption Modes | Choose WPA2 encryption modes:  
4) AES Only: choose AES encryption mode;  
5) TKIP Only: choose TKIP encryption mode;  
6) TKIP and AES: choose TKIP and AES encryption mode; | TKIP and AES |
| WPA Type            | Choose WPA2 Type:  
1) WPA-PSK, ASCII Key;  
2) WPA-PSK, Hex Key;  
3) WPA-RADIUS and needs to configure Radius server. | WPA-PSK, ASCII Key |
| PSK Key String      | ASCII code or hexadecimal key. The length of ASCII code is 8-63; the length of Hex is 64. | N/A       |
| Pre-authentication  | Enable or disable pre-authentication                                         | Disabled  |

**Saving configuration for BSS Security**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.
5.2.4. Configuring BSS VLAN

Click the “VLAN” tab to enter the VLAN configuration page.

Table below describes the VLAN settings for BSS interface.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>VLAN Setting</td>
<td>No VLAN: the BSS doesn’t belong to any VLAN; Access VLAN: the BSS belongs to a VLAN. The value range is 1-4094</td>
<td>No VLAN</td>
</tr>
</tbody>
</table>

Saving configuration for BSS VLAN

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

5.2.5. Configuring BSS IPv4

Click the “IPv4” tab to enter the IPv4 configuration page.
Table below describes the IPv4 settings for BSS interface.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>IP Address</td>
<td>Configure the IPv4 address for this BSS: 1) Static IP address/Mask, format: A.B.C.D/M 2) Do not configure</td>
<td>Do not configure</td>
</tr>
<tr>
<td>DHCP Server/Relay</td>
<td>Configure DHCP server/relay: 1) Disabled 2) Configure DHCP pool of DHCP Server 3) Configure DHCP relay Option 82</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Saving configuration for BSS IPv4**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**5.2.6. Configuring BSS QoS**

Click the “QoS” tab to enter the QoS configuration page.
Figure 5-18 QoS Configuration Screen

Table below describes the QoS settings for BSS interface.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>Access Category Mapping</td>
<td>Configure the BSS’s 802.11e mapping priority: None/Best Effort/Background/Video/Voice.</td>
<td>None</td>
</tr>
<tr>
<td>WMM</td>
<td>Enable/disable WMM service</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
| Whether allow WMM client to access | Allowed: allow clients that don’t support WMM to access  
Not Allowed: only allow clients that support WMM to access | Allowed |

**Saving configuration for BSS QoS**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**5.2.7. Configuring BSS Advanced Settings**

Click the “Advanced” tab to enter the Advanced configuration page.
**Figure 5-19 BSS Advanced Configuration Screen**

Table below describes the Advanced settings for BSS interface.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Name</td>
<td>Display the BSS’s Radio interface and BSS ID. Each radio supports up to 16 BSS</td>
<td>N/A</td>
</tr>
<tr>
<td>DTIM Interval</td>
<td>DTIM stands for Delivery Traffic Indication Message. It carries the DTIM interval. At DTIM interval, AP sends out buffered multicast and broadcast frames to clients in power-saving mode. The value range is 1-255. The default DTIM interval is 1, i.e., one beacon interval. That is, AP sends out buffered multicast and broadcast frames to power-saving clients every one beacon.</td>
<td>1</td>
</tr>
<tr>
<td>Fragmentation Threshold</td>
<td>Configure the threshold value (256-2346) for frame fragmentation. When the length of a frame exceeds the threshold value, the frame will be fragmented before being sent, 2346: disable fragmentation</td>
<td>2346</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>Configure the threshold value (0-2347) for sending RTS frame. When the length of a frame exceeds the threshold value, a RST frame will be sent before the frame being sent, asking for avoiding conflict. 0: always enable RTS 2347: disable RTS</td>
<td>2347</td>
</tr>
<tr>
<td>Unicast Rate</td>
<td>Configure the unicast rate of this BSS: auto/fixed rate. The BSS will attempt to only apply the specified rate between clients and the BSS. The setting also prevents clients that do not support the specified rate from associating with this BSS.</td>
<td>Auto</td>
</tr>
<tr>
<td>Multicast Rate</td>
<td>Configure the multicast rate of this BSS: auto/fixed rate. The BSS will attempt to only apply the specified rate between clients and the BSS.</td>
<td>Auto</td>
</tr>
</tbody>
</table>
### Multicast Optimization

Configure multicast frames to reduce packet loss rate of the multicast packet between the AP and the Client

**Disabled**

**Saving configuration for BSS Advance Setting**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

### 5.2.8. Deleting a BSS

To delete existing BSSs, check the boxes beside each BSS to be deleted and click the “Delete Selected BSS” button.

*Figure 5-20 Deleting a BSS*

### 5.3. Mesh Configuration

#### 5.3.1. Configuring Mesh Basic

Click “Wireless Settings” > “Mesh” listed in the main menu tree. The resulting page shows the configuration and status of the mesh.
Table below describes the Mesh basic settings in this page.

### Table 5-11 Mesh Basic Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh ID</td>
<td>Configure the Mesh ID</td>
<td>DefaultMesh</td>
</tr>
<tr>
<td>WDS IP Pool</td>
<td>Configure IP address pool for WDS links:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1) Automatically generated from MAC</td>
<td>Automatically generated from MAC</td>
</tr>
<tr>
<td></td>
<td>2) Manually configure, format: A.B.C.D/M</td>
<td></td>
</tr>
</tbody>
</table>

**Saving configuration for Mesh Basic**

To save the configuration after editing the above settings, click the “Apply Changes” button.

**5.3.2. Configuring Mesh Security**

WDS supports 802.11 security standards. By clicking the “Security” tab in the Mesh Configuration page, enter the Authentication page. Choose Open/None, Open WEP, Shared WEP, WPA, WPA2 from the drop-down menu besides the “Security Type” to enter the security configuration page.
Open WEP

By clicking the drop down button beside the “Security Type” in the WDS Configuration page, choose Open WEP to enter the security configuration page.

In Open WEP encryption mode, the user can configure up to 4 keys and specify one of them as default key.

Shared WEP

By clicking the drop down button beside the “Security Type” in the WDS Configuration page, choose Shared WEP to enter the security configuration page.
In Shared WEP encryption mode, the user can configure up to 4 keys and specify one of them as default key.

**WPA**

By clicking the drop down button beside the “Security Type” in the WDS Configuration page, choose WPA to enter the security configuration page.

Table below describes the WPA settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>Choose WPA</td>
<td>N/A</td>
</tr>
<tr>
<td>WPA Type</td>
<td>Choose WPA Type:</td>
<td>WPA-PSK, ASCII</td>
</tr>
</tbody>
</table>
1) WPA-PSK, ASCII Key;
2) WPA-PSK, Hex Key;

PSK Key String | ASCII code or hexadecimal key. The length of ASCII code is 8-63; the length of Hex is 64.
--- | ---
N/A

### WPA2

By clicking the drop down button beside the “Security Type” in the WDS Configuration page, choose WPA2 to enter the security configuration page.

![Figure 5-26 WPA2 Configuration Page](image)

Table below describes the WPA2 settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>Choose WPA2</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| WPA Type         | Choose WPA2 Type: 
|                  | 1) WPA-PSK, ASCII Key; 
|                  | 2) WPA-PSK, Hex Key; | WPA-PSK, ASCII Key |
| PSK Key String   | ASCII code or hexadecimal key. The length of ASCII code is 8-63; the length of Hex is 64. | N/A              |

### Saving configuration for Mesh Security

To save the configuration after editing the above settings, click the “Apply Changes” button.

### 5.3.3. Configuring Mesh ACL List

Click the “Mesh ACL List” tab to enter the its configuration page.
Table below describes the Mesh ACL List settings for BSS interface.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor List Type</td>
<td>Choose neighbor list type, including:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1) Inactive: don’t care about the neighbor list when forming WDS links;</td>
<td>Inactive</td>
</tr>
<tr>
<td></td>
<td>2) White list: the neighbors defined in neighbor list are allowed to form WDS links</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Black list: the neighbors defined in neighbor list are not allowed to form WDS links</td>
<td></td>
</tr>
<tr>
<td>Neighbor ID Type</td>
<td>Choose neighbor ID type, using neighbor hostname or router ID</td>
<td>Host Name</td>
</tr>
<tr>
<td>Neighbor ID</td>
<td>The neighbor’s hostname or router-id</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Saving configuration for Mesh ACL List**

To save the configuration after editing the above settings, click the “Apply Changes” button.

**5.3.4. Configuring Preferred Links**

Click the “Preferred Links” tab to enter its configuration page.
In the above configuration page, click “Create Preferred Link” button to enter the “Create Preferred Link” page.

![Menu](image)

**Figure 5-28 Preferred Links Configuration Screen**

In this page, choose link index from the drop-down menu besides the Link Index. The “Configure Preferred Link” page appears.

![Configure Preferred Link](image)

**Figure 5-29 Create a Preferred Link**

In this page, choose link index from the drop-down menu besides the Link Index. The “Configure Preferred Link” page appears.
Table below describes the Preferred Links settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor ID</td>
<td>Configure Neighbor ID, using hostname or router ID.</td>
<td>None</td>
</tr>
<tr>
<td>Preferred Radio</td>
<td>Choose the radio to form connection. For MSR4000, you can choose 0-3; for MSR2000/MSR1200, you can choose 0-1</td>
<td>None</td>
</tr>
<tr>
<td>Preferred Channel</td>
<td>Choose preferred channel</td>
<td>N/A</td>
</tr>
<tr>
<td>Maximum Bandwidth</td>
<td>Configure maximum bandwidth gotten by preferred WDS link. 0 is unset.</td>
<td>0</td>
</tr>
</tbody>
</table>

**Saving configuration for Preferred Link**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**5.3.5. Configuring Mesh Advanced Settings**

Click the “Advanced” tab to enter the Advanced configuration page.
Table below describes the Advanced settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSI Minimum Limit</td>
<td>Minimum RSSI required for links to form</td>
<td>15</td>
</tr>
<tr>
<td>Default Maximum Bandwidth</td>
<td>Configure maximum bandwidth gotten by each WDS link (&lt;1-300000&gt; unit kbits/s, 0 is unset)</td>
<td>0</td>
</tr>
</tbody>
</table>

**Saving configuration for Mesh Advanced Settings**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the "Cancel Changes" button.

**5.4. Client Mode Connection Configuration**

Click “Wireless Settings” > “Client Mode” listed in the main menu tree.
In this page, users could create a client connection (STA) as well as configure or delete an existing one.

5.4.1. Creating a New/Entering an Existing Client-mode Connection

In this page, click “Create” button to enter the “Create Client-mode Connection” page.

Select radio interface and station interface from the drop-down menu and click “Create” button to enter Client-mode Connection basic configuration page; click “Cancel Changes” button to discard any changes and return to the previous page.
After clicking “Create” button, the basic configuration page for the new client-mode connection will appear, as shown in figure below:

![Image](image_url)

**Figure 5-34 Basic Configuration Screen for a New Client-mode Connection**

To enter an existing client-mode connection, click its Sta Name to enter the configuration page.

![Image](image_url)

**Figure 5-35 Entering an Existing Client-mode Connection Page**
5.4.2. Configuring a Client-mode Connection (STA)

To configure a new created /an existing client-mode connection, enter the client-mode connection configuration page as stated above.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sta Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>SSID of AP</td>
<td>The 802.11 SSID for this AP</td>
<td>N/A</td>
</tr>
<tr>
<td>BSSID of AP</td>
<td>The 802.11 BSSID for this AP</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Description | Describe the client-mode connection | N/A

**Saving Configuration for the Client-mode Connection**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**5.4.3. Configuring Client-mode Connection Security**

Client-mode connection supports 802.11 security standards. By clicking the “Security” tab in the Configure Client-mode Connection page, enter the Security page. Choose Open WEP, Shared WEP, WPA, WPA2 from the drop-down menu besides the "Authentication Type" to enter the security configuration page.

Note: if choose Open/None from the drop-down menu besides “Authentication Type”, no security configuration page appears.

![Figure 5-38 Client-mode Connection Authentication Configuration Screen](image)

**Open WEP**

By clicking the drop down button beside the "Authentication Type" in the page, choose Open WEP to enter the security configuration page.
In Open WEP encryption mode, the user can configure up to 4 keys and specify one of them as default key.

**Shared WEP**

By clicking the drop down button beside the “Authentication Type” in the page, choose Shared WEP to enter the security configuration page.

In Shared WEP encryption mode, the user can configure up to 4 keys and specify one of them as default key.

**WPA**

By clicking the drop down button beside the “Authentication Type” in the page, choose WPA to enter the security configuration page.
Aruba Mesh Router Web-based Configuration Guide

Figure 5-41 Client-mode Connection WPA Configuration Page

Table below describes the WPA settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sts Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Choose WPA</td>
<td>N/A</td>
</tr>
<tr>
<td>WPA Type</td>
<td>Choose WPA Type: 1) WPA-PSK, ASCII Key; 2) WPA-PSK, Hex Key;</td>
<td>WPA-PSK, ASCII Key</td>
</tr>
<tr>
<td>PSK Key String</td>
<td>ASCII code or hexadecimal key. The length of ASCII code is 8-63; the length of Hex is 64.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

WPA2

By clicking the drop down button beside the “Authentication Type” in the page, choose WPA2 to enter the security configuration page.
Table below describes the WPA2 settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sts Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Choose WPA2</td>
<td>N/A</td>
</tr>
<tr>
<td>WPA Type</td>
<td>Choose WPA2 Type: 1) WPA-PSK, ASCII Key; 2) WPA-PSK, Hex Key;</td>
<td>WPA-PSK, ASCII Key</td>
</tr>
<tr>
<td>PSK Key String</td>
<td>ASCII code or hexadecimal key. The length of ASCII code is 8-63; the length of Hex is 64.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Saving configuration for Client-mode Connection Security**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**5.4.4. Configuring Client-mode Connection VLAN**

Click the “VLAN” tab to enter the VLAN configuration page.
Table below describes the VLAN settings for client-mode connection.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sts Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>VLAN Setting</td>
<td>No VLAN: the client-mode connection doesn’t belong to any VLAN; Access VLAN: the client-mode connection belongs to a VLAN. The value range is 0-4094, 0 for no access VLAN.</td>
<td>No VLAN</td>
</tr>
</tbody>
</table>

**Saving Configuration for Client-mode Connection VLAN**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

**5.4.5. Configuring Client-mode Connection IPv4**

Click the “IPv4” tab to enter the IPv4 configuration page.
Table below describes the IPv4 settings for client-mode connection.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>IP Address</td>
<td>Configure the IPv4 address for this client-mode connection:</td>
<td>Do not configure</td>
</tr>
<tr>
<td></td>
<td>1) Use DHCP: Enter vendor ID, configure DHCP Option 60 (up to 64 characters)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Static IP address/Mask, format: A.B.C.D/M</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Do not configure</td>
<td></td>
</tr>
</tbody>
</table>

Saving configuration for Client-mode Connection IPv4

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

5.4.6. Configuring Client-mode Connection Scanning

Click the “Scanning” tab to enter the Scanning configuration page.
Figure 5-45 Client-mode Connection Scanning Configuration Screen

Table below describes the scanning settings for client-mode connection.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sta Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>Scan Modes</td>
<td>Configure the scan modes</td>
<td>Default</td>
</tr>
<tr>
<td>Scan Interval</td>
<td>Configure the seconds between each scan (15-300 seconds)</td>
<td>0</td>
</tr>
<tr>
<td>Scan Threshold</td>
<td>Configure the threshold value for scanning</td>
<td>15</td>
</tr>
</tbody>
</table>

Saving configuration for Client-mode Connection Scanning

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

5.4.7. Configuring Client-mode Connection Advanced Settings

Click the “Advanced” tab to enter the Advanced configuration page.
Figure 5-46 Client-mode Connection Advanced Configuration Screen

Table below describes the Advanced settings for client-mode connection.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sta Name</td>
<td>Display the station’s radio interface and station interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>AP Inactivity Limit</td>
<td>Configure the maximum amount of time (1-60 seconds) an AP is allowed to be inactive before the inactivity policy takes effect.</td>
<td>2</td>
</tr>
<tr>
<td>Fragmentation Threshold</td>
<td>Configure the threshold value (256-2346) for frame fragmentation. When the length of a frame exceeds the threshold value, the frame will be fragmented before being sent,</td>
<td>2346: disable fragmentation</td>
</tr>
</tbody>
</table>

Table 5-23 Client-mode Connection Advanced Configuration Fields

Saving configuration for Client-mode Connection Advance Setting

To save the configuration after editing the above settings, click the "Apply Changes" button. To discard any changes and return to the previous page, click the "Cancel Changes" button.
Chapter 6  Network Settings

This chapter contains the following content:

- Configuring Routing
- DHCP Configuration
- VLAN Configuration
- Loopback Configuration
- NTP Configuration

6.1. Configuring Routing

The Routing Table is the information database used by routers to track the topology of the network and to determine how each data packet would be forwarded. This chapter describes how routing tables may be viewed using the wireless mesh router’s Web-based Management Interface and how static routes, OSPF routes, AWR routes and Multicast may be configured.

6.1.1. Routing Table Configuration

In the menu tree, select “Network Settings” > “Routing” > “Static Routes” to bring up the Static Routes configuration page.

![Figure 6-1 Static Routes Page](image)

Table below explains the various fields in the static routes page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td></td>
</tr>
<tr>
<td>Mask</td>
<td></td>
</tr>
<tr>
<td>Getway</td>
<td></td>
</tr>
</tbody>
</table>

Aruba Mesh Router Web-based Configuration Guide
53
6.1.2. Adding an IPv4 Static Route

To add a new IPv4 Static Route, enter destination, mask and gateway in the boxes indicated in the red circle, and click the “Add Static Route” button.

Table below describes the settings for an IPv4 static route entry.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination network or host address. <em>This field is required; when creating a default route, use 0.0.0.0</em></td>
<td>N/A</td>
</tr>
<tr>
<td>Mask</td>
<td>The mask indicating the prefix for the destination; the destination and mask are used together to determine whether a packet’s destination address matches a particular route</td>
<td>N/A</td>
</tr>
<tr>
<td>Gateway</td>
<td>The gateway IP address that this route points to.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

This field is required; when creating a default route, use 0.0.0.0

The figure below shows the resulting page when the new IPv4 static route is successfully added.

![IPv4 Static Route Table](image)

**Figure 6-3** An IPv4 Static Route is Successfully Added

### 6.1.3. Deleting an IPv4 Static Route

To delete an existing IPv4 static route, check the boxes beside the routes to be deleted and click the "Delete Static Route" button.
6.1.4. View IPv4 System Routing Table

To view the IPv4 system routing table, enter destination, click the “View System Routing Table” button.
Table below explains the various fields in the system routing table page.

### Table 6-3 System Routing Table Fields

<table>
<thead>
<tr>
<th>Column</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination network or host address.</td>
</tr>
<tr>
<td>Mask</td>
<td>The mask indicating the prefix for the destination; the destination and mask are used together to determine whether a packet’s destination address matches a particular route.</td>
</tr>
<tr>
<td>Gateway/Interface</td>
<td>The gateway IP address that this device points to. If an IP address is shown, then packets would be forwarded to this address. If an interface is shown, then packets would be forwarded using this interface.</td>
</tr>
<tr>
<td>Hop Count</td>
<td>The number of hops between the device and the destination network. However, the following special values may apply:</td>
</tr>
<tr>
<td>Type</td>
<td>A three-character code that indicates the type of the route.</td>
</tr>
<tr>
<td></td>
<td>First character: K indicates a kernel route, C indicates a directly-connected route, S indicates a static route, H indicates a host route, O indicate a OSPF route, A indicate a AWR route, d indicate a direct route obtained by DHCP.</td>
</tr>
<tr>
<td></td>
<td>Second character: ‘&gt;’ indicates the selected route when there are other routes with the same destination and mask.</td>
</tr>
<tr>
<td></td>
<td>Third character: ‘*’ indicates that the route is active in the router kernel.</td>
</tr>
</tbody>
</table>

**IPv4**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Mask</th>
<th>Gateway/Interface</th>
<th>Hop Count</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>10.65.12.1/gigabit-ethernet 0</td>
<td>1/0</td>
<td>S&gt;^*</td>
</tr>
<tr>
<td>10.44.81.209</td>
<td>255.255.255.255</td>
<td>loopback 0</td>
<td></td>
<td>C&gt;^*</td>
</tr>
<tr>
<td>10.65.12.0</td>
<td>255.255.255.0</td>
<td>gigabit-ethernet 0</td>
<td></td>
<td>C&gt;^*</td>
</tr>
</tbody>
</table>

**Figure 6-5 IPv4 System Routing Table Page**
6.1.5. OSPF Configuration Page

Select “Network Settings” > “Routing” > “OSPF” from the left menu tree to open the OSPF configuration page. The OSPF Configuration Page appears.

![OSPF Configuration Page](image)

Table below describes the OSPF settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Status</td>
<td>OSPF is enabled or disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Router Priority</td>
<td>The OSPF priority, and its value range is 1-255. When the priority is 0, the router can’t become DR.</td>
<td>0</td>
</tr>
<tr>
<td>Redistribute AWR</td>
<td>Redistribute AWR to OSPF field and define metric type (1-2) and metric value</td>
<td>Disabled</td>
</tr>
<tr>
<td>Redistribute Direct Connected Route</td>
<td>Redistribute Direct Connected Route to OSPF field and define metric type (1-2) and metric value</td>
<td>Disabled</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Define metric type (1-2)</td>
<td>2</td>
</tr>
<tr>
<td>Network Prefix</td>
<td>Configure the network segment that runs OSPF route. The format is A.B.C.D/M</td>
<td>N/A</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>Integer or A.B.C.D. Currently only support one OSPF Area ID</td>
<td>N/A</td>
</tr>
<tr>
<td>Summary Address</td>
<td>OSPF supports route aggregation function, summarizing the specified network segment. The format is A.B.C.D/M</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Saving configuration for OSPF

To save the configuration after editing the above settings, click the “Apply Changes” button.

6.1.6. Adding OSPF Network

To add a new OSPF network, enter the network prefix and OSPF Area ID in the boxes indicated in the red circle and clicks the “Add OSPF Network” button.

![Image of OSPF configuration interface]

**Figure 6-7 Adding New OSPF Network**

6.1.7. Deleting OSPF Network

To delete an existing OSPF network, check the boxes beside the network to be deleted and click the “Delete OSPF Network” button.
6.1.8. Adding Summary Address

To add a new summary address, enter the summary address in the box and click the “Add Summary Address” button.
6.1.9. Deleting Summary Address

To delete an existing summary address, check the boxes beside the summary address to be deleted and click the "Delete Summary Address" button.
6.1.10. AWR Configuration Page

Select “Network Settings” > “Routing” > “AWR” from the left menu tree to open the AWR configuration page. The AWR Configuration Page appears.
Table below describes the AWR Route settings in this page.

### Table 6-5 AWR Route Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWR Status</td>
<td>AWR is enabled or disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Debug Level</td>
<td>Configure the debug level for AWR, including None, Error, Event, Info, Dump</td>
<td>Error</td>
</tr>
<tr>
<td>Use Hello Protocol on Mesh Links</td>
<td>Enable or disable &quot;Use Hello Protocol on Mesh Links&quot;</td>
<td>Disabled</td>
</tr>
<tr>
<td>Primary Gateway Election</td>
<td>Enable or disable Primary Gateway Election</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Saving configuration for AWR**

To save the configuration after editing the above settings, click the “Apply Changes” button.
6.1.11. Multicast Configuration Page

Select “Network Settings” > “Routing” > “Multicast” from the left menu tree to open the Multicast configuration page. The Multicast Configuration Page appears.

![Multicast Configuration Page](image)

**Figure 6-12 Multicast Configuration Page**

Table below describes the Multicast settings in this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Status</td>
<td>Multicast is enabled or disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Debug Level</td>
<td>Configure the debug level for AWR, including None, Error, State, Info, Dump</td>
<td>State</td>
</tr>
<tr>
<td>Static RP Address for PIM</td>
<td>Configure the IP address of the RP (Rendezvous Point). Each router (including the RP router) enabling multicast should configure the RP address. 0.0.0.0 is unset.</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

**Saving configuration for Multicast**

To save the configuration after editing the above settings, click the “Apply Changes” button.

6.2. Configuring DHCP
6.2.1. DHCP Server Configuration

Enter the DHCP Server configuration page by selecting “Network Settings” > “DHCP” > “DHCP Server” in the left-side menu tree.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default lease time</td>
<td>The amount of time (in seconds) allowed for an IP address assignment (hereby referred to a lease) before it expires, if the client did not request for a specific lease length, it will be the default value. Value Range: 0-31536000s</td>
<td>7200</td>
</tr>
<tr>
<td>Max lease time</td>
<td>The maximum amount of time (in seconds) allowed for a lease regardless of the client’s request Value Range: 0-31536000s</td>
<td>86400</td>
</tr>
<tr>
<td>DNS Addresses</td>
<td>A comma-separated list of DNS server addresses that would be given to clients along with the lease. Example: 206.56.44.1,206.56.33.1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Saving configuration for DHCP Basic

To save the configuration after editing the above settings, click the “Apply Changes” button.
6.2.2. Adding a New DHCP Pool

To add a new DHCP pool, click the “DHCP Pools” tab, and then click the “Add New Pool” button, the configuration page appears:

In this page, enter the Pool name you want to call the new DHCP pool, such as test, in the blank box.

6.2.3. Configuring the New DHCP Pool

To configure the new DHCP pool, click the “Add New Pool” button, the configuration page appears:
The table below describes the settings for a DHCP pool.

### Table 6-8 Settings for DHCP Pool

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Name</td>
<td>An alphanumeric name for the pool to be created. This name must start with a letter and cannot contain any spaces.</td>
</tr>
<tr>
<td></td>
<td>Example: Test</td>
</tr>
<tr>
<td></td>
<td><strong>This parameter is required and cannot be changed after the pool is created.</strong></td>
</tr>
<tr>
<td>Domain Name</td>
<td>The network domain name that will be given to DHCP clients that will use addresses from this DHCP pool.</td>
</tr>
<tr>
<td></td>
<td>Example: Arubanet.com</td>
</tr>
<tr>
<td>Network</td>
<td>The network (with mask) from which the IP addresses in this DHCP pool will be part of.</td>
</tr>
<tr>
<td></td>
<td>Format: A.B.C.D/M</td>
</tr>
<tr>
<td>Gateway</td>
<td>The gateway information. DHCP server will provide gateway information to DHCP clients.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Configure DNS Server, format: A.B.C.D,A.B.C.D</td>
</tr>
<tr>
<td>Option 7 (Log Server)</td>
<td>Configure Log Server, format: A.B.C.D,A.B.C.D</td>
</tr>
<tr>
<td>Option 66 (TFTP Server)</td>
<td>Configure TFTP Server, format: A.B.C.D</td>
</tr>
<tr>
<td>Option 151 (NetLink SVP Server)</td>
<td>Configure NetLink SVP Server, format: A.B.C.D,A.B.C.D</td>
</tr>
</tbody>
</table>

### Deleting an Existing DHCP Option

To delete an existing DHCP Option, delete the content in the box beside Option 7, Option 66 and Option 151 and click “Apply Changes”.

---

Aruba Mesh Router Web-based Configuration Guide
Saving configuration for DHCP Pool

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

6.2.4. Deleting an Existing DHCP Pool

To delete an existing DHCP pool, check the box beside it and click “Delete Selected Pool”.

![Figure 6-16 Deleting an Existing DHCP Pool](image)

6.2.5. Adding an IP Address Range

IP address ranges make up the available addresses in this DHCP pool. DHCP clients can only obtain IP addresses from these ranges. To define IP address ranges, click a pool name to open the “Edit the Pool Parameters” page, and then click the “IP Address Ranges” tab, the configuration page appears. Enter the Begin IP Address and End IP Address, click “Add IP Range” button, the IP Address range will be added to the list area.
Click “Return to previous configuration” button, return to the basic page of configuring DHCP Pool

6.2.6. Deleting an IP Address Range

To delete an existing IP address range, check the boxes beside the IP range to be deleted and click the “Delete IP Range” button.
6.2.7. Adding an Fixed IP Assignment

In general, the DHCP protocol assigns unused addresses arbitrarily from each DHCP pool for each client. This behavior allows the number of clients that could access the network to be greater than that of the IP addresses, as long as these clients do not connect at the same time. It also, however, causes the IP address obtained by the same client to vary from session to session. Sometimes, a network administrator or client user may have the need to obtain the same IP address at all times. To satisfy this requirement, user may specify a set of fixed IP Address assignments beneath the IP Address ranges.

Fixed IP assignments are allocated based on the MAC address of each client device. To create a fixed assignment, click the “Fixed Assignment” tab to enter the configuration page, and specify the MAC Address and the desired IP address, then click the “Add Fixed IP Assignment” button, the fixed assignment will be added to the list area, the appears:

![Figure 6-19 Adding an Fixed Assignment](image)

6.2.8. Deleting an Existing Fixed Assignment

To delete an existing Fixed Assignment check the box beside it and click “Delete Fixed IP Assignment”.

Aruba Mesh Router Web-based Configuration Guide
70
6.2.9. Deleting DHCP Option

To delete an existing DHCP Option, delete the content in the box beside Option 7, Option 66 and Option 151 and click “Apply Changes”. To discard any changes and return to the previous page, click the “Cancel Changes” button.
6.2.10. DHCP Relay Configuration

DHCP Relay is a service provided by mesh routers that allows client devices connecting to the router to obtain IP Address from an external DHCP server. The mesh router relays both the DHCP request from the client to the DHCP server and the reply from the server to the client.

Select "Network Settings" > "DHCP" > "DHCP Relay" in the left-side menu tree to open the DHCP server configuration page. The “DHCP Relay configuration” page appears.

![Figure 6-22 DHCP Relay Configuration Page](image)

In this page, the external DHCP Servers can be configured. Users can enter a comma-separated list of external DHCP server IP addresses and click "Apply Changes”.

6.2.11. Deleting DHCP Relay

To delete an existing DHCP relay configuration, delete the IP address in the box beside DHCP Servers and click “Apply Changes”.

6.3. Configuring VLAN

6.3.1. VLAN Configuration

In the menu tree, select “Network Settings” > “VLAN” to bring up the VLAN configuration page.
6.3.2. Adding VLAN Interface

To add a new VLAN interface, click the “Add VLAN Interface” button.
### 6.3.3. Configuring VLAN Basic Settings

Enter VLAN ID, for example "100", click "Add VLAN Interface" button, pop up the configuration page as shown in figure below.

![Add VLAN Interface Page](image-url)
Table below describes the basic settings for VLAN.

### Table 6-9 VLAN Interface Basic Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Describe the VLAN interface</td>
<td>N/A</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Can be up or down.</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>If down, this interface would be inactive (shutdown).</td>
<td></td>
</tr>
</tbody>
</table>

**Saving configuration for VLAN Basic**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

### 6.3.4. Configuring VLAN Interface IPv4

To configure the VLAN interface IPv4, click the “IPv4” tab to enter the IPv4 configuration page.
Figure 6-27 IPv4 Configuration Screen

Table below describes the settings for the IPv4.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
</table>
| IP Address      | 1) Use DHCP:  
|                 | a) Enter manufacturer ID, configure DHCP Option 60 (up to 64 characters)     | Do not configure |
|                 | 2) Static IP/mask: manually configure static IP/mask, format A.B.C.D/M       |               |
|                 | 3) Do not configure: not configure IP address                               |               |
| Management Interface | Whether configure this interface as Management interface                  | No            |
| Router-ID Interface | Whether configure this interface as Router-ID interface                     | No            |
| DHCP Server     | 1) Disabled                                                                  | Disabled       |
|                 | 2) DHCP Server                  
|                 | DHCP Pool: configure DHCP address pool                                       |               |
|                 | 3) DHCP Relay: enter Option 82 Circuit ID configuration                     |               |

Saving configuration for VLAN IPv4

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.
6.3.5. VLAN Interface Advanced Configuration

To configure the VLAN advanced features, click the “Advanced” tab to enter the Advanced edit page.

![Ethernet Interface Advanced Configuration Screen](image)

**Figure 6-28 Ethernet Interface Advanced Configuration Screen**

Table below describes the settings for the advanced features.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU (Maximum Transmission Unit)</td>
<td>Maximum transmission unit in bytes; controls how Layer-3 packets would be fragmented when they are sent through this interface. Range: 256-1500</td>
<td>1500</td>
</tr>
<tr>
<td>Traffic Isolation</td>
<td>Enable or disable the traffic isolation feature</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Saving configuration for VLAN Advanced Settings**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

6.3.6. Deleting a VLAN Interface

To delete an existing VLAN interface, check the boxes beside the VLAN ID to be deleted and click the “Delete Selected VLAN Interface(s)” button.
6.4. Configuring Loopback

6.4.1. Loopback Configuration

In the menu tree, select “Network Settings” > “Loopback” to bring up the Loopback configuration page.
6.4.2. Adding a Loopback Interface

To add a new Loopback interface, click the "Add" button. The following page appears:
In this page, choose Loopback Index and click "Create" button, enter the Loopback configuration page:

Table below describes the settings for loopback.
### Table 6-12 Loopback Configuration Fields

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Add the information to describe the loopback interface</td>
<td>N/A</td>
</tr>
<tr>
<td>IP Address</td>
<td>Configure the IP address for the loopback interface:</td>
<td>Generated from MAC</td>
</tr>
<tr>
<td></td>
<td>1) Static IP/Mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Generated from MAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Do not configure</td>
<td></td>
</tr>
<tr>
<td>Management Interface</td>
<td>Whether configure this interface as Management interface</td>
<td>No</td>
</tr>
<tr>
<td>Router-ID Interface</td>
<td>Whether configure this interface as router-ID interface</td>
<td>No</td>
</tr>
</tbody>
</table>

**Saving configuration for Loopback Interface**

To save the configuration after editing the above settings, click the “Apply Changes” button. To discard any changes and return to the previous page, click the “Cancel Changes” button.

### 6.4.3. Deleting an Existing Loopback Interface

To delete an existing loopback interface, check the boxes beside the loopback interface to be deleted and click the “Delete” button.

![Figure 6-33 Deleting an Existing Loopback Interface](image)

### 6.5. Configuring NTP

#### 6.5.1. NTP Configuration

In the menu tree, select “Network Settings” > “NTP” to bring up the NTP configuration page.
Table below describes the settings for NTP.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Client</td>
<td>Enable or disable NTP client</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP Server Address</td>
<td>Configure the IP address of NTP server, format: A.B.C. 0.0.0.0 is unset.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Refresh Interval</td>
<td>NTP refresh interval in seconds (5-86400)</td>
<td>1024</td>
</tr>
<tr>
<td>Time Zone Name</td>
<td>Name of time zone</td>
<td></td>
</tr>
<tr>
<td>Time Zone Offset</td>
<td>Offset in hours and minutes</td>
<td>0:0</td>
</tr>
</tbody>
</table>

**Saving configuration for NTP**

To save the configuration after editing the above settings, click the “Apply Changes” button.
Chapter 7 Configuring Services

This chapter contains the following content:

- Mobility
- VPLM Configuration
- Auto Recovery
- AVT

7.1. Mobility

To enter the “Mobility” configuration page, select “Services” > “Mobility” from the left-side menu tree.

![Figure 7-1 Roaming Configuration Page]

The table below describes the roaming configuration fields:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Roaming service enabled or disabled.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Debug Level</td>
<td>Configure the debug level.</td>
<td>Dump</td>
</tr>
</tbody>
</table>

Saving configuration for Mobility Settings

To save the configuration after editing the above settings, click the “Apply Changes” button.

7.2. VPLM

Select “Services” > “VPLM” from the left-side menu tree to enter the “VPLM” configuration page.
The table below describes the settings for VPLM.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Whether the VPLM service is to be enabled or disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allowed VLAN</td>
<td>Configure the allowed VLAN</td>
<td>Auto</td>
</tr>
<tr>
<td>Spanning Tree Compatibility</td>
<td>Enable or disable Spanning Tree Compatibility</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Saving configuration for VPLM**

To save the configuration after editing the above settings, click the “Apply Changes” button.

**7.3. Auto Recovery**

Select “Services” > “Auto Recovery” from the left-side menu tree to enter the “Auto Recovery” configuration page.
The table below describes the settings for Auto Recovery.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Whether the Auto Recovery service is to be enabled or disabled.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Debug Level</td>
<td>Configure the debug level.</td>
<td>Error</td>
</tr>
</tbody>
</table>

Saving configuration for Auto Recovery

To save the configuration after editing the above settings, click the “Apply Changes” button.

7.4. AVT

Select “Services” > “AVT” from the left-side menu tree to enter the “AVT” configuration page.
The table below describes the settings for AVT.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Disabled: disable AVT service</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>AVT Egress: enable AVT service and set the router as egress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVT Ingress: enable AVT service and set the router as ingress</td>
<td></td>
</tr>
<tr>
<td>Buffer time</td>
<td>1-100, unit is 100 milliseconds</td>
<td>5</td>
</tr>
<tr>
<td>Ingress interface</td>
<td>When a video encoder connects to the Ethernet interface of the device, the Ethernet interface can act as AVT Ingress.</td>
<td>None</td>
</tr>
<tr>
<td>Ingress Encoder</td>
<td>Set the encoder type (video server). Generic for most encoders (default) such as Hikvision AXIS, Avinfo and D-Link Tycosun for Tycosun encoder; and Visiondigi for Visiondigi encoder</td>
<td>Generic</td>
</tr>
</tbody>
</table>

**Saving configuration for AVT**

To save the configuration after editing the above settings, click the “Apply Changes” button.

**7.4.1. Adding an Ingress IP**

To add an ingress IP, enter the IP address in the box and click the “Add” tab.
7.4.2. Deleting an Existing Ingress IP

To delete an ingress IP, check the boxes beside the ingress IP to be deleted and click the “Delete” button.
Chapter 8  SNMP Configuration

Wireless mesh routers all provide remote management through the popular Simple Network Management Protocol (SNMP). Using SNMP, network management products can read/write configuration and store data on the wireless mesh routers.

This chapter describes how SNMP service can be configured using the web-based management interface. It includes the following sections:

- Configuring Device Information
- Configuring SNMP Communities
- Configuring SNMP Trap Receivers
- Configuring SNMPv3 User Accounts

8.1. Device Info

Select “SNMP” > “Device Info” from the left-side menu tree to enter “Device Info” configuration page. The resulting page is shown below. It displays all of the configured SNMP location and contact information.

![SNMP Device Info Page](image)

The table below describes the SNMP device info fields.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysname</td>
<td>System Name</td>
<td>N/A</td>
</tr>
<tr>
<td>Syslocation</td>
<td>SNMP Agent location</td>
<td>Beijing</td>
</tr>
<tr>
<td>Syscontact</td>
<td>SNMP Agent contact info</td>
<td><a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a></td>
</tr>
</tbody>
</table>
Saving configuration for SNMP Device Info

To save the configuration after editing the above settings, click the “Apply Changes” button.

8.2. SNMP Communities

SNMP Communities is the basic authentication scheme used by SNMP v1 and v2. Each mesh router may have one or more community strings defined; each string can have an access-mode of read-only or read-write. When the router receives an SNMP command (which is usually a read or a write), it allows the operation if it matches a known community string with a matching access-mode.

8.2.1. Configuring SNMP Communities

Select “SNMP” > “Communities” from the left-side menu tree to enter “SNMP Communities” configuration page. The resulting page displays all of the configured communities and their access modes in a table.

8.2.2. Adding a New Community

To add a community, enter the community name in the box at the bottom of the table and select access mode from the drop-down menu, and then click the “Add Community” button.
# 8.2.3. Deleting a Community

To delete a Community, check the boxes beside each entry to be deleted, and click the “Delete Community” button.

## 8.3. SNMP Trap Receivers

SNMP Trap Receivers are external hosts that receive the SNMP trap message sent by the MESH ROUTER product. These receivers are generally Network Management Systems. Currently, only SNMPv1 and v2 trap messages are supported. Each MESH ROUTER product may configure several receivers.

Aruba Mesh Router Web-based Configuration Guide
8.3.1. Configuring SNMP Trap Receivers

Select “SNMP” > “Trap Receivers” from the left-side menu tree to open the “SNMP Trap Receivers” configuration page. The resulting page displays all of the configured receivers with their ports and communities in a table.

8.3.2. Adding a New Receiver

To add a receiver, enter the Receiver Address, Port and Community in the corresponding boxes at the bottom of the table and choose Version and Type from the drop-down menu, and then click the “Add SNMP Trap Receiver” button.

The Table below summarizes the settings for an SNMP Trap Receiver.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Address</td>
<td>The IP Address for the trap receiver.</td>
<td>N/A</td>
</tr>
<tr>
<td>Port</td>
<td>The port number at which the trap receiver would receive the trap messages.</td>
<td>N/A</td>
</tr>
<tr>
<td>Trap Community</td>
<td>The community string for the trap messages sent to this receiver. The community must be alphanumeric, starting with a letter, and contain no spaces.</td>
<td>N/A</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the trap receiver. V1 and V2C are available.</td>
<td>v1</td>
</tr>
<tr>
<td>Message Type</td>
<td>The message type of the trap receiver. Trap and Inform are available.</td>
<td>Trap</td>
</tr>
</tbody>
</table>

Note: The Version V1 cannot be configured with the message type Inform at the same time.

8.3.3. Deleting a Trap Receiver

To delete a trap receiver, check the boxes beside each receiver to be deleted, and click the “Delete SNMP Trap Receiver” button.

8.4. SNMP v3 Users

SNMPv3 introduced the concept of user accounts along with strong encryption and authentication methods. MESH ROUTER products support SNMPv3 and allow the configuration of multiple SNMPv3 users, each with different access rights as well as authentication and encryption methods.

8.4.1. Configuring SNMPv3 Users

Choose “SNMP” > “V3 Users” from the left-side menu tree to open the “SNMPv3 Users”
configuration page. The resulting page displays all of the configured v3 users and their information.

![Figure 8-8 SNMPv3 Users Configuration Page](image)

### 8.4.2. Adding a New v3 User

To add a new v3 user, enter the v3 Username, Auth password and Priv password in the corresponding boxes and choose Access Mode and User Type from the drop-down menu, and then click the "Add SNMPv3 User" button at the bottom of the table.

![Figure 8-9 Add a New SNMPv3 Users](image)

The table below summarizes the settings for a SNMPv3 user.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3 Username</td>
<td>The SNMPv3 User Name; must be an alphanumeric string, start with a letter, and contain no spaces.</td>
<td>N/A</td>
</tr>
<tr>
<td>Access Mode</td>
<td>Can be Read-only or Read-write</td>
<td>Read-only</td>
</tr>
</tbody>
</table>
Read-only: the user may retrieve information from the router MIB, but not change it

Read-write: the user may both retrieve and change information in the router MIB.

| User Type | The authentication and encryption methods used by this v3 user; can be NoAuthNoPriv, AuthNoPriv, or AuthPriv. NoAuthNoPriv: No secure authentication or encryption AuthNoPriv: Use secure authentication, but do not use encryption. AuthPriv: Use both secure authentication and encryption | No-auth No-priv |
| Auth Password | The authentication password used for AuthNoPriv and AuthPriv users. Must be an alphanumeric string between 8 and 16 characters long. Example: a1a2a3a4a5 | N/A |
| Priv Password | The encryption password used for AuthPriv users. Must be an alphanumeric string between 8 and 16 characters long. Example: a1a2a3a4a5 | N/A |

### 8.4.3. Deleting an SNMPv3 User

To delete a SNMPv3 User, check the boxes beside each user to be deleted, and click the “Delete SNMP v3 User” button.

![Figure 8-10 Deleting an SNMPv3 User](image)
Chapter 9  Syslog Configuration

Wireless mesh routers use syslog feature to automatically send the important local system events to the remote syslog server.

9.1. Configuring Syslog Client

Choose “Syslog” > “Client” from the left-side menu tree to open the “Syslog Client Configuration” page. The resulting page displays all of the configured syslog server and facilities/severity levels.

![Figure 9-1 Syslog Client Configuration Page](image)

9.2. Remote Syslog Service

Choose the “Enabled” or “Disabled” from the drop-down menu beside the Remote Logging, and click “Apply Changes” button.
9.3. Adding a Syslog Server

To add a syslog server, enter the server address in the box at the bottom of the syslog server list, and click “Add Syslog Server” button.

![Figure 9-3 Adding an Syslog Server](image)

9.4. Deleting a Syslog Server

To delete a syslog server, check the boxes beside each server to be deleted, and click the “Delete Syslog Server” button.

![Figure 9-4 Deleting a Syslog Server](image)
9.5. Adding Facility and Severity Level

To add facility and severity level, choose the facility and severity level from the drop-down menu, and click “Add Facility/Severity” button.

![Figure 9-5 Adding Facility and Severity Level](image)

9.6. Deleting Facility and Severity

To delete facility/severity, check the boxes beside each facility/severity to be deleted, and click the “Delete Facility/Severity” button.

![Figure 9-6 Deleting Facility/Severity](image)
Chapter 10  Troubleshooting

Wireless mesh routers provide some tools for network diagnosis, including:

- Tools
- Logs

10.1. Tools

The Tools page provides many common tools to see the working status and performance of routers.

Click "Troubleshooting" -> "Tools" to enter Tools page.

![Figure 10-1 Troubleshooting Tools Page](image)

The table below describes the information of these troubleshooting tools.

<table>
<thead>
<tr>
<th>Troubleshooting Tools</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Obtain the device’s basic information, including running configuration file, startup configuration file, mesh node list, interface list, hardware inventory</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Tools to check connectivity, including Ping and Traceroute</td>
</tr>
<tr>
<td>RF Management</td>
<td>RF management status, including active links, active portals, qualified neighbors and all neighbors</td>
</tr>
<tr>
<td>Radio</td>
<td>View radio interfaces information, including radio status and scanned device</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RF Scan</td>
<td>View the neighbors of radio interfaces after full spectrum scan</td>
</tr>
<tr>
<td>Neighbor RSSI</td>
<td>View the neighbor RSSI status continuously according to local radio index and neighbor MAC address</td>
</tr>
<tr>
<td>Routing Table</td>
<td>View routing table, including AWR route, connected route, OSPF route, static route and route summary</td>
</tr>
<tr>
<td>AWR</td>
<td>View AWR database and neighbor information</td>
</tr>
<tr>
<td>OSPF</td>
<td>View OSPF database, interfaces and neighbor information</td>
</tr>
<tr>
<td>Multicast Routing Table</td>
<td>View the Multicast Routing table</td>
</tr>
<tr>
<td>PIM</td>
<td>View the PIM interface or neighbor status</td>
</tr>
<tr>
<td>IGMP</td>
<td>View the IGMP group member or interface status</td>
</tr>
<tr>
<td>Ethernet Status</td>
<td>View Ethernet interface status</td>
</tr>
<tr>
<td>VLAN Interface</td>
<td>View VLAN interface status</td>
</tr>
<tr>
<td>Radio Client List</td>
<td>View the Radio client list according to radio index and BSS index</td>
</tr>
<tr>
<td>Client Details</td>
<td>View the client detailed information according to client MAC address</td>
</tr>
<tr>
<td>Client Mode</td>
<td>View client modes according to radio index and station index</td>
</tr>
<tr>
<td>Motrix</td>
<td>View Motrix roaming information, including status, interfaces, local client list, LMS client list, TGW client list, specified clients (specified MAC addresses) roaming information</td>
</tr>
<tr>
<td>VPLM</td>
<td>View VPLM information, including VPLM MAC table and VPLM database</td>
</tr>
<tr>
<td>Multicast Optimization</td>
<td>View which station connected is enable Multicast Optimization</td>
</tr>
<tr>
<td>Other</td>
<td>View ARP table and DHCP server lease address and AVT status</td>
</tr>
</tbody>
</table>

For example, Ping is a common tool used to check the reachability to destination network.

Click “Tools” -> “Connectivity” -> “Ping” to enter Ping page, and enter IP address to ping in the box beside “IP Address”.
Click “Execute” button, the device sends 4 packets. The result of Ping will be displayed at the bottom of this page.

10.2. Logs

MESH ROUTER products provide many types of logs, including system log, upgrade log, boot log, and etc. Click “Troubleshooting” -> “Logs” from the left-side menu tree to enter Logs page.
10.2.1. Viewing Logs

Choose the log type from the drop-down menu beside the “Log” and click “View Log” button.

10.2.2. Downloading Logs

To download logs, select the logs to download and click “Download All Logs” button.
Figure 10-5 Downloading Logs
Chapter 11   Maintenance

This chapter describes the maintenance operation provided by wireless mesh routers, including:

- Upgrade
- Import/Export
- Reboot
- Factory Reset
- Change Password

11.1. Upgrade

Wireless mesh routers can be easily upgraded by downloading an updated software image file and upgrading a MESH ROUTER's on-board software with it. To upgrade the MESH ROUTER, click on the menu tree item "Upgrade" to open the “Upgrade” page. Enter the location of the image file or click the “Browse” button to choose the image file.

Click “Upgrade” button, the device start the upgrading process.

After the upgrading complete successfully, click "Reboot” button.
Then, the system enters reboot process, click “Yes, perform reboot” button.

Note: The device must be rebooted to run the new image.

11.2. Import/Export Configuration

To ensure the stability of the device, we recommend users to backup the configuration file when the configuration is changed. And users should also periodically backup the configuration file of routers.

11.2.1. Export Configuration

To export the current configuration file, click “Maintenance” > “Import/Export” to enter the configuration page. Click “Export Current Configuration” button and choose the location from the pop-up window to save the configuration file. Before exporting the configuration file, check the box in front of “Save Recent Changes Before Export".
11.2.2. Import Configuration

To import new configuration, click “Browse” button and choose the configuration file to be imported from the pop-up window, such as D:\device.conf, and click “Import New Configuration” button, the configuration file will be imported into the device.
During the process, the following page will appear to ask for rebooting the device. The device will use the new configuration file after reboot.

![Import/Export Configuration](image)

**Figure 11-7 Import Configuration Successfully**

### 11.3. Reboot

To reboot the device, click “Maintenance” -> “Reboot” from the left-side menu tree. Click “Yes, perform reboot” to reboot the device immediately, or select “No, return to homepage” to cancel.

![Reboot Device](image)

**Figure 11-8 Reboot Page**

Click “Yes, perform reboot” button, the device will reboot.
In the reboot process, the user can not conduct any operation.

11.4. Factory Reset

To restore factory default setting, click “Maintenance” -> “Factory Reset” from the left-side menu tree. Click “Yes, perform factory reset” to restore the factory setting immediately, or select “No, return to homepage” to cancel.

Click “Yes, perform factory reset”, the device will reboot.

Another method of restoring the unit to the factory default state is:

- Power off the device, power it back on, and wait for about 60 seconds

Aruba Mesh Router Web-based Configuration Guide
108
• Repeat the above procedure six times
• The seventh time the unit powers on, it should revert to factory default state.

The device will restore factory settings after reboot. And WMI connection fails, the user need to re-configure IP address via CLI, and log in WMI page using the configured IP address.

11.5. Change Password

To ensure the security of device, we recommend users to change password regularly. To change password, click “Maintenance” -> “Password” from the left-side menu tree. Enter current password in the “Old password” box.

![Figure 11-12 Change Password Page](image)

The password must be an alphanumeric string between 1-32 characters long that starts with a letter and has no spaces. When the password is changed, users are required to login again for any operation.