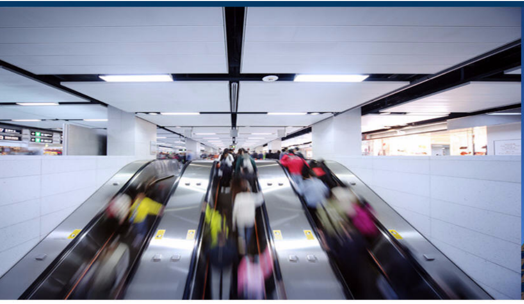
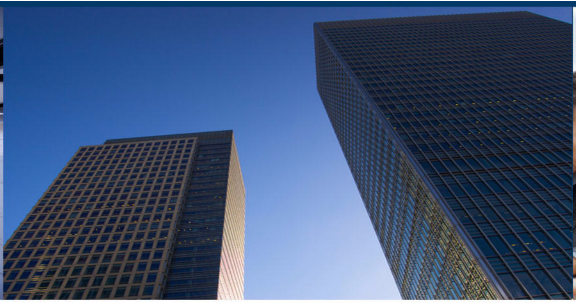
ORiNOCO® 802.11n Access Points

Software Management Guide

Products Covered

ORiNOCO® AP-800
ORiNOCO® AP-8000
ORiNOCO® AP-8100





Copyright

Trademarks

Disclaimer

Proxim reserves the right to revise this publication and to make changes in the content from time-to-time without obligation on the part of Proxim to provide notification of such revision or change. Proxim may make improvements or changes in the product(s) described in this guide at any time. When using these devices, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons.

GPL License Note

ORiNOCO® products include, in part, some free software that is developed by Free Software Foundation. A user is granted license to this software under the terms of either the GNU General Public License or GNU Lesser General Public License (See http://www.gnu.org/licenses/licenses.html). This license allows the user to freely copy, modify and redistribute this software and no other statement or documentation from us. To get a copy of this software or for any other information please contact our customer support team (For telephone numbers, see Telephone Support).

OpenSSL License Note

This product contains software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) and that is subject to the following copyright and conditions:

ORiNOCO® 802.11n Access Points - Software Management Guide

Documentation Version: 4.2
P/N 765-00155, March 2013

Contents

Preface

This chapter contains the information on the following:

About this Guide

This guide gives a jump-start working knowledge on the ORiNOCO® 802.11n Access Points. It explains the step-by-step procedure to configure, manage and monitor the device by using Web Interface.

Products Covered

Tabulated below are the ORiNOCO® 802.11n Access Points covered in this guide, with the latest software version supported.

Product(s)	Supported SKUs	Supported Software Version
ORiNOCO® AP-800	WD, US, JP	4.0.0
ORiNOCO® AP-8000	WD, US, JP	4.0.0
ORiNOCO® AP-8100	WD, US, JP, EU	4.1.1

Audience

The intended audience for this guide is the network administrator who configures, manages and/or monitors the device, by using the Web Interface.

Prerequisites

You should have a basic working knowledge on Wireless Networks, Local Area Networking (LAN) concepts, Network Access Infrastructures and Client-Server Applications.

Documentation Conventions

Screenshots

This guide uses the screenshots of AP-8100, as a base to explain the step-by-step procedures of configuring, managing and monitoring the device by using Web Interface. Based on your device, the screenshots may vary. Hence, we request you to refer to the screenshots that are valid for your device.

Device Naming Conventions

Naming Convention	Description
AP Device	Refers to any ORiNOCO® 802.11n AP device (AP-800 / AP-8000 / AP-8100)
AP-800	Refers to the ORiNOCO® AP-800 device
AP-8000	Refers to the ORiNOCO® AP-8000 device
AP-8100	Refers to the ORiNOCO® AP-8100 device

Icon Representation

Name	Image	Meaning
Note	📝	A special instruction that draws the attention of the user.
Important	❗	A note of significant importance, that a user should be aware of.
Caution	⚠	A warning, that cautions the user of the possible danger.

Related Documents

For more information, please refer to the following additional documents that are available at the Proxim's support site http://support.proxim.com.

- **Quick Installation Guide (QIG)**: A quick reference guide that provides essential information to install and configure the device.
- **Hardware Installation Guide**: A guide that provides a hardware overview and details the installation procedures and hardware specifications of ORiNOCO® 802.11n Access Points.
- **Reference Guide**: A guide that provides essential information on how to configure, manage and monitor the device by using Command Line Interface.
- **Safety and Regulatory Compliance Guide**: A guide that provides essential information on country specific safety and regulatory norms, to be followed while installing the device.

❗: **Proxim recommends you to visit its support site** http://support.proxim.com **for regulatory information and latest product updates.**

Introduction 1

This chapter contains information on the following:

1.1 Introduction to Wireless Networking

Wireless Networking refers to the technology that enables two or more computers to communicate by using standard network protocols, but without network cabling, generally referred to Wireless LAN (WLAN). A WLAN is grouping of network components connected by electromagnetic (radio) waves instead of cables. A WLAN basically consists of:

- The network backbone
- End-user devices such as data collection units, handheld computers and laptop
- Wireless LAN Access Points
- Wireless cards
- Software that will help you manage the network.

In a WLAN, an Access Point (AP) Device extends the capability of an existing ethernet network to the devices on a wireless network, acting as a bridge between the wired and wireless devices.

A wireless network with atleast one AP Device (either connected to a wired network infrastructure or a wireless backhaul) and a set of wireless devices form a Basic Service Set (BSS). Each BSS is identified by a Service Set Identifier (SSID) which uniquely identifies a WLAN. In a typical network environment, the AP Device functions as a wireless network access point to data and voice networks.

1.2 About ORiNOCO® 802.11n Access Points

Proxim's ORiNOCO® 802.11n Access Point family comprises of the products tabulated below:

Product(s)	Description	Image
ORiNOCO® AP-800	Proxim's ORiNOCO® AP-800 is an indoor 802.11n Access Point with dual-band, 3x3 MIMO (Multiple Input and Multiple Output) and a single radio which operates either in 2.4 or 5 GHz. This connectorized device comes with 3 omni-directional antennas.	
ORiNOCO® AP-8000	Proxim's ORiNOCO® AP-8000 is an indoor 802.11n Access Point with dual-band, 3x3 MIMO (Multiple Input and Multiple Output) and dual radio, where one operates in 2.4GHz and other in 5GHz. This connectorized unit comes with 6 omni-directional antennas, 3 per radio.	
ORiNOCO® AP-8100	Proxim's ORiNOCO® AP-8100 is an indoor 802.11n Access Point with dual-band, 2x2 MIMO (Multiple Input and Multiple Output) and dual radio, where one operates in 2.4GHz and other in 5GHz. This integrated unit comes with built-in 4 omni-directional antennas, 2 per radio.	

1.2.1 Salient Features

- Easy operation and installation
- Industry-leading throughput in 802.11b/g/n and 802.11a/n modes in 2.4GHz and 5GHz respectively.
- Highest throughput with single radio rates of 150 - 170 Mbps and dual radio rates of 250 - 300 Mbps.
- Advanced 802.11i support for enterprise-grade security.
- Tested against Wi-Fi Alliance interoperability test suite and certified as interoperable with Wi-Fi client access product.
- Provides wall mounting or ceiling option for flexible device installation.
- Distributed WLANs with Centralized Management.
- Management through a Web Interface (HTTP), Command Line Interface (CLI), Simple Network Management Protocol (SNMP) and Network Management System (ProximVision ES v2.3 and above)

1.2.2 Applications

1. Multiple high definition **IP-surveillance** cameras used for monitoring airports, offices, restaurants, warehouses, etc., can be monitored and managed by using a single AP Device.
2. Proxim's AP Devices exhibit a secure data transfer via high speed network links and **over-the-air encryption of data**.
3. **Enterprise Connectivity**:

   Delivering a secure, flexible, scalable and reliable enterprise class 802.11n standard Data, Voice, and Video for small and medium Enterprise WLAN deployments, our AP Device can serve multiple service sets with:

   — **Multiple SSID Assignment**: Multiple wireless clients connected to a single AP Device are grouped together as different service sets and every service set is assigned an independent SSID, allowing you to maintain maximum number of groups under a single Virtual Access Point (VAP) network.

   — **Single SSID Assignment**: Different wireless clients belonging to different service sets (SSIDs) can access the wireless network from one single AP Device with a single SSID.

   — **RADIUS VLAN Assignment**: In addition to the manual VLAN assignment, every wireless client / service set connected to a single AP Device is assigned a specific VLAN ID via a pre-configured RADIUS server, reducing the load of manually configuring the VLAN parameters of each wireless client.

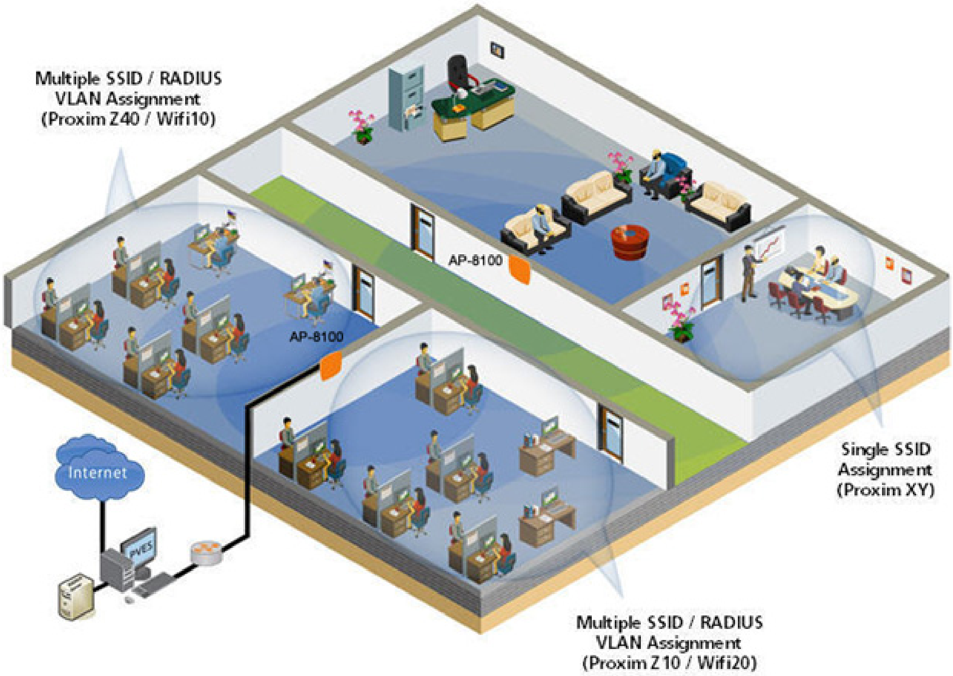


Figure 1-1 Enterprise Connectivity (Multiple SSID, Single SSID and RADIUS VLAN Assignment)

4. **Seamless client roaming for both data and voice (VoIP)**:

   Multiple wireless clients can connect to a single AP Device, or they can move between multiple AP Devices located within the same vicinity. As wireless devices move from one coverage cell to another, they maintain the network connectivity.

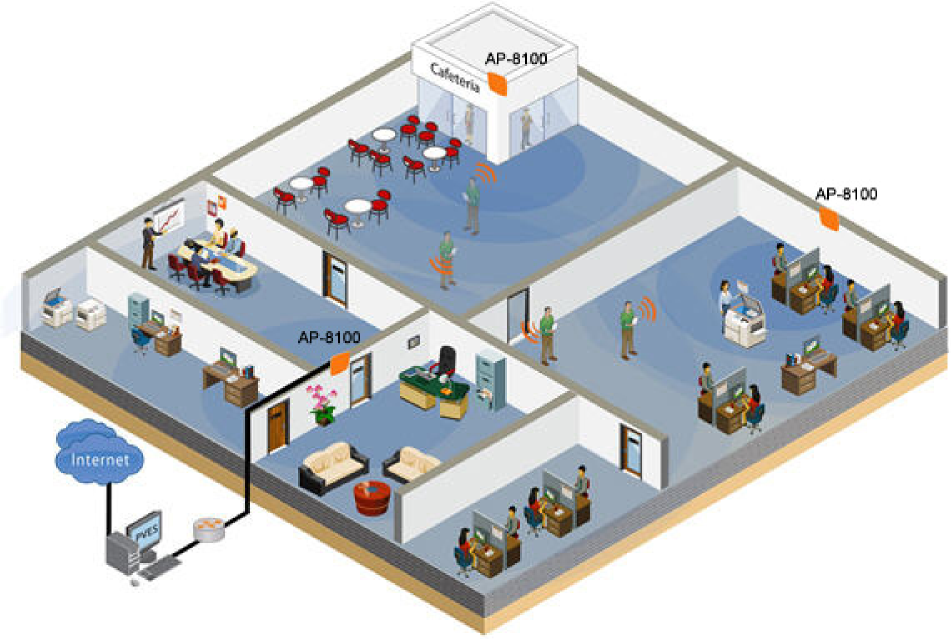


Figure 1-2 Seamless Client Roaming

5. **Extended Coverage Areas**:

   Proxim's high capacity, 802.11n AP Devices support Wireless Distribution System (WDS), that helps you establish a wireless communication between two AP Devices or two Basic Service Sets (BSS), thus allowing you to extend the WLAN or an access point coverage to wide areas.

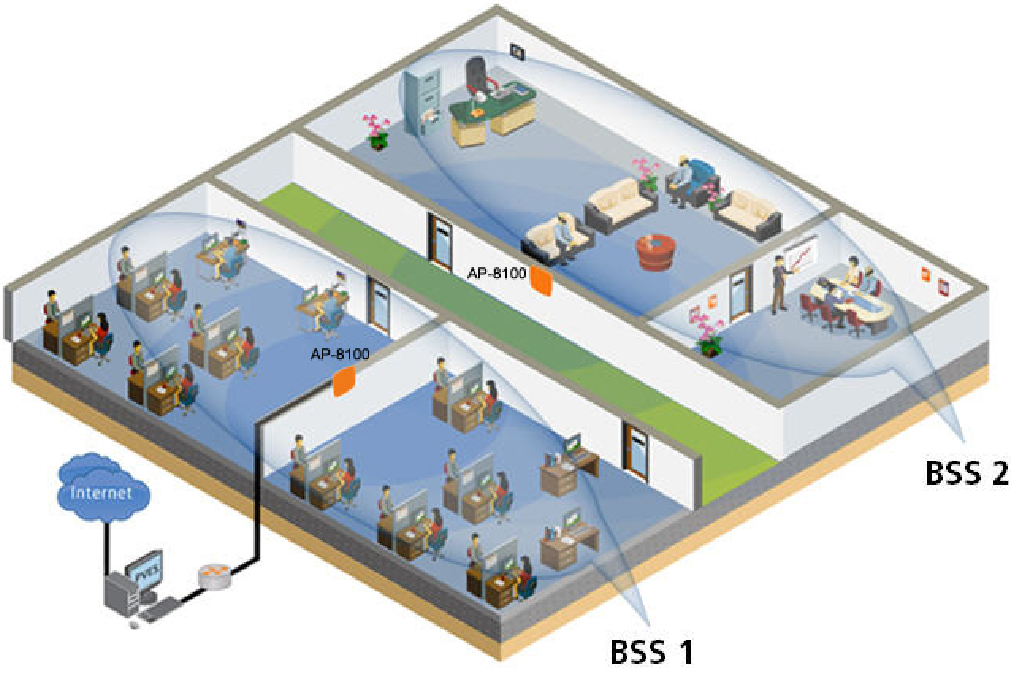


Figure 1-3 Extended Coverage Areas - Wireless Distribution Systems

1.3 Multiple-Input-Multiple-Output

ORiNOCO® 802.11n AP Devices support Multiple-Input-Multiple-Output (MIMO) antenna technology that uses multiple antennas at both the transmitting end and receiving end to improve communication performance. The underlying technology of these access point radio(s) are based on a combination of MIMO and OFDM (Orthogonal Frequency Division Multiplexing). MIMO-OFDM combination radios solve interference, fading and multipath problems. Having multiple receivers at the receiving end, increases the amount of received power and also reduces multipath problems by combining the received signals for each frequency component separately. Hence, MIMO significantly improves the overall gain.

MIMO also uses Spatial multiplexing transmission technique to transmit independent and separately encoded data signals from each of the multiple transmit antennas while reusing or multiplexing in the space dimension. These independent data signals are called Spatial streams. The transmitting end of the device uses multiple radio Tx chains and signal paths to simultaneously transmit different data streams, whereas the receiving end combines the Rx signals resulting in higher throughput.

By increasing the number of receiving and transmitting antennas, the throughput of the channel increases linearly resulting in high spectral efficiency.

Management and Monitoring Capabilities 2

This chapter contains information on the following:

2.1 Managing and Monitoring Capabilities

A Network Administrator can use the following interfaces to configure, manage and monitor the device.

- Web (HTTP/HTTPS) Interface
- Command Line Interface (CLI) (Terminal Emulator Programs)
- Simple Network Management Protocol (SNMP) v1/v2c/v3
- ProximVision ES (PVES) [v2.3 and above]

2.1.1 Web (HTTP/HTTPS) Interface

The HTTP interface provides an easy access to configuration settings and network statistics from any computer on the network. You can access the HTTP Interface via your LAN (switch, hub and so on), internet, or with an ethernet cable connected directly to your computer's ethernet Port.

HTTPS interface provides an HTTP connection over a Secure Socket Layer (SSL). HTTPS allows the user to access the device in a secure fashion by using SSL over port 443. The device supports SSLv3 with a 128-bit encryption certificate maintained by the device for secure communication between the device and the HTTP client. All communications are encrypted by using the server and the client-side certificate.

2.1.2 Command Line Interface (CLI) (Terminal Emulators)

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure, manage and monitor the device. You can enter command statements, composed of CLI commands and their associated parameters. Statements may be issued from the keyboard for real time control, or from scripts that automate the configuration. For example, when downloading a file, an administrator enters the download CLI Command along with the IP Address, file name, and file type parameters.

2.1.2.1 Serial Connection

You can access the CLI over a HyperTerminal serial connection. HyperTerminal is a program that you can use to connect to other Computers, Telnet Sites, Bulletin Board Systems (BBS), Online Services, and Host Computers, by using either a modem or a null modem cable.

If you are using an RS-232 cable, verify the following information in the HyperTerminal serial port setup:

Port	COM1 (default)
Baud Rate	115200
Data	8-bit
Parity	None
Stop	1-bit
Flow Control	None

:

- *If you are using Windows 7 operating system, then use Terminal Emulator programs for serial connection.*
- *HyperTerminal Serial Connection is not applicable to AP-8100, as it does not have a serial port. However, you can access the CLI via your LAN (switch, hub and so on), internet, or with an ethernet cable connected directly to your computer's ethernet Port.*

2.1.2.2 Telnet

You can access the device through CLI by using Telnet. With Telnet, you can communicate with the device through your LAN (switch, hub and so on), Internet, or with an ethernet cable connected directly to your computer's ethernet port.

2.1.2.3 Secure Shell (SSH)

You can securely access the device through CLI by using Secure Shell (SSH). The device supports SSH version 2, for secure remote CLI (Telnet) sessions. SSH provides strong authentication and encryption of session data. The SSH server has host keys - a pair of asymmetric keys (a private key that resides on the device) and a public key that is distributed to clients that need to connect to the device. Clients need to verify that it is communicating with the correct SSH server.

: For details on configuring the device through CLI, please refer to the ORiNOCO® 802.11n Access Points - Reference Guide.

2.1.3 Simple Network Management Protocol (SNMP)v1/v2c/v3

You can also configure, manage and monitor the device by using the Simple Network Management Protocol (SNMP). This requires an SNMP Manager Program (sometimes called MIB browser) or a Network Manager program using SNMP. The device supports the following Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- PXM-SNMP.mib
- RFC-1213.mib
- RFC-1215.mib
- RFC-2571.mib
- RFC-2790.mib
- RFC-3412.mib
- RFC-3414.mib
- IEEE 802.11mib

The Enterprise MIB defines the read and read-write objects that can be viewed or configured by using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. All Read-Only (RO) and Read-Write (RW) parameters supported by the IEEE802dot11-MIB are as tabulated below.

S.No.	MIB Object Name	Access (RO / RW)
1	dot11StationID	RO
2	dot11PrivacyOptionImplemented	RO
3	dot11PowerManagementMode	RO
4	dot11DesiredSSID	RW
5	dot11DesiredBSSType	RO
6	dot11BeaconPeriod	RW
7	dot11DTIMPeriod	RW
8	dot11MultiDomainCapabilityImplemented	RO
9	dot11MultiDomainCapabilityEnabled	RO
10	dot11CountryString	RO
11	dot11AuthenticationAlgorithmsIndex	RO
12	dot11AuthenticationAlgorithm	RO
13	dot11AuthenticationAlgorithmsEnable	RO
14	dot11MACAddress	RO
15	dot11RTSThreshold	RW
16	dot11FragmentationThreshold	RW
17	dot11ManufacturerID	RO
18	dot11ProductID	RO
19	dot11ResourceTypeIDName	RO
20	dot11manufacturerName	RO
21	dot11manufacturerProductName	RO
22	dot11PHYType	RO
23	dot11CurrentRegDomain	RO
24	dot11TempType	RO
25	dot11RegDomainsSupportedIndex	RO
26	dot11RegDomainsSupportedValue	RO
27	dot11SupportedDataRatesTxIndex	RO
28	dot11SupportedDataRatesTxValue	RO
29	dot11SupportedDataRatesRxIndex	RO
30	dot11SupportedDataRatesRxValue	RO
31	dot11CurrentFrequency	RW

These MIB files are available on Proxim's web site at http://support.proxim.com. You need to compile one or more of the above MIBs into your SNMP program’s database before you can manage the device by using SNMP. The MIB can be opened with any text editor, such as Microsoft Word, Notepad, or WordPad.

: For details on configuring the device through the SNMP Interface, please refer to the ORiNOCO® 802.11n Access Points - Reference Guide.

2.1.4 ProximVision ES (PVES)

ProximVision ES (commonly known as PVES) is Proxim's Network Management System that helps to manage and administer your wireless network effectively and efficiently. ProximVision ES combines industry-leading functionality with an intuitive user interface, enabling Network Administrators and Help Desk staff to support and control a wireless network.

ProximVision ES offers you a single intelligent console from which you can manage, monitor, analyze and even configure your device. For more information, see ProximVision ES user guide available at http://support.proxim.com.

Tabulated below are the AP devices and the corresponding ProximVision ES firmware version supporting them.

AP	ProximVision ES
AP-800 (SW v4.0.x) AP-8000 (SW v4.0.x)	v2.3 and above
AP-8100 (SW v4.1.x)	V2.6.2 onwards

: For more details on configuring, managing and monitoring the device by using CLI or SNMP interfaces, we recommend you to refer the *ORiNOCO® 802.11n Access Points - Reference Guide*.

Device Initialization 3

This chapter contains information on the following:

3.1 Initialization

You can initialize the device either through CLI commands, Web Interface or SNMP Interface.

- To initialize the device by using CLI commands, connect a serial RS-232 cable to the **Serial Port** of the device.

  : AP-8100 does not have a serial port. However, you can initialize, configure, manage and monitor the device through CLI commands via Telnet/SSH.

- To initialize the device by using Web or SNMP interface, connect an ethernet cable to the **Ethernet Port** of the device.

For all the modes of connection, you will need to configure the IP address of the device. As each network is different, a suitable IP address on the network must be assigned to the device. This IP address helps you to configure, manage and monitor the device through the Web Interface, SNMP, or Telnet/CLI.

The device can either have a **static** IP or **dynamic** IP address. By default, the device obtains its IP address automatically through DHCP (dynamic IP address); or else, you must set the IP Address manually (static IP address).

To access the HTTP interface and configure the device, the device must be assigned an IP address, which is valid on its ethernet network. By default, the IP Address type is set to Dynamic. If there is no response from the DHCP server, then the device will fall back to the IP Address 169.254.128.132.

3.1.1 ScanTool

Proxim's ScanTool (Answer ID 1735) is a software utility that runs on Microsoft's Windows machine.

By using ScanTool, you can

- Scan devices within the local IP subnet, which respond to the ScanTool.

  : To scan a device in Bootloader mode by using ScanTool, see Bootloader CLI and Scan Tool.

- Obtain device's IP address
- Modify device's IP configuration parameters (IP Address, Address Type, Gateway, etc.)
- Switch between the network adapters, if there are multiple network adapters in the system.
- Launch the Web interface.

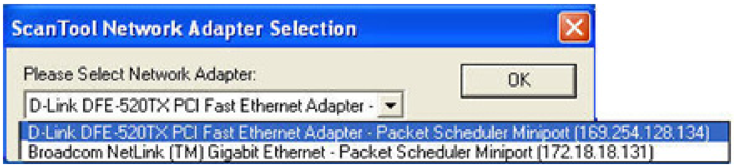
:

- *The user may need to disable Windows Firewall for ScanTool to function or to detect the radio.*
- *ScanTool works only for the Proxim products.*

3.1.2 Initialize the Device by using ScanTool

To scan and locate the devices on a network by using ScanTool, do the following:

1. Power on, or reset the device
2. To download Proxim's ScanTool, log on to Proxim's support site at http://support.proxim.com and search for ScanTool with (Answer ID 1735). Upon successful download, double-click the ScanTool icon on the Windows desktop to launch the program (if the program is not already running).
3. If your computer has more than one network adapter installed, you will be prompted to select the adapter that you want ScanTool to use. You can use either an ethernet or a wireless adapter. Select an adapter and click **OK**.

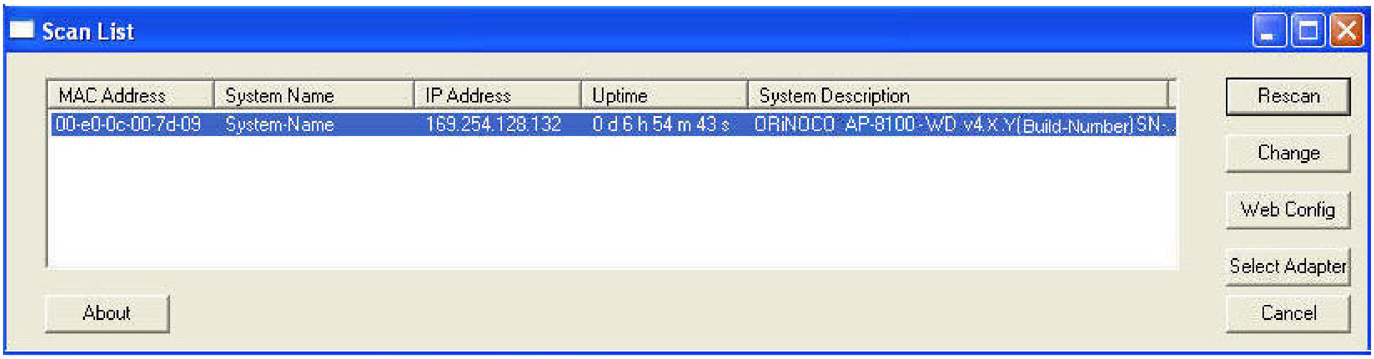

ScanTool Network Adapter Selection
Please Select Network Adapter:
OK

D-Link DFE-520TX PCI Fast Ethernet Adapter -

D-Link DFE-520TX PCI Fast Ethernet Adapter - Packet Scheduler Miniport (169.254.128.134)

Broadcom NetLink (TM) Gigabit Ethernet - Packet Scheduler Miniport (172.18.18.131)

4. The **Scan List screen** appears.



MAC Address	System Name	IP Address	Uptime	System Description
00-e0-0c-00-7d-09	System-Name	169.254.128.132	0 d 6 h 54 m 43 s	ORiNOCO AP-8100-WD v4.X.Y(Build-Number) SN-...

Figure 3-1 Scan List

5. ScanTool scans the subnet and displays a list of detected devices in the Scan List. You can change your adapter setting at any time by clicking the **Select Adapter** on the **Scan List** screen.
6. The screen contains the following information:
   - **MAC Address**
   - **System Name**
   - **IP Address**
   - **Uptime**
   - **System Description**: System Description contains the following information.
     — Device Description (ORiNOCO® AP-8100-WD)
     — Firmware Version v4.X.Y (v4.1.0)
     — Serial Number (SN-SN000000000000121212)

- — Bootloader Version (BL-V1.0.2)

7. Click **Select Adapter**, to change the adapter settings.
8. Locate the MAC address of the device you want to initialize from the Scan List and click **Web Config** to logon to the Web Interface. See Logging onto the Web Interface

:

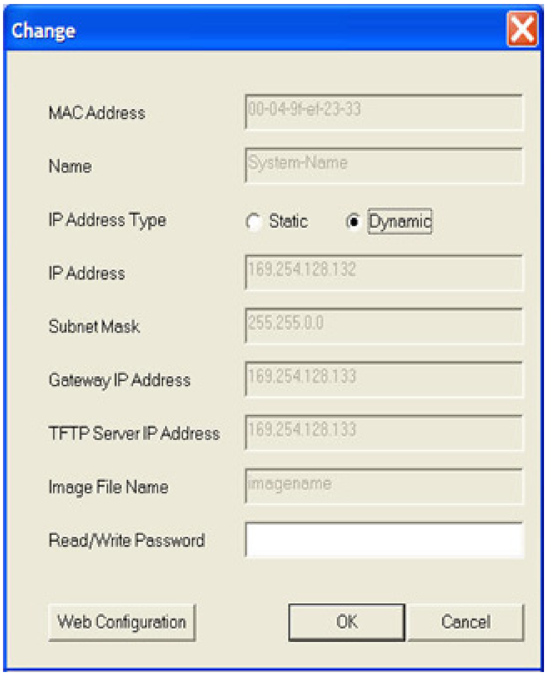
- *If device does not appear in the Scan List, click Rescan in the Scan List to update. If the device still does not appear in the list, see* Troubleshooting*.*
- *Note that after rebooting the device, it may take up to five minutes for the device to appear in the Scan List.*

3.1.3 Modifying the IP Address

The IP address assigned to the device can be obtained and, if required, can be changed to the IP address that is appropriate on the network. The ScanTool automatically detects the devices installed on the network segment, regardless of the IP address, and enables the configuration of each device's IP settings

By using ScanTool, you can change the IP address of the device as explained below:

1. Select the device details from the Scan List and click **Change**. A **Change** screen appears as shown in the following figure.



MAC Address: 00-04-9f-ef-23-33
Name: System-Name
IP Address Type: ○ Static ● Dynamic
IP Address: 169.254.128.132
Subnet Mask: 255.255.0.0
Gateway IP Address: 169.254.128.133
TFTP Server IP Address: 169.254.128.133
Image File Name: imagename
Read/Write Password:

Figure 3-2 Modifying the IP Address

2. The system automatically generates the **MAC address**, **System Name**, **TFTP Server IP Address** and **Image File Name** of the device.

3.1.3.1 Assigning the IP Address Manually

1. Select the **IP Address Type** as **Static** and enter the appropriate **IP Address**, **Subnet Mask**, and the **Gateway IP Address** parameters.
2. Enter the SNMP Read/Write password in the **Read/Write Password** field. By default, it is **public**.

3. Click **OK** to save the changes.
4. Click **Rescan** to verify the changes applied.

3.1.3.2 Assigning the IP Address Dynamically

*: Before setting the IP Address Type as **Dynamic**, ensure there is a DHCP server on the network.*

To change the IP Address type from Static to Dynamic, follow these steps:

1. Select the **IP Address Type** as **Dynamic.** The **IP Address**, **Subnet Mask** and the **Gateway IP Address** fields get disabled.
2. Enter the SNMP Read/Write password in the **Read/Write Password** field. By default, it is **public**.
3. Click **OK** to save the changes.
4. Click **Rescan** to verify the changes applied.

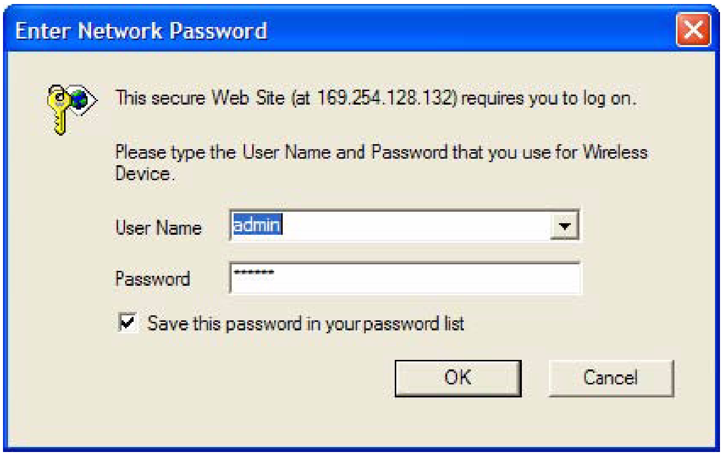
*: The device automatically reboots after clicking **OK**.*

To log on to the Web Interface, click **Web Config**.The user is then prompted to enter its username and password. For more information on how to login, please see Logging onto the Web Interface

3.2 Logging onto the Web Interface

Once the device is connected to your network, use a web browser to configure, manage and monitor the device. Enter the device IP address (For example http://169.254.128.132) in the address bar or access the Web Interface by using ScanTool.

The user is prompted to enter the username and password. The default User Name is **admin** and Password is **public**.



Enter Network Password

This secure Web Site (at 169.254.128.132) requires you to log on.

Please type the User Name and Password that you use for Wireless Device.

User Name: admin

Password: *******

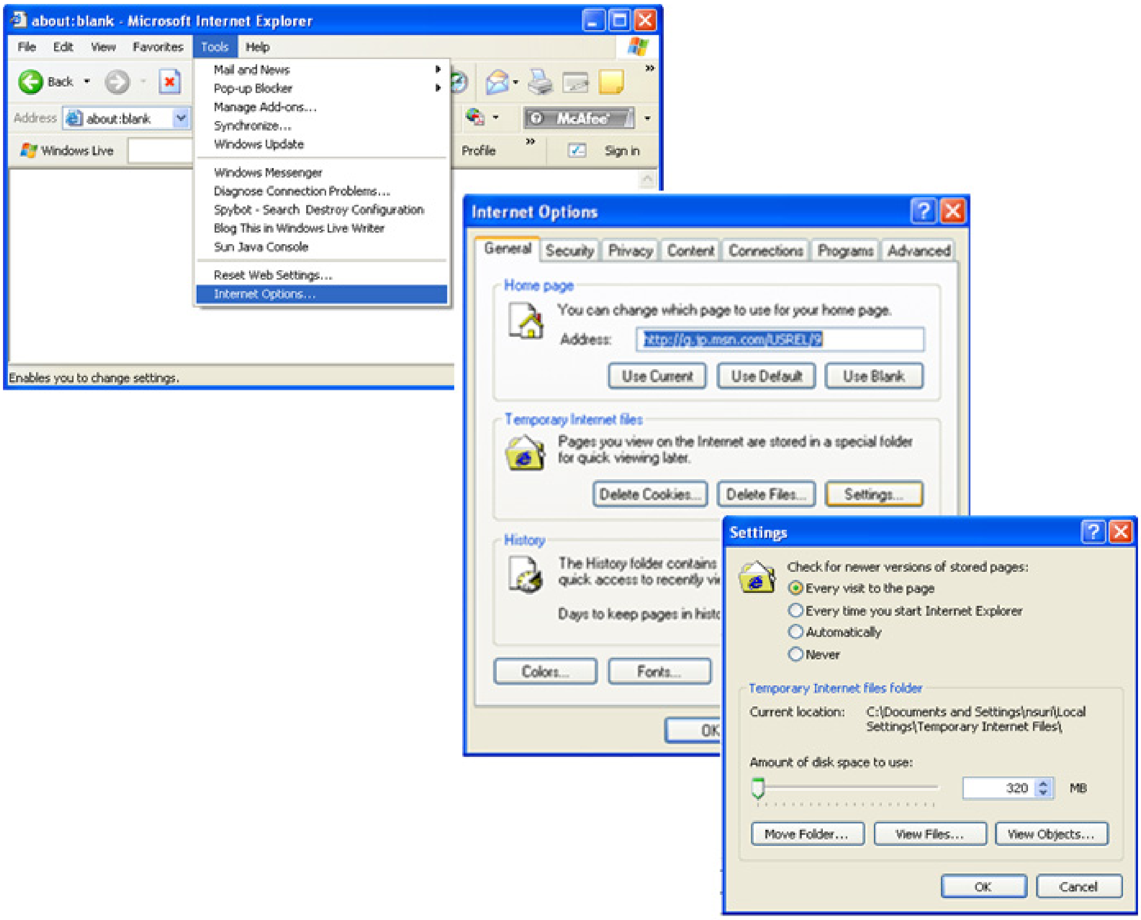
☑ Save this password in your password list

Figure 3-3 Login Screen

:

- *For security purposes, it is recommended to change the default **Password** to restrict unauthorized access to the device.*
- *Depending on the settings made during the device initialization, the IP address may be either a dynamic IP address assigned by a network DHCP server or a static IP address which is manually configured. Refer to ScanTool for information on how to determine the device's IP address and manually configure a new IP address.*

- *If the connection is slow or unable to connect, use the Internet Explorer **Tools** option to ensure that you are not using a proxy server for the connection.*
- *If you are unable to log on to the configuration pages by using default user name and password, please check with the administrator or follow* Forced Reload *procedures.*
- *If using Internet Explorer, and you enter wrong password consecutively for three times, the HTTP session will get disconnected. If case of other browsers, the login screen will reset until you enter the correct password.*
- *In the Internet Explorer, to get best results, navigate to **Tools** > **Internet Options** > **General**. Click **Settings** in the Browsing History and select "**Every visit to the webpage**".*



Enables you to change settings.

You can change which page to use for your home page.

Address: http://g.ip.msn.com/USREL/9

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains
quick access to recently vi

Days to keep pages in histo

Check for newer versions of stored pages:

● Every visit to the page
○ Every time you start Internet Explorer
○ Automatically
○ Never

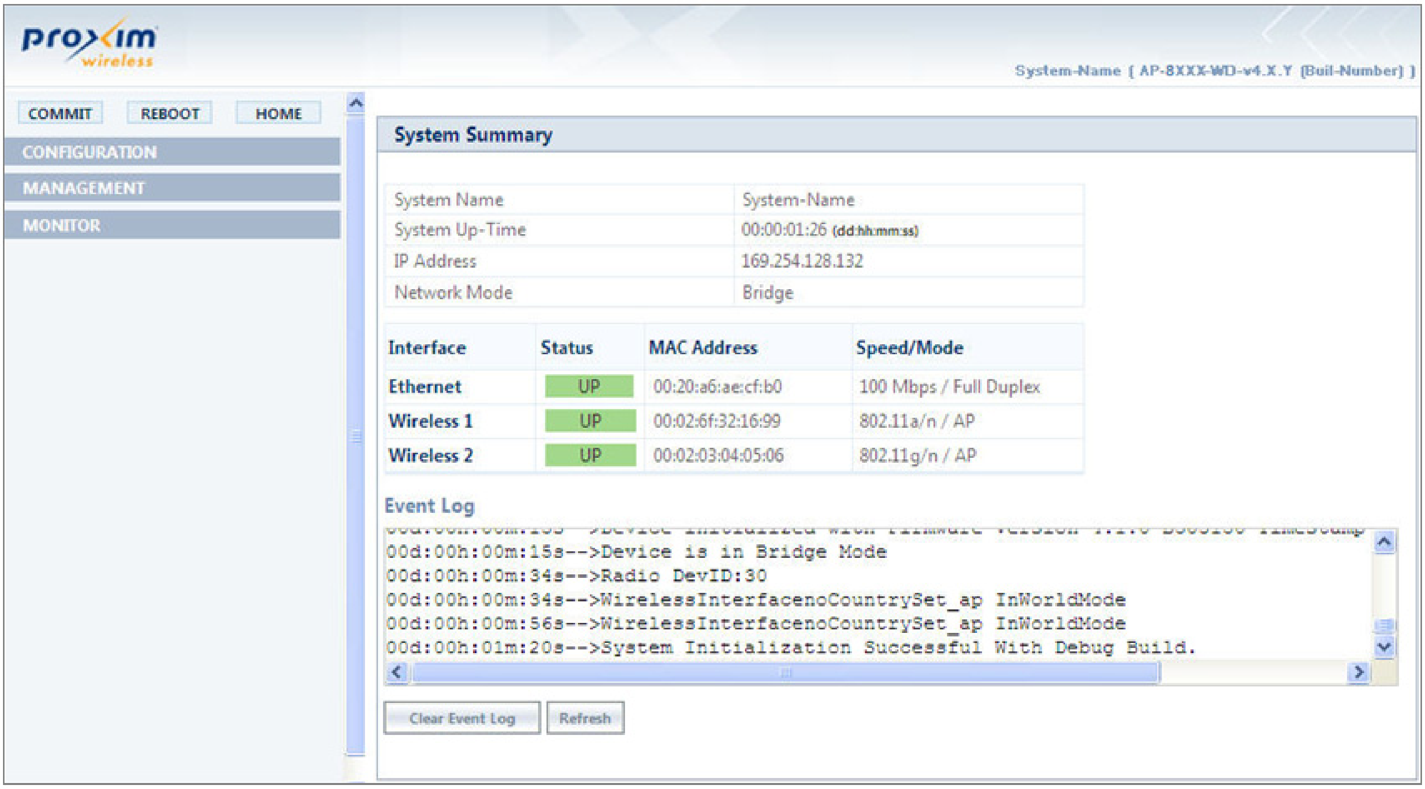
Current location: C:\Documents and Settings\nsuri\Local Settings\Temporary Internet Files\

Amount of disk space to use: 320 MB

Figure 3-4 Internet Explorer Settings

3.3 Home Page

Upon successful login, the **Home Page** screen appears.



System-Name [AP-8XXX-WD-v4.X.Y (Buil-Number)]

System Summary

System Name	System-Name
System Up-Time	00:00:01:26 (dd:hh:mm:ss)
IP Address	169.254.128.132
Network Mode	Bridge

Interface	Status	MAC Address	Speed/Mode
Ethernet	UP	00:20:a6:ae:cf:b0	100 Mbps / Full Duplex
Wireless 1	UP	00:02:6f:32:16:99	802.11a/n / AP
Wireless 2	UP	00:02:03:04:05:06	802.11g/n / AP

Event Log

```
00d:00h:00m:15s-->Device is in Bridge Mode
00d:00h:00m:34s-->Radio DevID:30
00d:00h:00m:34s-->WirelessInterfacenoCountrySet_ap InWorldMode
00d:00h:00m:56s-->WirelessInterfacenoCountrySet_ap InWorldMode
00d:00h:01m:20s-->System Initialization Successful With Debug Build.
```

Figure 3-5 System Summary

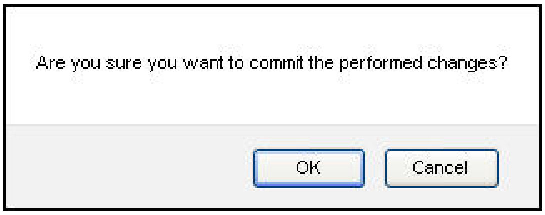
The home page contains the following information:

1. **Device Description**: The device description is displayed on the top-right corner of the home page. It displays the system-name, device type, regulatory domain, latest software version supported and firmware version loaded on the device.
2. **System Summary**: The System Summary screen displays the summary of system information such as System Name, IP Address, Network Mode, Interface Status, MAC Address, Event Log, etc.
3. **COMMIT**: See Commit
4. **REBOOT**: See Reboot
5. **HOME**: Displays the System Summary Screen.
6. **CONFIGURATION**: The CONFIGURATION tab allows the user to configure the set of parameters required for a device to be operational and establish link in the network. For more details, see Device Configuration.
7. **MANAGEMENT**: The MANAGEMENT tab allows the user to manage the device. For more details, see Device Management
8. **MONITOR**: The MONITOR tab allows the user to monitor the device. For more details, see Device Monitoring

3.3.1 Commit

COMMIT operation is used to apply the configuration changes to the device. When changes are made to the configuration parameters of the device, the changes will not take effect, until the **COMMIT** is clicked. Some parameters may require system reboot for the changes to take effect. On clicking **COMMIT**, the system evaluates all the configuration dependencies and displays the configuration status.

Before applying commit, the system displays a confirmation message, as shown in the following figure:

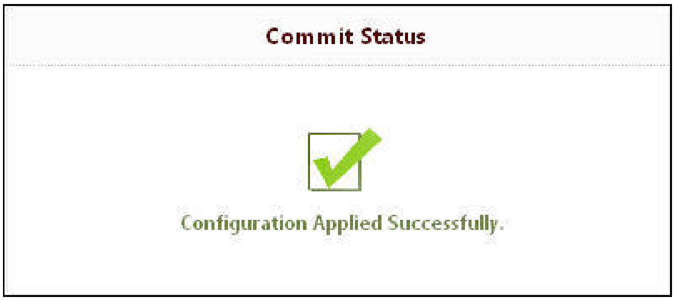


Are you sure you want to commit the performed changes?

Figure 3-6 Commit

Click **OK**, if you wish to commit the changed parameters.

On successful **Commit** operation, the following screen appears:

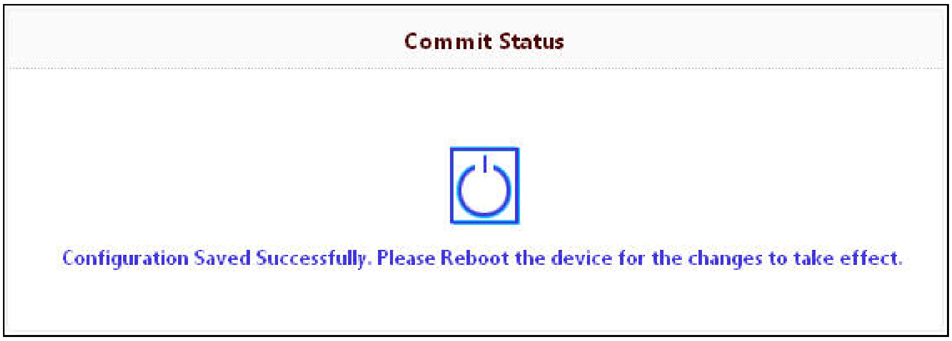


Commit Status

Configuration Applied Successfully.

Figure 3-7 Commit Status

If the configured parameters requires reboot, on committing the following screen appears.



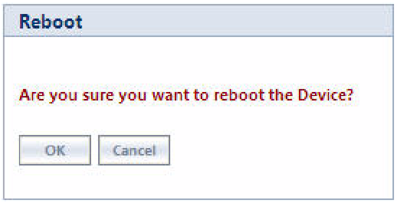
Commit Status

Configuration Saved Successfully. Please Reboot the device for the changes to take effect.

Figure 3-8 Commit Status with Reboot Message

3.3.2 Reboot

Reboot operation is required for any change in the key parameters to take effect. For example, settings such as configuring the Radio Mode, IP Address, and Network Mode need reboot to take effect. See Parameters requiring Reboot, for more details. On clicking **REBOOT**, system displays a confirmation window as shown below.



Reboot

Are you sure you want to reboot the Device?

Figure 3-9 Reboot

Click **OK**, if you want to reboot the device.

:

- *Every parameter requiring REBOOT upon its configuration, is marked with a red asterisk and it is recommended to reboot the device immediately after modifying a rebootable parameter.*
- *If the device does not reboot and redirect you to the HOME Page within 2 minutes, then we recommended you to check the network connectivity and try accessing the page later.*

4 Basic Configuration

This chapter contains information on the following:

- Basic Configuration
- Factory Default Configuration
- Parameters requiring Reboot

❗: All the interface (radio) 2 parameters discussed in this chapter are applicable only to a dual-radio device.

4.1 Basic Configuration

Tabulated below are the parameters to be configured to operate the AP device at a basic level:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>IP Address</td><td>If you have DHCP Server on your network, then set the Address Type as <b>Dynamic</b>. When set to Dynamic, the device gets its IP Address from the DHCP Server. If there is no response from the DHCP Server, then the device will fall back to 169.254.128.132.
If you do not have the DHCP Server on your network, change the Address Type as <b>Static</b>. For details on how to configure the Address Type and the IP address, refer to IP Configuration</td></tr>
<tr><td>Country Code</td><td>Select a country from the drop down menu. For more details on how to configure the Country Code, refer to Properties</td></tr>
<tr><td>Radio Mode</td><td>By default, the radio mode on both <b>Radio1 (Interface1)</b> and <b>Radio 2 (Interface 2)</b> is set to AP. For details on how to configure the radio mode, refer to Properties</td></tr>
<tr><td>Operational Mode</td><td>Default Operational Mode set on both the radios, is as tabulated below:
<table>
<tr><th rowspan="2">Device Type</th><th colspan="2">Operational Mode</th></tr>
<tr><th>Radio 1</th><th>Radio 2</th></tr>
<tr><td><b>AP-800</b></td><td>802.11g/n</td><td>Not Applicable</td></tr>
<tr><td><b>AP-8000</b></td><td>802.11a/n</td><td>802.11g/n</td></tr>
<tr><td><b>AP-8100</b></td><td>802.11a/n</td><td>802.11g/n</td></tr>
</table>
For details on how to change the operational mode, refer to Properties</td></tr>
<tr><td>Current Bandwidth</td><td>By default, the current bandwidth is set to 40 MHz. For details on how to change the current bandwidth, refer to Properties</td></tr>
</table>

<table>
<tr><td>SSID</td><td>Default SSID set on both the radios, is as tabulated below:
<table>
<tr><th rowspan="2">Device Type</th><th colspan="2">SSID</th></tr>
<tr><th>Radio 1</th><th>Radio 2</th></tr>
<tr><td><b>AP-800</b></td><td>My Wireless Network 1_1</td><td>Not Applicable</td></tr>
<tr><td><b>AP-8000</b></td><td>My Wireless Network 1_1</td><td>My Wireless Network 2_1</td></tr>
<tr><td><b>AP-8100</b></td><td>My Wireless Network 1_1</td><td>My Wireless Network 2_1</td></tr>
</table>
For details on how to change SSID, refer to Virtual Access Point (VAP)</td></tr>
<tr><td>Security</td><td>By default, the security is set to <b>None</b>. For details, refer to Wireless Security</td></tr>
</table>

Ensure to COMMIT the configured changes and REBOOT the device.

4.2 Factory Default Configuration

Parameter	Default Values
User Name	admin
Password	public
System Name	System-Name
Network Mode	Bridge
IP Address Assignment Type	Dynamic
Fall Back IP Address	169.254.128.132
Subnet Mask	255.255.0.0
Gateway IP Address	169.254.128.133
Link Integrity Status	Disabled
STP Status	Disabled
Radio Mode	Radio1: AP Radio2: AP
Radio Status	Enabled
Country Code	NoCountry (World Regulatory Domain) US (US Regulatory Domain) JP (JP Regulatory Domain) UnitedKingdom (EU Regulatory Domain)

<table>
<tr><td>Operational Mode</td><td>
<table>
<tr><th rowspan="2">Device Type</th><th colspan="2">Operational Mode (Supported Frequency Band)</th></tr>
<tr><th>Radio 1</th><th>Radio 2</th></tr>
<tr><td><b>AP-800</b></td><td>802.11g/n (2.4 GHz)</td><td>Not Applicable</td></tr>
<tr><td><b>AP-8000</b></td><td>802.11a/n (5 GHz)</td><td>802.11g/n (2.4 GHz)</td></tr>
<tr><td><b>AP-8100</b></td><td>802.11a/n (5 GHz)</td><td>802.11g/n (2.4 GHz)</td></tr>
</table>
</td></tr>
<tr><td>Current Bandwidth</td><td>40 MHz</td></tr>
<tr><td>VAP SSID</td><td>
<table>
<tr><th rowspan="2">Device Type</th><th colspan="2">SSID</th></tr>
<tr><th>Radio 1</th><th>Radio 2</th></tr>
<tr><td><b>AP-800</b></td><td>My Wireless Network 1_1</td><td>Not Applicable</td></tr>
<tr><td><b>AP-8000</b></td><td>My Wireless Network 1_1</td><td>My Wireless Network 2_1</td></tr>
<tr><td><b>AP-8100</b></td><td>My Wireless Network 1_1</td><td>My Wireless Network 2_1</td></tr>
</table>
</td></tr>
<tr><td>Wireless Distribution System (WDS)</td><td>Disabled</td></tr>
<tr><td>Local MAC Authentication</td><td>Disabled</td></tr>
<tr><td>RADIUS MAC Authentication</td><td>Disabled</td></tr>
<tr><td>RADIUS Accounting</td><td>Disabled</td></tr>
<tr><td>RADIUS Server Profile</td><td>Enabled with Profile Name “Default Radius”</td></tr>
<tr><td>VLAN Status</td><td>Disabled</td></tr>
<tr><td>RADIUS VLAN Status</td><td>Disabled</td></tr>
<tr><td>Security Profile Name</td><td>AP Security</td></tr>
<tr><td>QoS Profile Name</td><td>Default</td></tr>
<tr><td>Security Auth Mode</td><td>None</td></tr>
<tr><td>Global Filtering</td><td>Disabled</td></tr>
<tr><td>Proxy ARP Status</td><td>Disabled</td></tr>
<tr><td>Packet Forwarding</td><td>Disabled</td></tr>
<tr><td>DHCP Server Status</td><td>Disabled</td></tr>
<tr><td>SNMP Management Interface</td><td>Enabled with SNMPv1-v2c</td></tr>
<tr><td>Telnet Management Interface</td><td>Enabled with login “admin” and password “public”</td></tr>
</table>

4.3 Parameters requiring Reboot

If you have configured any of the parameters (marked with an asterisk) tabulated below, then reboot the device.

Parameter(s)	Web Page(s)
Address Type	**CONFIGURATION** - > **Network** - > **IP Configuration**
IP Address	
Subnet Mask	
Gateway IP Address	
DNS Primary IP and Secondary IP Address	
Radio Mode	**CONFIGURATION** - > **Wireless** - > **Interface 1**/ **Interface 2** - > **Properties**
Country Code	
Operational Mode	
Current Bandwidth	
Frequency Extension	**CONFIGURATION** - > **Wireless** - > **Interface 1**/ **Interface 2** - > **11n Properties**
Update Firmware (HTTP / TFTP)	**MANAGEMENT** - > **File Management** - > **Update Firmware**
Update Configuration (HTTP / TFTP)	**MANAGEMENT** - > **File Management** - > **Update Configuration**
Password	**MANAGEMENT** - > **Services** - > **HTTP / HTTPS**
HTTP	
HTTP Port	
HTTPS	
Password	**MANAGEMENT** - > **Services** - > **Telnet / SSH**
Telnet	
Telnet Port	
Telnet Sessions	
SSH	
SSH Port	
SSH Sessions	
SNMP	**MANAGEMENT** - > **Services** - > **SNMP**
Version	
Read Password	
Read / Write Password	
Access Table Status	**MANAGEMENT** - > **Access Control**

5 Device Configuration

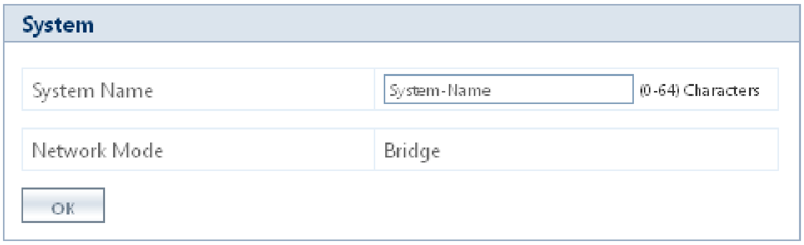
This chapter explains the step-by-step procedure to configure the following features on the device, by using Web Interface:

- System
- Network
  - IP Configuration
  - Link Integrity
  - Spanning Tree Protocol (STP)
- Ethernet
- Wireless Interface
  - Interface 1
    - Properties
    - 11n Properties
    - Virtual Access Point (VAP)
  - Interface 2
- Security
  - Wireless Security
  - RADIUS
  - MAC Access Control
- Quality of Service (QoS)
  - Enhanced Distributed Channel Access (EDCA)
  - 802.1d to IP DSCP
  - 802.1d to 802.1p
  - QoS Profile
  - QoS Policy
- Virtual Local Area Network (VLAN)
  - VLAN Ethernet Configuration
- Filters
  - Protocol Filters
  - Static MAC Address Filters
  - Advanced Filters
  - TCP/UDP Port Filters
  - Storm Threshold Filters
  - Packet Forwarding
- DHCP
  - DHCP Server

❗ **: All the interface (radio) 2 parameters discussed in this chapter are applicable only to a dual-radio device.**

5.1 System

The **System** feature enables you to configure system specific information. Navigate to **CONFIGURATION > System**. The **System** screen appears.



System

System Name: System-Name (0-64) Characters

Network Mode: Bridge

Figure 5-1 System

Tabulated below are ‘System’ parameters and the method to configure the configurable parameters:

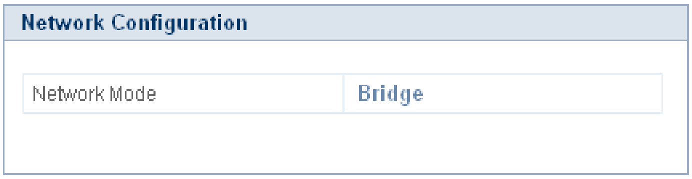
Parameter	Description
System Name	Specifies the name assigned to the device. To assign a name to the device, enter a name in the **System Name** box. You can enter a name of maximum 64 characters.
Network Mode	Specifies the network mode of the device. The device supports only Bridge mode.

Click **OK** and **COMMIT**, to save the configured parameters.

5.2 Network

The **Network** feature displays the network specific information of the device.

To view the network mode, navigate to **CONFIGURATION** > **Network**. The **Network Configuration** screen appears.



Network Configuration

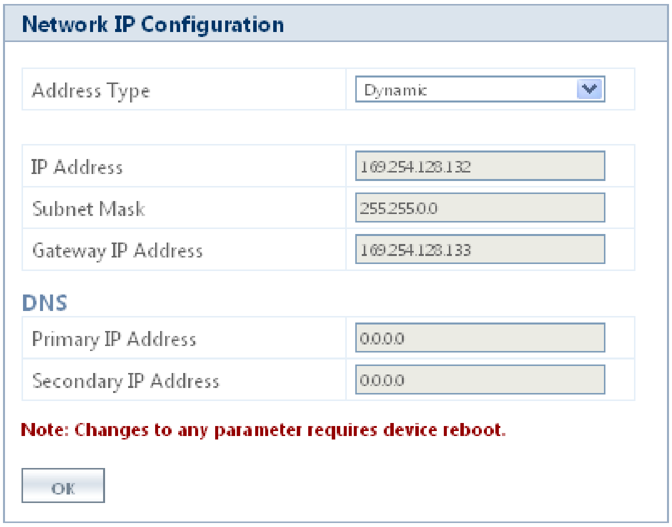
Network Mode: Bridge

Figure 5-2 Network Configuration

The device supports only Bridge mode.

5.2.1 IP Configuration

The **IP Configuration** feature enables you to configure the TCP/IP settings of the device on a network. Navigate to **CONFIGURATION** > **Network** > **IP Configuration**. The **Network IP Configuration** screen appears.



Network IP Configuration

Address Type: Dynamic

IP Address: 169.254.128.132

Subnet Mask: 255.255.0.0

Gateway IP Address: 169.254.128.133

DNS

Primary IP Address: 0.0.0.0

Secondary IP Address: 0.0.0.0

Note: Changes to any parameter requires device reboot.

Figure 5-3 Network IP Configuration

Tabulated below are 'Network IP' parameters and the method to configure the configurable parameters:

Parameter	Description
Address Type	By default this parameter is set to **Dynamic**. When set to dynamic, the device will obtain IP settings from a network Dynamic Host Configuration Protocol (DHCP) server automatically during the boot-up. If you do not have a DHCP server or if you want to manually configure the device IP address, set this parameter to **Static**.
IP Address	Specifies the IP Address of the device. When the address type is set to **Dynamic**, this parameter is read-only and displays the device's current IP address obtained from the DHCP server. The device will be set to the default IP address 169.254.128.132, if the device cannot obtain the IP address from a DHCP server. If the Address Type is set to **Static** then you will have to manually enter the IP Address in the **IP Address** box.
Subnet Mask	Specifies the device subnet mask. When the address type is set to **Dynamic**, this parameter is read-only and displays the device current subnet mask obtained from the DHCP server. The device will be set to the default subnet mask 255.255.0.0, if the device cannot obtain the subnet mask from a DHCP server. If the Address Type is set to **Static** then you will have to manually enter the subnet mask in the **Subnet Mask** box.
Gateway IP Address	Specifies the IP address of the device gateway. When address type is set to **Dynamic**, this parameter is read-only and displays the IP address of the device gateway. The device will be set to the default Gateway IP address 169.254.128.133, if it cannot obtain the gateway IP address from a DHCP server. If the Address Type is set to **Static** then you will have to manually enter the gateway IP address in the **Gateway IP Address** box.

Primary IP Address	Specifies the IP Address of the Primary DNS Server. When the address type is set to **Dynamic**, this parameter is read-only and displays the DNS Primary IP Address obtained from the DHCP server. If the Address Type is set to **Static** then you will have to manually enter the IP Address in the **Primary IP Address** box.
Secondary IP Address	Specifies the IP Address of the Secondary DNS Server. When the address type is set to **Dynamic**, this parameter is read-only and displays the DNS Secondary IP Address obtained from the DHCP server. If the Address Type is set to **Static** then you will have to manually enter the IP Address in the **Secondary IP Address** box.

Click **OK** and **COMMIT**, to save the configured parameters.

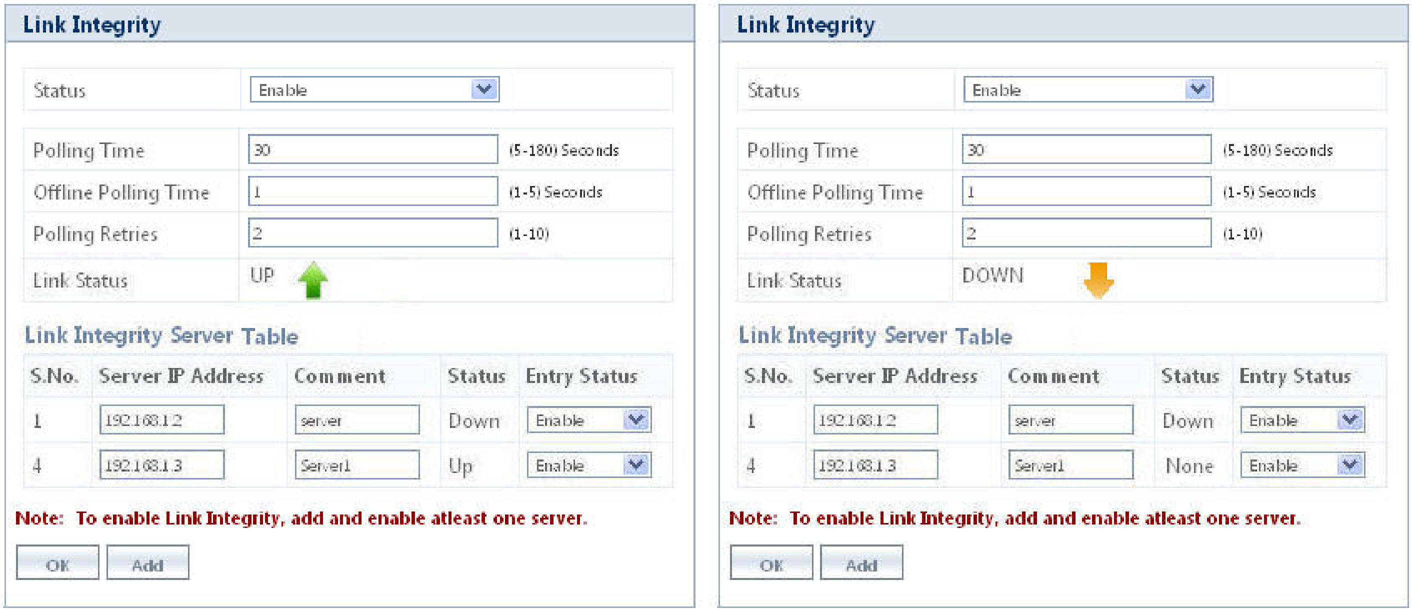
: If you have changed any of the TCP/IP parameters, then reboot the device.

5.2.2 Link Integrity

Link Integrity helps you to check connectivity between the AP device and its pre-configured servers (routers, gateway devices and other devices in the vicinity), by sending ICMP (Internet Control Message Protocol) echo probes periodically. If the device receives an acknowledgment from a server within the configured time interval, then the link between that server and the AP device is active and the link integrity status is set to UP, otherwise it is set to DOWN.

If atleast one server responds back, then the over all Link Status is set to UP and the device performs standard AP functionality. If all the servers configured fail to respond, then the over all Link Status is set to DOWN and all the VAPs enabled in AP mode are disabled. (VAPs in WDS mode remain unaffected. See Virtual Access Point (VAP)). The VAPs in AP mode resume as Link Status is set to UP.

Navigate to **CONFIGURATION** > **Network** > **Link Integrity**. The **Link Integrity** screen appears.



Link Integrity

Status	Enable	
Polling Time	30	(5-180) Seconds
Offline Polling Time	1	(1-5) Seconds
Polling Retries	2	(1-10)
Link Status	UP	

Link Integrity Server Table

S.No.	Server IP Address	Comment	Status	Entry Status
1	192.168.1.2	server	Down	Enable
4	192.168.1.3	Server1	Up	Enable

Note: To enable Link Integrity, add and enable atleast one server.

Link Integrity

Status	Enable	
Polling Time	30	(5-180) Seconds
Offline Polling Time	1	(1-5) Seconds
Polling Retries	2	(1-10)
Link Status	DOWN	

Link Integrity Server Table

S.No.	Server IP Address	Comment	Status	Entry Status
1	192.168.1.2	server	Down	Enable
4	192.168.1.3	Server1	None	Enable

Note: To enable Link Integrity, add and enable atleast one server.

Figure 5-4 Link Integrity

Tabulated below are ‘Link Integrity’ parameters and the method to configure the configurable parameters:

Parameter	Description
Status	Specifies the status of the link integrity feature on the device. By default, it is disabled. To enable, select **Enable** from the drop down menu.
Polling Time	Specifies the time interval, during which the device will check the link integrity with its configured server(s) by sending the ICMP echo probes. By default, the **Polling Time** is 30 seconds. To configure, enter the time interval between 5 seconds - 180 seconds.
Offline Polling Time	Specifies the time interval, during which the device will send the ICMP echo probes to server(s) in offline mode (When the Link status is DOWN). By default, the **Offline Polling Time** is 1 second. To configure, enter the time interval between 1 second - 5 seconds
Polling Retries	Specifies the number of attempts made by the device in sending the ICMP echo probes to the server(s), before declaring the overall link status as DOWN. By default, the **Polling Retries** taken is 2. To configure, enter the number of attempts between 1-10
Link Status	Specifies the connectivity status between a server and a device. Link Status can either be UP, DOWN or NONE. – **UP:** Specifies the status of the link when AP device receives the server’s acknowledgment. – **DOWN:** Specifies the status of the link when AP device does not receive the server’s acknowledgment. – **NONE:** Specifies the status of the link when the AP device is trying to connect to the server(s), that is when the Link Status is neither UP nor DOWN.

Click **OK** and **COMMIT**, to save the configured parameters.

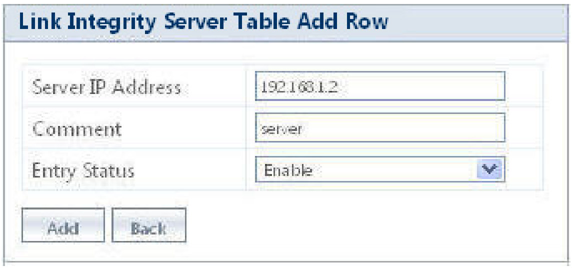
5.2.2.1 Link Integrity Server Table

The Link Integrity Server Table displays the list of pre-configured servers. Atleast one server should be added to the table, to enable the link integrity feature on the device.

Link Integrity Server Table - Add Row

To add a server:

1. Click **Add** in the Link Integrity screen, the **Link Integrity Server Table - Add Row** screen appears.



Link Integrity Server Table Add Row

Server IP Address	192.168.1.2
Comment	server
Entry Status	Enable

Figure 5-5 Link Integrity Server Table - Add Row

2. Configure the following properties:

Parameter	Description
Server IP Address	Specifies the IP Address of the configured server.
Comment	Specifies the user comment on the configured server.
Entry Status	Specifies the entry status of the server. By default, it is disabled. To configure, set the entry status as **Enable**/**Disable**/**Delete** from the drop down menu. – **Enable**: Enables the server added. – **Disable**: Disables the server added. – **Delete**: Deletes the server added.

Click **OK** and **COMMIT**, to save the configured parameters.

: A maximum of five servers can be added.

5.2.3 Spanning Tree Protocol (STP)

The Spanning Tree Protocol (STP) helps to avoid bridged loops in a wireless network and ensures a loop-free topology for bridged LAN (connected on both wireless and ethernet interface). Following is the step-by-step procedure explaining how STP feature works:

a. **Disable**: In this state, STP is disabled and no traffic is allowed through wireless and ethernet interfaces of the bridged LAN.

b. **Listening**: When STP is enabled, the AP devices exchange Bridge Protocol Data Unit (BPDU) packets in listening state. These BPDU packets contain Bridge Priority and MAC address information, based on which a *Root Bridge* and *Designated Bridge* are selected.

   - **Root Bridge**: It is the device that has the lowest MAC address or highest priority. Based on a Root Bridge, the shortest low cost path is selected and alternate high cost paths are blocked, therefore avoiding loops on the network. Root Bridge transmits the network topology information continuously to other bridges on the network.
   - **Designated Bridge:** It is the device closest to the Root Bridge and is responsible for forwarding the data towards the root port of the root bridge. Designated Bridge determines the shortest low cost path to the destination, via root port. All the other devices in the network other than Root Bridge, act as Designated Bridge.

c. **Learning**: Once the Root Bridge and Designated Bridge are selected, all the devices learn and update the Bridge Priority and MAC address information in their learn table. Designated Bridge determines the shortest low cost path via root port, to forward the packets to the destination.

d. **Blocking**: After selecting the low cost path, the device blocks and disables all the other high cost paths active on other interfaces. Once the path is blocked, no traffic is allowed via that high cost path.

e. **Forwarding**: The device easily forwards the data packet to the destination via single low cost path selected, with zero loops and interference on the bridged network.

: The state of the port must change from blocking state to listening and learning state, before it can change to the forwarding state.

Example: Let us consider a network with three Bridges (Bridge 1, Bridge 2 and Bridge 3)

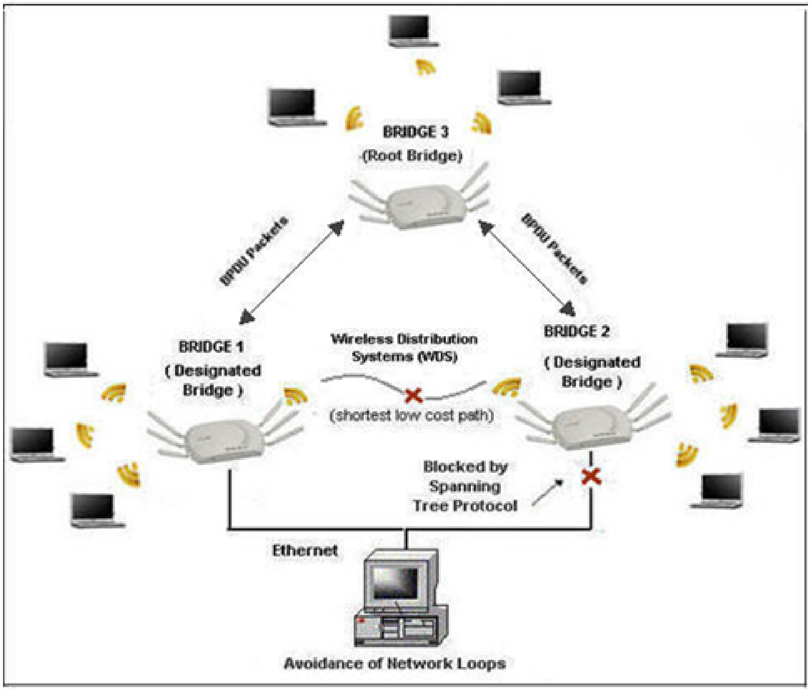
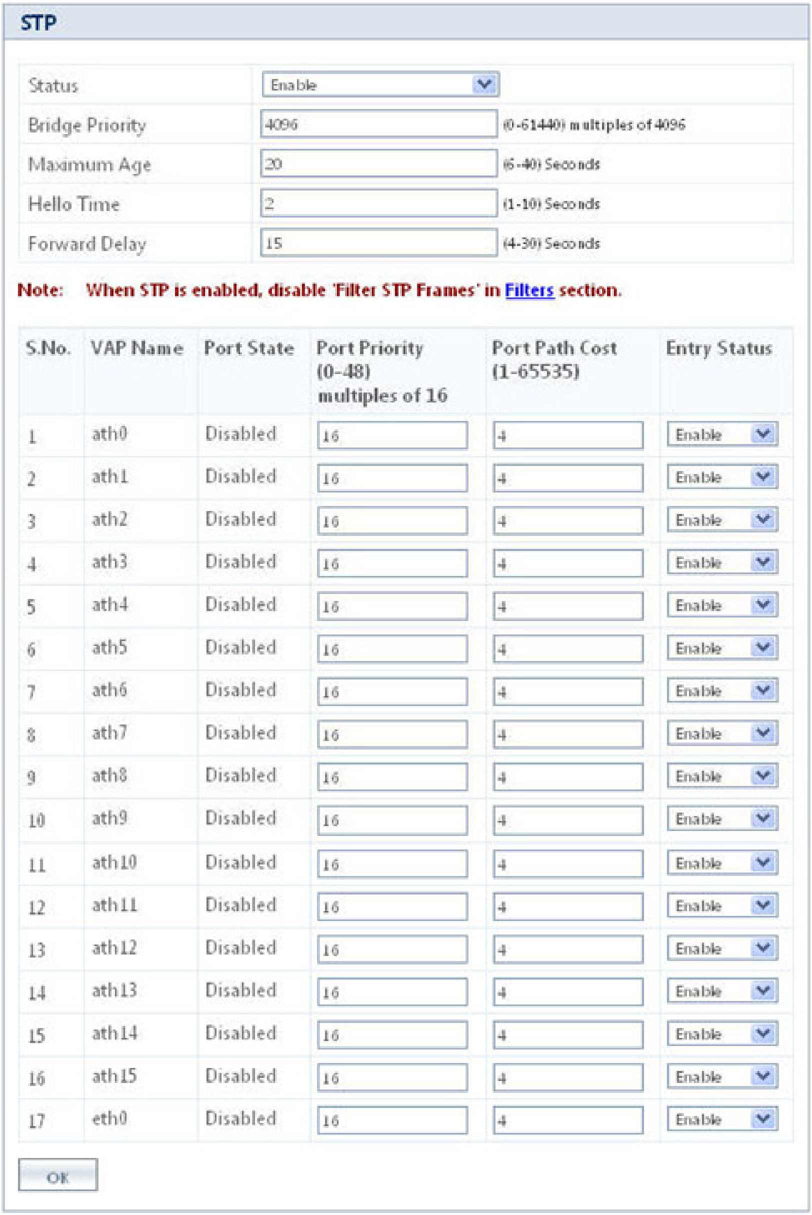


Figure 5-6 STP Topology

- Bridge 1 and Bridge 2 are connected via both Wireless and Ethernet interface, while Bridge 3 is connected to Bridge 1 and Bridge 2 only via Wireless interface.
- To avoid a network loop between Bridge 1 and Bridge 2, the STP feature should be enabled on all the devices.
- Once the STP feature is enabled, Bridge 1, Bridge 2 and Bridge 3 change from **Disable** state to **Listening** state and start exchanging the BPDU packets. Bridge 3, having the highest priority and smallest MAC address, acts as the **Root Bridge**, and Bridge 1 and Bridge 2 act as **Designated Bridges**.
- The Designated Bridges (Bridge 1 and Bridge 2) then determine the shortest low cost path via root port, to forward the data from bridge 1 to bridge 2, on a loop- free bridged network.
- Bridge 1 and Bridge 2 switch from **Listening** state to **Learning** state where they update the learn tables and enable the shortest low cost path determined.
- The STP enabled Bridge 2 then changes from **Learning** state to **Blocking** state and blocks all the longest high cost paths, near both wireless and ethernet interfaces.
- Bridge 1 finally changes from **Learning** state to **Forwarding** state and forwards the data packet to Bridge 2 through the shortest low cost path (via the root port of Bridge 3) enabled, avoiding loops on the network.

Navigate to **CONFIGURATION** > **Network** > **STP**. The **Network STP Configuration** screen appears.



STP

Status	Enable	
Bridge Priority	4096	(0-61440) multiples of 4096
Maximum Age	20	(6-40) Seconds
Hello Time	2	(1-10) Seconds
Forward Delay	15	(4-30) Seconds

Note: When STP is enabled, disable 'Filter STP Frames' in Filters section.

S.No.	VAP Name	Port State	Port Priority (0-48) multiples of 16	Port Path Cost (1-65535)	Entry Status
1	ath0	Disabled	16	4	Enable
2	ath1	Disabled	16	4	Enable
3	ath2	Disabled	16	4	Enable
4	ath3	Disabled	16	4	Enable
5	ath4	Disabled	16	4	Enable
6	ath5	Disabled	16	4	Enable
7	ath6	Disabled	16	4	Enable
8	ath7	Disabled	16	4	Enable
9	ath8	Disabled	16	4	Enable
10	ath9	Disabled	16	4	Enable
11	ath10	Disabled	16	4	Enable
12	ath11	Disabled	16	4	Enable
13	ath12	Disabled	16	4	Enable
14	ath13	Disabled	16	4	Enable
15	ath14	Disabled	16	4	Enable
16	ath15	Disabled	16	4	Enable
17	eth0	Disabled	16	4	Enable

Figure 5-7 STP Configuration

Tabulated below are ‘STP’ parameters and the method to configure the configurable parameters:

Parameter	Description
Status	Specifies the status of the STP feature on the AP device. By default, STP is disabled. To enable, select **Enable** from the drop down menu. *: If you enable STP, disable 'Filter STP Frames' in Filters. See Filters.*

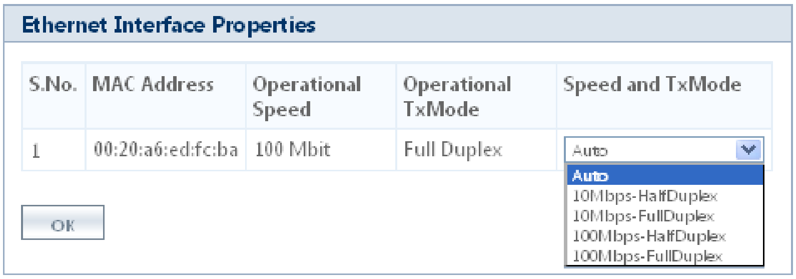
Bridge Priority	Specifies the priority assigned to a bridge. By default, a bridge is assigned with a priority of 4096. To configure, enter a value between 0 - 61440 (as multiples of 4096). *: Bridge assigned with the lowest value gets the highest priority, and is selected as Root Bridge.*
Maximum Age	Specifies the maximum time period for an AP device to hold the BPDU packet before discarding it. By default, it is 20 seconds. To configure, enter the **Maximum Age** between 6 seconds - 40 seconds.
Hello Time	Specifies the time interval in which the Root Bridge sends the BPDU packets periodically. By default, it is 2 seconds. To configure, enter the **Hello Time** between 1 second - 10 seconds.
Forward Delay	Specifies the time interval, for the bridge to be in **Learning** state and **Listening** state. By default, it is 15 seconds. To configure, enter the **Forward Delay** time between 4 seconds - 30 seconds. *: Forward Delay depends on the **Maximum Age**.*
VAP Name	Specifies the name of the VAP enabled with the STP feature.
Port State	Specifies the current state of the port, in which the AP device enabled with STP feature is functioning. **Port State** varies between **Disabled**, **Listening**, **Learning**, **Blocking** and **Forwarding**.
Port Priority	Specifies the priority assigned to a port, to participate in the STP process and act as a Root Port (port maintaining connectivity with root bridge, on the interface of an AP device). When the AP device experiences a tie in determining the low cost path towards root, it uses port priority value as a tiebreaker. By default, the **Port Priority** is 16. To configure, enter a value in the range of 0 - 48 (as multiples of 16). *: The state of the root port is always in **Forwarding** state.*
Port Path Cost	Specifies the cost of the path. Path cost is a pre-determined value of the IEEE 802.11 standards, based on the bandwidth and speed of that path. The port with the lowest path cost to the root bridge becomes the root port, gaining high priority. By default, the **Port Path Cost** is 4. To configure, enter a value in the range of 1 - 65535.

Entry Status	Specifies the status of the selected port. By default, the **Entry Status** is disabled. To enable, select **Enable** from the drop down menu.

Click **OK** and **COMMIT**, to save the configured parameters.

5.3 Ethernet

This feature enables you to view and configure the speed and transmission mode of the ethernet interface. Navigate to **CONFIGURATION > Ethernet.** The **Ethernet Interface Properties** screen appears.



Ethernet Interface Properties

S.No.	MAC Address	Operational Speed	Operational TxMode	Speed and TxMode
1	00:20:a6:ed:fc:ba	100 Mbit	Full Duplex	Auto

Figure 5-8 Ethernet Interface Properties

Tabulated below are 'Ethernet Interface' parameters and the method to configure the configurable parameters:

Parameter	Description
MAC Address	Displays the MAC address of the ethernet Interface.
Operational Speed	Displays the current operational speed of the ethernet interface.
Operational TxMode	Displays the current operational mode of transmission over the ethernet interface. There are two types of transmission modes: – **Half Duplex**: Allows one-way transmission at a time; where only receive or transmit operation can be performed at once. – **Full Duplex**: Allows two-way transmission, where both receive and transmit operations can be performed simultaneously.
Speed and TxMode	Specifies the speed and transmission mode of the ethernet interface. By default, the AP device is in **Auto** mode, which means that the AP device negotiates with its switch or hub to automatically select the highest throughput option supported by both the ends of a wireless link. To configure, select the **Speed and TxMode** from the drop down menu. 📝: • *'**Speed and TxMode**' is configurable only for AP-8100.* • *Ensure that the same '**Speed and TxMode**' is configured at both the ends of a wired link.*

Click **OK** and **COMMIT**, to save the configured parameters.

5.4 Wireless Interface

The **Wireless** feature enables you to use **Multiple Input Multiple Output (MIMO)** technology, that uses several antennas to transfer multiple data streams thus enabling more data to be transferred in the same period of time. The wireless architecture is based on the cellular architecture where the systems are divided into cells, and each cell is called a **Basic Service Set (BSS)**. Each BSS is controlled by a base station called **Access Point**, which manages the associated wireless clients. BSS is identified by a Basic Service Set Identifier (BSSID), which corresponds to the Access Point's MAC address.

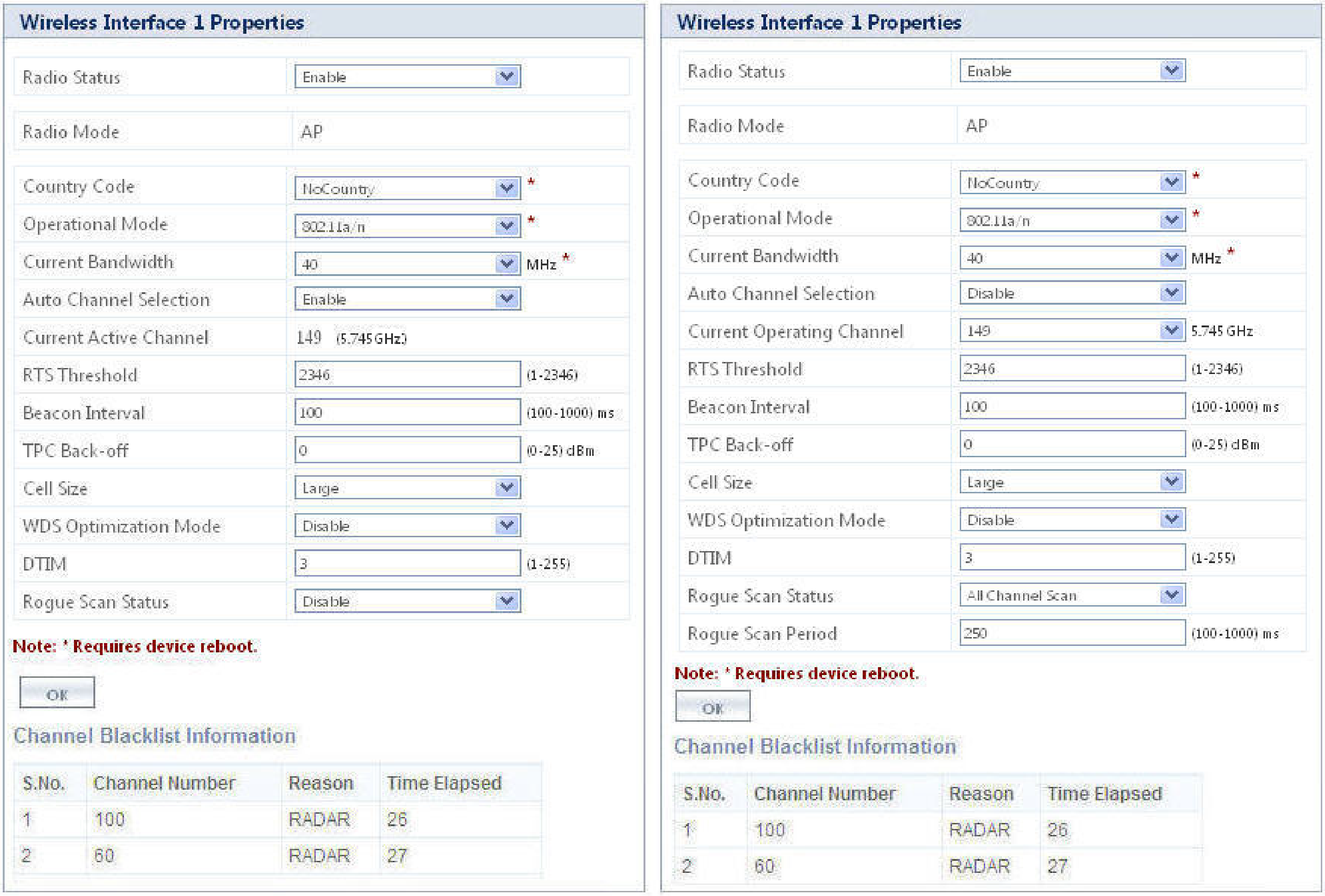
The Wireless LAN (WLAN) can be formed of a single cell or of many cells. Each of the WLAN has an entry point which is called **Virtual Access Point (VAP)**. A VAP is a logical entity that exists within a physical WLAN access device. Each VAP is assigned a unique BSSID and other relevant protocols that make these VAPs an independent entity. Each of the VAP can be configured independently so that the user can provide unique authentication and security features. (Refer Virtual Access Point (VAP))

5.4.1 Interface 1

The 'Interface (Radio)' of the AP device enables wireless Coverage. By default, Interface (Radio) 1 is enabled in AP mode (See AP Mode).

5.4.1.1 Properties

Navigate to **CONFIGURATION** > **Wireless** > **Interface 1** > **Properties**. The **Wireless Interface - 1 Properties** screen appears.



Wireless Interface 1 Properties

Radio Status	Enable
Radio Mode	AP
Country Code	NoCountry *
Operational Mode	802.11a/n *
Current Bandwidth	40 MHz *
Auto Channel Selection	Enable
Current Active Channel	149 (5.745 GHz)
RTS Threshold	2346 (1-2346)
Beacon Interval	100 (100-1000) ms
TPC Back-off	0 (0-25) dBm
Cell Size	Large
WDS Optimization Mode	Disable
DTIM	3 (1-255)
Rogue Scan Status	Disable

Note: * Requires device reboot.

OK

Channel Blacklist Information

S.No.	Channel Number	Reason	Time Elapsed
1	100	RADAR	26
2	60	RADAR	27

Wireless Interface 1 Properties

Radio Status	Enable
Radio Mode	AP
Country Code	NoCountry *
Operational Mode	802.11a/n *
Current Bandwidth	40 MHz *
Auto Channel Selection	Disable
Current Operating Channel	149 5.745 GHz
RTS Threshold	2346 (1-2346)
Beacon Interval	100 (100-1000) ms
TPC Back-off	0 (0-25) dBm
Cell Size	Large
WDS Optimization Mode	Disable
DTIM	3 (1-255)
Rogue Scan Status	All Channel Scan
Rogue Scan Period	250 (100-1000) ms

Note: * Requires device reboot.

OK

Channel Blacklist Information

S.No.	Channel Number	Reason	Time Elapsed
1	100	RADAR	26
2	60	RADAR	27

Figure 5-9 Wireless Interface 1 Properties

Tabulated below are ‘Wireless Interface’ parameters and the method to configure the configurable parameters:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Radio Status</td><td>Specifies the status of the Interface (Radio).
By default, it is enabled. To disable, select <b>Disable</b> from the drop down menu. If the radio status is disabled, the interface gets shutdown.</td></tr>
<tr><td>Radio Mode</td><td>This parameter enables you to set the radio mode of the AP device. The available radio mode is AP.</td></tr>
<tr><td>Country Code</td><td>Specifies the country where the AP device is used.
<ul>
<li><b>US Regulatory Domain</b>: The <b>US</b> country is by default selected, and is not configurable.</li>
<li><b>Japan Regulatory Domain</b>: The <b>JP</b> country is by default selected, and is not configurable.</li>
<li><b>World Regulatory Domain</b>: By default, <b>NoCountry</b> is selected. Select the country, where the device would operate, from the available list of countries. Setting the <b>Country Code</b>, makes the AP Device automatically compliant with the rules of the regulatory domain in which it is used.</li>
<li><b>Europe Regulatory Domain</b>: By default, <b>UnitedKingdom</b> is selected. If operating in a country other than United Kingdom, select the country from the available list of countries. Setting the <b>Country Code</b>, makes the AP Device automatically compliant with the rules of the regulatory domain in which it is used.</li>
</ul></td></tr>
<tr><td>Operational Mode</td><td>Specifies the mode of communication between the AP device and the wireless client(s). Tabulated below are the default and configurable operational modes for interface (radio) 1 of AP device.
<table>
<tr><th rowspan="2">Device Type</th><th colspan="2">Interface (radio) 1</th></tr>
<tr><th>Default Operational Mode</th><th>Configurable Operational Modes</th></tr>
<tr><td><b>AP-800</b></td><td>802.11a/n</td><td>802.11a, 802.11a/n, 802.11g or 802.11g/n</td></tr>
<tr><td><b>AP-8000</b></td><td>802.11a/n</td><td>802.11a, 802.11a/n, 802.11g or 802.11g/n</td></tr>
<tr><td><b>AP-8100</b></td><td>802.11a/n</td><td>802.11a or 802.11a/n</td></tr>
</table>
📝 :
<ul>
<li><i>Operational mode configuration varies based on the Current Bandwidth set.</i></li>
<li><i>The Interface (Radio) 1 of AP-8000-JP (Japan SKU) and AP-8100 can be configured only in 5 GHz frequency band (802.11a or 802.11a/n modes).</i></li>
<li><i>Configuring the Current Bandwidth to 20 MHz sets back the operational mode to factory default value. Hence, ensure that you re-configure the operational mode and <b>COMMIT</b> the changes.</i></li>
</ul></td></tr>
</table>

Current Bandwidth	Specifies the frequency band used to transmit the wireless data. The available bandwidths are 20 MHz and 40 MHz. By default, **Current Bandwidth** is set to 40MHz. To configure, select a value from the drop down menu. ✎: *Set the current bandwidth to 20 MHz, to enable the legacy operational modes of 802.11a or 802.11g.* ❗: • **When AP device operates with a channel bandwidth of 40 MHz (i.e. Dynamic 20/40 Mode) and finds the extension channel is busy, then AP will dynamically use 20 MHz bandwidth. This avoids unnecessary retries at a higher rate. Once, the extension channel is available, the device will switch back to the 40 MHz channel bandwidth.** • **If a VAP is enabled in WDS mode, see** WDS Optimization Mode **for details.**
Auto Channel Selection	This parameter enables the AP device to determine the best channel for wireless data transmission with less interference. By default, **Auto Channel Selection** is disabled. To enable, select **Enable** from the drop down menu. When enabled, the AP device scans all the available channels and selects the best channel to establish a connection. ✎: *When the AP device detects RADAR on the current operating channel, the **Auto Channel Selection** gets enabled automatically though it is disabled.*
Current Active Channel	This parameter is applicable only when the **Auto Channel Selection** is enabled and it displays the current active channel on the wireless interface.
Current Operating Channel	This parameter is applicable only when the **Auto Channel Selection** is disabled and the **Radio Mode** is set to AP. This parameter enables the user to select the current operating channel for the wireless interface. For more details on the available frequency domains and channels, refer to Frequency Domains and Channels. To configure, select the **Current Operating Channel** from the drop down menu. ✎: *When you select the current operating channel, its corresponding frequency is displayed on the right-side of the drop down menu.*
RTS Threshold	Specifies the RTS (Request-to-Send) threshold value. If the size of the MPDU is of the specified threshold value or greater than that, the AP device then uses the RTS mechanism for data transmission. By default, it is 2346. To configure, enter a value ranging from 1 to 2346 in the **RTS Threshold** box.
Beacon Interval	Specifies the interval between two successive beacons. By default, it is 100ms. To configure, enter a value ranging from 100 to 1000ms in the **Beacon Interval** box.

<table>
<tr>
<td>TPC (Transmit Power Control) Back-off</td>
<td>
<p>The AP device transmits maximum output power, as per the selected frequency and country (regulatory domain). With <b>TPC Back-off</b>, you can adjust the output power of the AP device to a lower level, in order to reduce the interference with the neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your regulatory domain.</p>
<p>By default, it is set to 0 dBm. To configure, enter a value ranging from 0 to 25 dBm in the <b>TPC Back-off</b> box.</p>
<p>: <i>TPC Back-off range (0-25 dBm) varies for different cell sizes (Large, Medium, Small, Micro and Mini).</i></p>
</td>
</tr>
<tr>
<td>Cell Size</td>
<td>
<p>Specifies the parameter that enables you to control the coverage area of the AP device in different types of deployment scenarios. For instance, usage of small cell size in dense device deployment, minimizes the interference caused by one device on another.</p>
<p>Cell sizes supported by the AP device are Large, Medium, Small, Micro and Mini. By default, it is <b>Large</b>. To configure, select the <b>Cell Size</b> from the drop down menu.</p>
<table>
<tr><th colspan="2">Cell Size Functionality</th></tr>
<tr><td colspan="2">It is classified for different VAP types (See Virtual Access Point (VAP), for details), defining the relation between transmit power, receive sensitivity and CCA threshold associated with different Cell Sizes.</td></tr>
<tr><th>Type</th><th>Description</th></tr>
<tr>
<td>AP Cell Size Functionality</td>
<td>
<p>When the cell size is set to Large, the transmit power and receive sensitivity are high. When the Cell Size is set from Large to Micro, Mini, Small or Medium, the transmit power is reduced.</p>
<p>Data tabulated below explains the <i>AP Cell Size Functionality</i> for different Cell Sizes.</p>
<table>
<tr><th>Cell Size</th><th>Maximum Tx Power* (dBm)</th><th>Receive Sensitivity Threshold (dBm)</th><th>Clear Channel Assessment Threshold (dBm)</th></tr>
<tr><td>Large</td><td>Maximum TxPower</td><td>-96</td><td>-62</td></tr>
<tr><td>Medium</td><td>Maximum TxPower-3</td><td>-86</td><td>-62</td></tr>
<tr><td>Small</td><td>Maximum TxPower-6</td><td>-78</td><td>-52</td></tr>
<tr><td>Micro</td><td>Maximum TxPower-9</td><td>-70</td><td>-42</td></tr>
<tr><td>Mini</td><td>Maximum TxPower-12</td><td>-62</td><td>-36</td></tr>
</table>
<p><i>* Maximum transmit power depends on the selected frequency domain and type of radio card.</i></p>
</td>
</tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>Cell Size</td>
<td>
<table>
<tr>
<td>WDS Cell Size Functionality</td>
<td>
In case of a WDS link (See WDS (Wireless Distribution System) Mode), when the cell size is set from Large to Micro, Mini, Small or Medium, the transmit power is retained to the maximum value.

Data tabulated below are the details that explain the *WDS Cell Size Functionality* for different Cell Sizes.
<table>
<tr><th>Cell Size</th><th>Maximum Tx Power* (dBm)</th><th>Receive Sensitivity Threshold (dBm)</th><th>Clear Channel Assessment Threshold (dBm)</th></tr>
<tr><td>Large</td><td>Maximum TxPower</td><td>-96</td><td>-62</td></tr>
<tr><td>Medium</td><td>Maximum TxPower</td><td>-86</td><td>-62</td></tr>
<tr><td>Small</td><td>Maximum TxPower</td><td>-78</td><td>-52</td></tr>
<tr><td>Micro</td><td>Maximum TxPower</td><td>-70</td><td>-42</td></tr>
<tr><td>Mini</td><td>Maximum TxPower</td><td>-62</td><td>-36</td></tr>
</table>
** Maximum transmit power depends on the selected frequency domain and type of radio card.*
</td>
</tr>
</table>
:
• *To balance transmit Power and receive sensitivity at both the ends (END-A and END-B) of a WDS link,* WDS Optimization Mode *should be enabled.*
• *If the user wants to have **AP cell size functionality** applied, irrespective of the VAP type, then the TPC value can be increased by using the **TPCBackoff** parameter.*
</td>
</tr>
<tr>
<td>WDS Optimization Mode</td>
<td>
Specifies the optimization mode (See WDS (Wireless Distribution System) Mode), that enables the user to balance the transmit power at both the ends (END-A and END-B) of a WDS link. To configure, select **Enable** or **Disable** from the drop down menu.

:
• *If WDS optimization mode is enabled, **WDS Cell Size Functionality** is applied. (See* WDS Cell Size Functionality*)*
• *If WDS optimization mode is disabled, **AP Cell Size Functionality** is applied. (See* AP Cell Size Functionality*)*
• *When WDS Optimization Mode is enabled, WDS Cell Size Functionality is applied even on the VAP enabled in AP mode.*
</td>
</tr>
</table>

WDS Optimization Mode	❗: **When WDS optimization mode is enabled with configured channel bandwidth of 40 MHz (i.e Dynamic 20/40 Mode), AP will not dynamically switch to 20 MHz bandwidth, when it finds extension channel is busy.**
DTIM (Delivery Traffic Indication Map)	Specifies the number of beacon frames that can be transmitted before another DTIM is transmitted. An increase in the DTIM period count, allows clients to sleep longer. However, it delays the delivery of multicast and unicast packets. By default, it is 3. To configure, enter a value ranging from 1 to 255 in the **DTIM** box. 📝: *Long DTIM intervals will allow the mobile wireless clients to sleep for longer hours thus maximizing the battery life. With short DTIM intervals, frequent frame delivery takes place thus reducing the power save efficiency of the battery.*
Rogue Scan Status	Specifies the status of the **Rogue Scan** feature on the AP device. **Rogue Scan** allows you to scan and monitor all the wireless devices (AP/STA/WDS/ADHOC) and rogue AP devices, within its vicinity and provides statistics of the interference caused by those devices. Rogue Scanning is done via two modes: a. **Current Channel Scan:** In this mode, the AP device scans all the wireless devices and rogue AP devices in the current operating channel, simultaneously performing the standard AP functionality. • AP device listens to all the data packets transmitted over the current operating channel, interprets the beacons and probe responses from the neighboring devices and maintains its BSS throughput performance. • A maximum of 32 wireless devices can be scanned. Once it exceeds the limit of 32 entries, it overwrites the oldest entry. b. **All Channel Scan:** In this mode, the AP device continuously scans all the available channels (both active and passive, depending on the channel flags) within its vicinity. A maximum of 512 wireless devices can be scanned. By default, **Rogue Scan Status** is disabled. To enable select either **Current Channel Scan** or **All channel Scan** from the drop down menu. 📝: • *When **Auto Channel Selection** is enabled, **Rogue Scan Status** cannot be set to **All Channel Scan**.* • *In **All Channel Scan** mode, the AP device does not support complete AP functionality.*
Rogue Scan Period	This parameter is enabled when **Rogue Scan Status** is set to **All channel Scan**. This parameter specifies the time period for which, the AP device scans each available channel to detect every wireless device in its vicinity. By default, it is 250ms. To configure, enter the time period value between 100- 1000ms.

Click **OK** and **COMMIT**, to save the configured parameters. **REBOOT** the device, if you have changed any of the parameters marked asterisk marked against it.

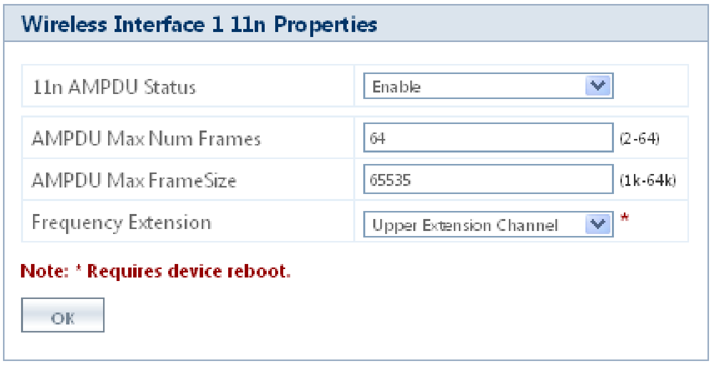
Channel Blacklist Information

A channel is blacklisted when a RADAR is detected in it. The *Channel Blacklist Information* table lists all the blacklisted channels, which includes the information tabulated below.

Parameter	Description
Channel Number	Specifies the channel number of the blacklisted channel.
Reason	Specifies the reason for blacklisting a channel.
Time Elapsed	Specifies the time period, during which a channel is not operational.

5.4.1.2 11n Properties

To configure the 11n properties of the wireless interface, navigate to **CONFIGURATION > Wireless > Interface 1 > 11n Properties**. The **Wireless Interface 1 11n Properties** screen appears.



Wireless Interface 1 11n Properties

11n AMPDU Status	Enable	
AMPDU Max Num Frames	64	(2-64)
AMPDU Max FrameSize	65535	(1k-64k)
Frequency Extension	Upper Extension Channel	*

Note: * Requires device reboot.

Figure 5-10 Wireless Interface 1 11n Properties

Tabulated below are the '11n Properties' and the method to configure the configurable parameters:

Parameter	Description
11n AMPDU (Aggregated MAC Protocol Data Unit)	This parameter enables the user to aggregate several MAC frames into a single large frame to achieve high throughput. By default, AMPDU status is enabled. To disable, select **Disable** from the drop down menu.
AMPDU Max Num Frames	Specifies the maximum number of frames that are aggregated and transmitted as a single Protocol Service Data Unit (PSDU) by the physical layer. By default, the **AMPDU Max Num Frames** is 64. To configure, enter a value ranging from 2 to 64 frames.
AMPDU Max FrameSize	Specifies the maximum AMPDU frame size (in bytes) that can be transmitted. By default, the **AMPDU Max FrameSize** is 65535 bytes. To configure, enter the frame size ranging from 1k to 64k bytes.

Frequency Extension	Specifies the frequency extension for the wireless interface. By default, *Upper Extension Channel* is taken. To configure, select frequency extension between Lower Extension Channel or Upper Extension Channel, from the drop down menu. *: Applicable only to 40 MHz bandwidth.*

Click **OK** and **COMMIT**, to save the configured parameters. **REBOOT** the device, if you have changed any of the parameters marked asterisk marked against it.

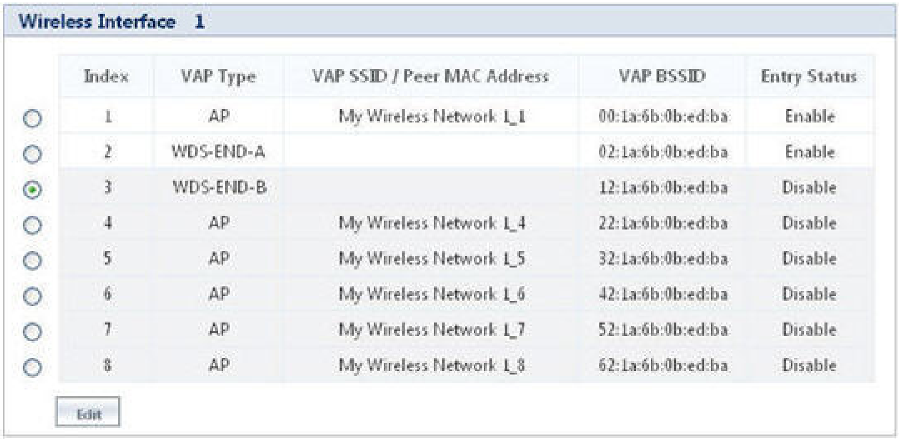
5.4.1.3 Virtual Access Point (VAP)

VAP is a logical entity that exists within the physical WLAN AP device. VAP enables single AP device to be divided into multiple VAPs, where each AP device can be configured independently, but physical properties like Channel, Operating Mode and Power will remain same for all the VAP's.

The device assigns clients to a VLAN, based on a 'Network Name (SSID)'. The AP device supports up to **eight SSIDs** per radio. This benefits the user to filter and group the data at a maximum rate.

: Multiple SSIDs can have same VLAN ID.

Navigate to **CONFIGURATION > Wireless > Interface 1> VAPs**. The **Wireless Interface - 1** screen appears.



Wireless Interface 1

	Index	VAP Type	VAP SSID / Peer MAC Address	VAP BSSID	Entry Status
○	1	AP	My Wireless Network 1_1	00:1a:6b:0b:ed:ba	Enable
○	2	WDS-END-A		02:1a:6b:0b:ed:ba	Enable
●	3	WDS-END-B		12:1a:6b:0b:ed:ba	Disable
○	4	AP	My Wireless Network 1_4	22:1a:6b:0b:ed:ba	Disable
○	5	AP	My Wireless Network 1_5	32:1a:6b:0b:ed:ba	Disable
○	6	AP	My Wireless Network 1_6	42:1a:6b:0b:ed:ba	Disable
○	7	AP	My Wireless Network 1_7	52:1a:6b:0b:ed:ba	Disable
○	8	AP	My Wireless Network 1_8	62:1a:6b:0b:ed:ba	Disable

Figure 5-11 Wireless Interface -1 VAP

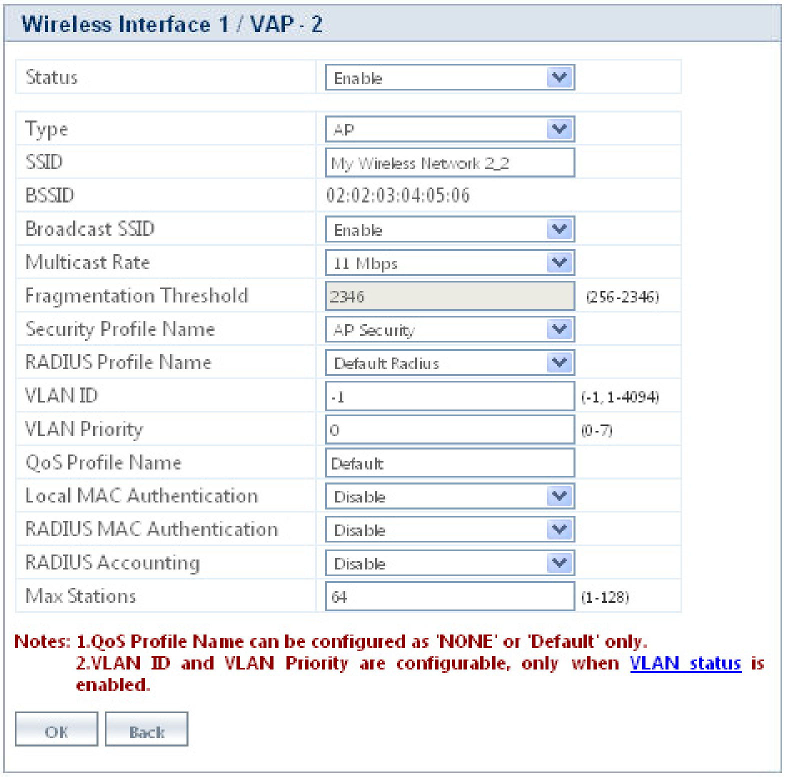
AP device supports two VAP types:

A. AP (Access Point) Mode

B. WDS (Wireless Distribution System) Mode

A. AP Mode

VAP enabled in AP mode will support the standard AP functionality. To configure a VAP in AP mode, select the radio button against the desired VAP and click **Edit** (See Wireless Interface -1 VAP). The configuration screen to edit the properties of the selected VAP appears:



Wireless Interface 1 / VAP - 2

Status	Enable	
Type	AP	
SSID	My Wireless Network 2_2	
BSSID	02:02:03:04:05:06	
Broadcast SSID	Enable	
Multicast Rate	11 Mbps	
Fragmentation Threshold	2346	(256-2346)
Security Profile Name	AP Security	
RADIUS Profile Name	Default Radius	
VLAN ID	-1	(-1, 1-4094)
VLAN Priority	0	(0-7)
QoS Profile Name	Default	
Local MAC Authentication	Disable	
RADIUS MAC Authentication	Disable	
RADIUS Accounting	Disable	
Max Stations	64	(1-128)

Notes: 1.QoS Profile Name can be configured as 'NONE' or 'Default' only.
2.VLAN ID and VLAN Priority are configurable, only when VLAN status is enabled.

Figure 5-12 Wireless Interface 1 / VAP in AP Mode - Edit Properties

Tabulated below are 'VAP-AP Mode' parameters and the method to configure the configurable parameters:

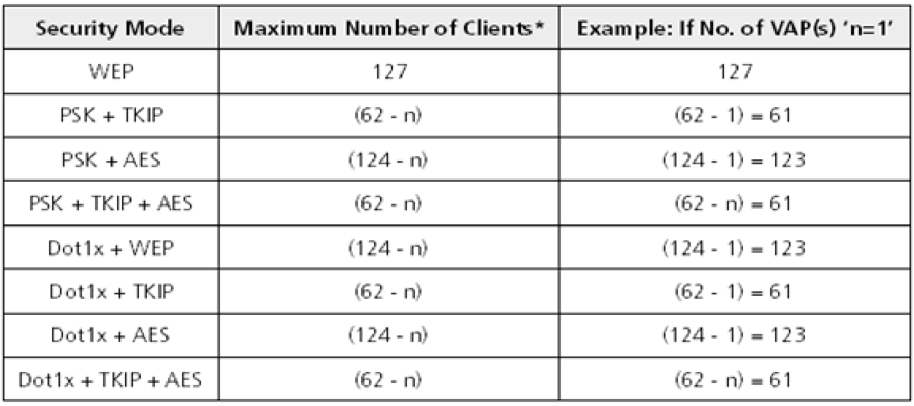
Parameter	Description
Status	Specifies the status of the VAP. By default, the first VAP is always enabled and other VAPs are disabled. To enable a VAP, select **Enable** from the drop down menu.
Type	Specifies the VAP Type. By default, the VAP Type is AP. Configurable VAP types are AP, WDS-END A, WDS-END B, WDS-Legacy. (See Wireless Distribution System (WDS) for details)
SSID	Specifies the unique network name used to identify a wireless network. To change the wireless network name, enter a new name in the **SSID** box with a maximum of 31 characters.
BSSID	Specifies a read-only parameter which displays the VAP's MAC address.
Broadcast SSID	The continuous announcement of the SSID in the beacons by VAP is called Broadcast SSID. The SSID is also broadcasted in probe response frames. For a VAP to broadcast SSID in beacons, select **Enable** from the **Broadcast SSID** box. When disabled, clients cannot detect the SSID and therefore cannot connect to the AP device.

Multicast Rate	Specifies the rate at which the multicast data packets are transmitted over the wireless network. By default, the **Multicast Rate** is 9 Mbps for operational modes 11na/a and 11 Mbps for operational modes 11ng/g. To configure, select the rate of data transmission from the drop down menu. : • *The configured multicast rate value rolls back to its default value when the operational mode of the AP device changes.* • *While configuring multicast rate, please ensure that all the clients in the network can communicate with the configured rate.*
Fragmentation Threshold	The process of dividing a MAC Service Data Unit (MSDU) into smaller MAC level frames for transmission over the wireless network is called Fragmentation.This reduces both the probability and adverse effects of wireless packet corruption, improving the overall wireless network performance. Unicast receiver address can be fragmented, whereas Broadcast/Multicast frames cannot be fragmented, even though they exceed a fragmentation threshold. If the size of the data packet is more than the configured value, AP device transmits the data by breaking it into pieces called fragments. Each fragment size is the **Fragmentation Threshold**. By default, it is 2346 bytes. To configure, enter a value ranging from 256 to 2346 bytes in the **Fragmentation Threshold** box. : *'Fragmentation Threshold' is not configurable in 11n mode.*
Security Profile Name	Specifies the name of the security profile assigned to a wireless VAP. By default, it is 'AP Security. To configure, select a **Security Profile Name** from the drop down menu. (Refer Wireless Security, for details on creating a new security profile.)
RADIUS Profile Name	Specifies the name of the RADIUS profile assigned to a wireless VAP. By default, the available *RADIUS Profile Name* is 'Default RADIUS'. (Refer RADIUS)
VLAN ID	Specifies the VLAN ID assigned to a wireless VAP. By default, the VLAN ID is set to -1, which means that VLAN tag is disabled. To enable VLAN tag, enter a value ranging from 1 to 4094 in the **VLAN ID** box.
VLAN Priority	Specifies the VLAN priority assigned to a wireless VAP. By default, it is 0. To configure, enter a value ranging from 0 to 7 in the **VLAN Priority** box. : *To configure the VLAN ID and VLAN Priority, **VLAN status** should be enabled. (See* Virtual Local Area Network (VLAN)*)*

QoS Profile Name	Specifies the name of the QoS profile assigned to a wireless VAP. You can configure the QoS Profile name as either '***Default***' or '***NONE***'. By default, it is '***Default***'. To configure, enter the **QoS Profile Name**. (See QoS Profile) 📝: • *If QoS Profile Name is **NONE**, then by default the QoS feature will be disabled.* • *By default, the QoS Profile Name taken for legacy mode is **NONE**. However, it can be manually enabled to QoS Profile Name '**Default**'.*
Local MAC Authentication	To either **Enable** or **Disable** the local MAC access control list, configure the **Local MAC Authentication** status from the drop down menu. For details, refer MAC Access Control.
RADIUS MAC Authentication	To **Enable** or **Disable** the MAC access control list for RADIUS profiles, configure the **RADIUS MAC Authentication** status from the drop down menu. 📝: • *Before configuring the **RADIUS MAC Authentication**, configure* RADIUS *Server.* • *If Local MAC Authentication is enabled, disable the RADIUS MAC Authentication.*
RADIUS Accounting	This parameter is used to either enable or disable the RADIUS Accounting Status. Click the **RADIUS Accounting** box to either enable or disable its status. 📝*:To enable RADIUS Accounting, RADIUS Accounting Server Status should be enabled.*

<table>
<tr>
<td>Max Stations</td>
<td>This parameter allows you to restrict maximum number of wireless clients that can be associated with each VAP. A maximum of 128 wireless clients can be connected per radio.
By default, it is 64 for each VAP. To configure, enter a value ranging from 1 to 128.

<i>: A VAP (connected to maximum number of clients) sends a probe response to the probe request from a new client. But, it responds to the authentication request with a proper error code, specifying the <b>Max Stations</b> limit.</i>

Tabulated below are the number of clients supported in different security modes, if ‘n’ is the number of VAPs enabled on a radio.

<table>
<tr><th>Security Mode</th><th>Maximum Number of Clients*</th><th>Example: If No. of VAP(s) ‘n=1’</th></tr>
<tr><td>WEP</td><td>127</td><td>127</td></tr>
<tr><td>PSK + TKIP</td><td>(62 - n)</td><td>(62 - 1) = 61</td></tr>
<tr><td>PSK + AES</td><td>(124 - n)</td><td>(124 - 1) = 123</td></tr>
<tr><td>PSK + TKIP + AES</td><td>(62 - n)</td><td>(62 - n) = 61</td></tr>
<tr><td>Dot1x + WEP</td><td>(124 - n)</td><td>(124 - 1) = 123</td></tr>
<tr><td>Dot1x + TKIP</td><td>(62 - n)</td><td>(62 - 1) = 61</td></tr>
<tr><td>Dot1x + AES</td><td>(124 - n)</td><td>(124 - 1) = 123</td></tr>
<tr><td>Dot1x + TKIP + AES</td><td>(62 - n)</td><td>(62 - n) = 61</td></tr>
</table>
<i>* Maximum number of clients per Radio.</i>
<i>* The maximum number of clients supported per VAP in an open authentication mode is 127.</i></td>
</tr>
</table>

Click **OK** and **COMMIT**, to save the configured parameters.

:

- *To configure VLAN on the AP device, the global VLAN status should be enabled.*
- *‘**Fragmentation Threshold**’ and ‘**Multicast Rate**’ roll back to their default values when the **Operational Mode** of the radio is changed.*
- *We recommend you to connect the AP Device to a maximum of 35 to 40 clients simultaneously, for better performance and higher throughput.*

B. Wireless Distribution System (WDS)

WDS helps you to establish a wireless link between two BSS and allows the clients of one BSS network to communicate with the clients of other BSS network. WDS helps in extending the WLAN, where it is difficult to use the wired ethernet to relay the packets between the networks.

Example: Access Point 1 of BSS1 wants to communicate with Access Point 2 of the BSS2.

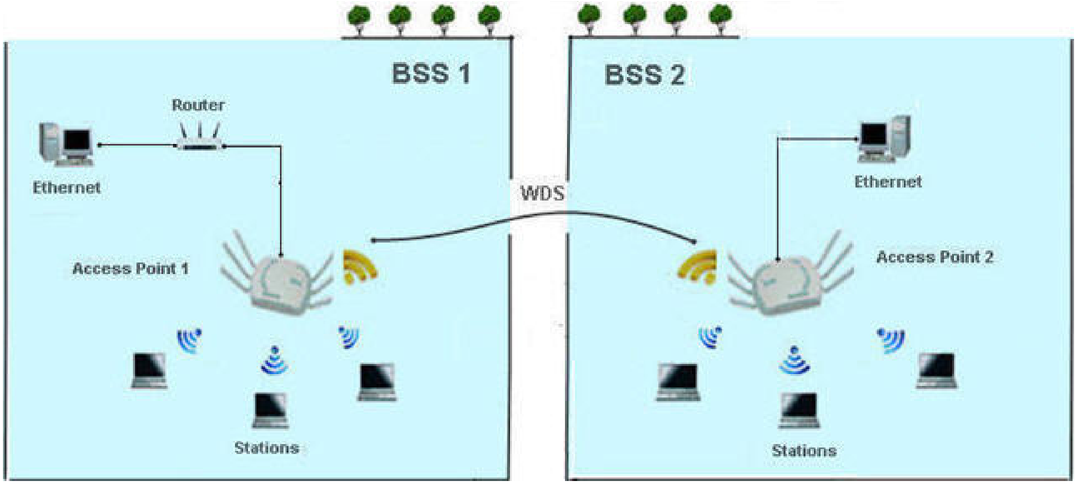


Figure 5-13 Wireless Distribution System

In such a scenario, the MAC address of Access Point 1 is configured on Access Point 2 (within the same vicinity) and vice versa. Once configured, a WDS link is established between BSS 1 and BSS 2. The data transmission over the WDS link follows a four address format, which contains 1) MAC address of the source, 2) MAC address of the destination, 3) MAC address of the transmitting AP device, 4) MAC address of the receiving AP device.

WDS supports two modes:

1. **WDS - Legacy Mode:** In this mode, a WDS link can be established between two Legacy AP devices supporting the IEEE 802.11 a/b/g modes, without serving the 11n authentication functionality while establishing the WDS link. This mode supports the WEP encryption type to secure the data.

   By using this mode, we can connect AP-800 / AP-8000 / AP-8100 with legacy products AP-700 / AP-4000. To establish a WDS link in this mode, configure both the VAPs in WDS-Legacy mode. To configure VAP in this mode, you need to configure the following parameters first:

   — **Operational Mode**: Set Operational Mode to 802 11a / 11g. Refer Properties

   — **Current Bandwidth**: Set Current Bandwidth to 20 MHz. Refer Properties

   Now, you can select the VAP Type as WDS-Legacy.

2. **WDS - 11n Mode:** In this mode, a WDS link can be established between two BSS supporting the IEEE 802.11na/ng modes, serving the association and authentication functionalities. This mode supports the AES (128 bit) encryption type to secure the data. In WDS-11n mode, each VAP can be configured as either:

   a. **WDS-END - A:** The VAP enabled in this mode will act as a WDS enabled AP device and performs standard AP functionality.

   b. **WDS-END - B:** The VAP enabled in this mode will act as a WDS enabled wireless client and perform the functions of a station/client.

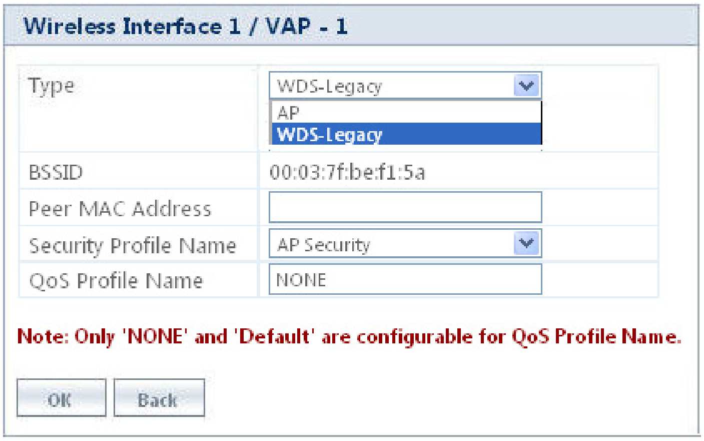
   By using this mode, we can connect only to AP-800 / AP-8000 / AP-8100. To establish a WDS link in this mode, one VAP should be set to "WDS-END-A" and other VAP should be set to "WDS-END-B". To configure VAP in this mode, you need to configure the following parameters first:

   — **Operational Mode**: Set Operational Mode to 802 11a/n or 11g/n. Refer Properties

   — **Current Bandwidth**: Set Current Bandwidth to 20 MHz or 40 MHz. Refer Properties

   Now, you can select the VAP Type as WDS-END A or WDS-END B.

Navigate to **Configuration** > **Wireless** > **Interface 1** / **Interface 2** > **VAP**, the configuration screens (WDS-legacy or WDS-11n, as selected) appear:

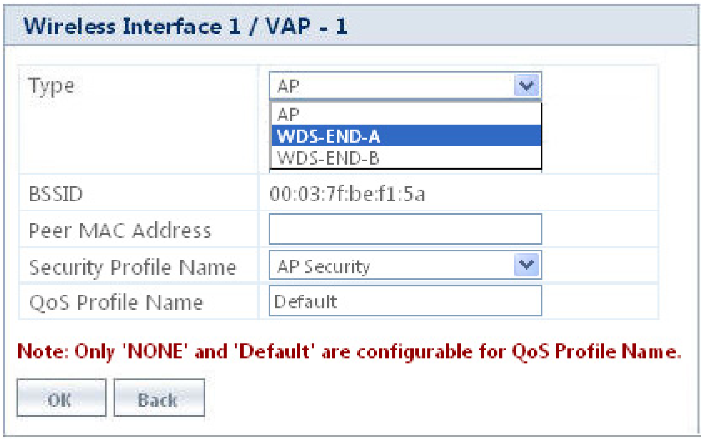


Wireless Interface 1 / VAP - 1

Type	WDS-Legacy AP WDS-Legacy
BSSID	00:03:7f:be:f1:5a
Peer MAC Address	
Security Profile Name	AP Security
QoS Profile Name	NONE

Note: Only 'NONE' and 'Default' are configurable for QoS Profile Name.

Figure 5-14 (a) VAP in WDS - Legacy Mode



Wireless Interface 1 / VAP - 1

Type	AP AP WDS-END-A WDS-END-B
BSSID	00:03:7f:be:f1:5a
Peer MAC Address	
Security Profile Name	AP Security
QoS Profile Name	Default

Note: Only 'NONE' and 'Default' are configurable for QoS Profile Name.

Figure 5-14 4 (b) VAP in WDS - 11n Mode

Tabulated below are the 'VAP-WDS Mode' parameters and the method to configure the configurable parameters:

Parameter	Description
Status	Specifies the status of the VAP. By default, it is enabled. To disable a VAP, select **Disable** from the drop down menu.
Type	Specifies the type of the VAP configured. (VAP Type may be in **AP**, **WDS-Legacy** or **WDS-END-A/END-B**). See WDS - Legacy Mode and WDS-11n Mode Select the VAP Type from the drop down menu and click **OK**. *: The AP device performs the standard AP functionality, if the VAP type is selected to AP (See* AP Mode*).*
BSSID	Specifies a read-only parameter which displays the VAP's MAC address.
Peer MAC Address	Specifies the MAC address of the destination VAP. Enter a valid MAC address in the **Peer MAC Address** box.
Security Profile Name	Specifies the security profile name assigned to a wireless VAP. By default, it is 'AP Security'. To configure, select the **Security Profile Name** from the drop down menu.
QoS Profile Name	Specifies the QoS profile name assigned to a wireless VAP. By default, the **QoS Profile Name** is set to 'Default'. (See QoS Profile). *: By default, the QoS Profile Name taken for legacy mode is **NONE**. However, it can be manually enabled to QoS Profile Name '**Default**'.*

: When WDS link is DOWN, the following behavior is expected:

- **If WDS-END-A and VAP-AP are on same radio, then the VAP-AP transmits the beacons.**
- **All the VAPs on the same interface (radio) as WDS-END-B, stop transmitting the beacons.**
- **The VAPs on an interface (radio) other than WDS-END-B, transmit the beacons.**

Click **OK** and **COMMIT**, to save the configured changes.

:

- *All the eight VAPs of an interface, can be enabled in WDS mode.*
- *WDS does not support Dynamic Frequency Selection (DFS).*
- *Same channel and security settings should be configured on the nodes present at both the ends of a WDS link.*
- *To achieve better throughput, we recommend you to enable VAP-WDS and VAP-AP on different radios. By not doing so, you may achieve only 50% of the throughput.*

5.4.2 Interface 2

The Interface (Radio) 2 on the AP device enables wireless Coverage and is applicable only to a dual-radio device. All the configuration properties for interface 2 (Radio 2) are same as interface (Radio) 1. To configure wireless interface 2 Properties, 11n Properties and Virtual Access Point (VAP) Properties, follow the same procedure explained in case of Interface 1.

Tabulated below are the default and configurable operational modes for interface (radio) 2 of AP device.

Device Type	Interface (radio) 2	
	Default Operational Mode	**Configurable Operational Modes**
AP-800	802.11g/n	802.11a, 802.11a/n, 802.11g or 802.11g/n
AP-8000	802.11g/n	802.11a, 802.11a/n, 802.11g or 802.11g/n
AP-8100	802.11g/n	802.11g or 802.11g/n

: The Interface (Radio) 2 of AP-8000-JP (Japan) SKU and AP-8100 can be configured only in 2.4 GHz frequency band (i.e in 802.11g or 802.11g/n modes).

5.5 Security

The AP device supports the following enhanced security features, that enable you to prevent unauthorized access or damage to the nodes on the wireless networks.

- **Wired Equivalent Privacy (WEP) Encryption**

  WEP provides confidentiality for network traffic by using the wireless protocol. WEP encrypts the data portion of each packet exchanged on an 802.11 network by using an Encryption Key (also known as a WEP Key). When Encryption is enabled, two 802.11 AP devices must have the same encryption Keys and both devices must be configured to use WEP Encryption, in order to communicate.

- **802.1x Authentication**

  802.1x provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. 802.1x uses an existing protocol, the Extensible Authentication Protocol (EAP, RFC 2284), that works on Ethernet, Token Ring, or wireless LANs for message exchange during the authentication process.

  In a wireless LAN with 802.1x, a user (known as the Supplicant) requests access to an access point (known as the Authenticator). The access point forces the user into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the user's identity. The client returns the identity, which is then forwarded by the access point to the authentication server (Remote Authentication Dial-In User Service (RADIUS)), which uses an algorithm to authenticate the user and then returns an accept or reject message back to the access point. Assuming an accept was received, the access point changes the client's state to authorized and normal traffic can now flow.

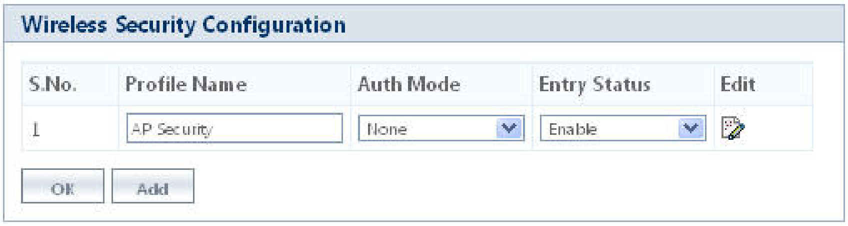
- **WPA/802.11i (WPA2) Security**

  — **WPA**: WPA is a replacement for WEP. WPA uses the Temporal Key Integrity Protocol (TKIP) for key management, and offers a choice of either the 802.1x authentication framework together with extensible authentication protocol (EAP) for enterprise WLAN security (Enterprise mode), or simpler pre-shared key (PSK) authentication for the home or small office network which does not have an authentication server (Personal mode).

  — **WPA2**: IEEE 802.11i, also known as WPA2, is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. 802.11i uses Advanced Encryption Standard (AES) block cipher.

5.5.1 Wireless Security

Navigate to **CONFIGURATION > Security > Wireless Security.** The **Wireless Security Configuration** screen appears.



Wireless Security Configuration

S.No.	Profile Name	Auth Mode	Entry Status	Edit
1	AP Security	None	Enable	

Figure 5-15 Wireless Security Configuration

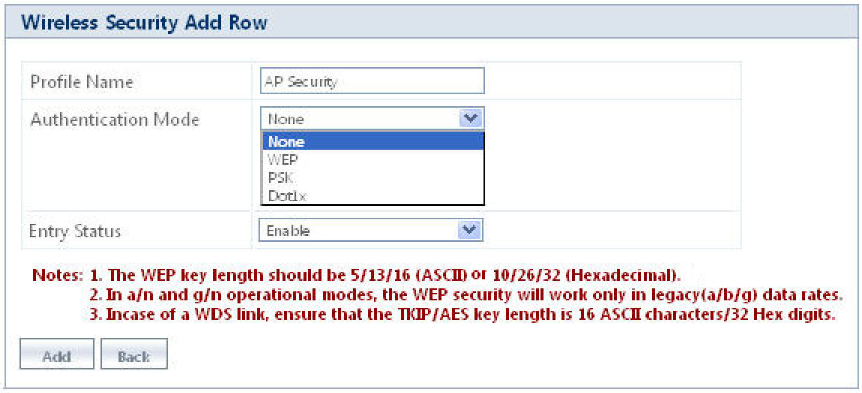
Tabulated below are the 'Wireless Security' parameters and the method to configure the configurable parameters:

Parameter	Description
Profile Name	Specifies the user-defined name for a security profile.
Auth Mode	Specifies the security mode for the wireless network. The **Auth Mode** may vary between **None**, **WEP, PSK**, **802.1x**. (See Create a New Security Profile.)
Entry Status	Specifies the status of the user-defined security profiles. The available status are: – **Enable**: Enables the user-defined Security profile. – **Disable**: Disables the user-defined Security profile. – **Delete**: Deletes the user-defined Security profile.

Click **OK** and **COMMIT**, to save the configured parameters.

5.5.1.1 Create a New Security Profile

To add a new security profile, click **Add** in the **Wireless Security Configuration** screen. The **Wireless Security Add Row** screen appears.



Wireless Security Add Row

Profile Name: AP Security

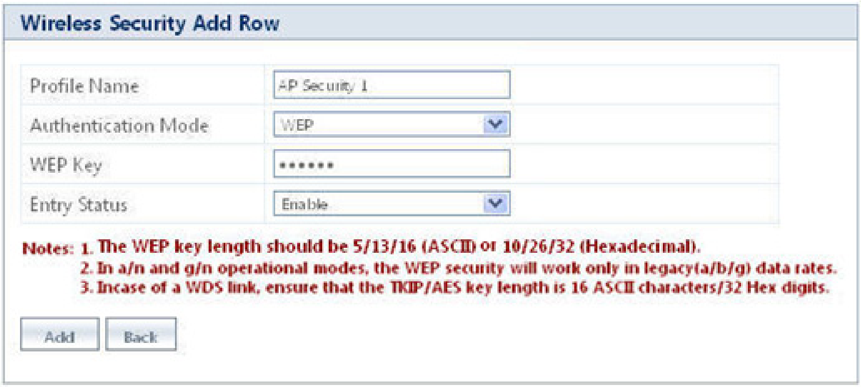
Authentication Mode: None

Entry Status: Enable

Notes: 1. The WEP key length should be 5/13/16 (ASCII) or 10/26/32 (Hexadecimal).
2. In a/n and g/n operational modes, the WEP security will work only in legacy(a/b/g) data rates.
3. Incase of a WDS link, ensure that the TKIP/AES key length is 16 ASCII characters/32 Hex digits.

Figure 5-16 Wireless Security Profile - Add Row

Tabulated below are the 'Wireless Security Profile' parameters and the method to configure the configurable parameters:

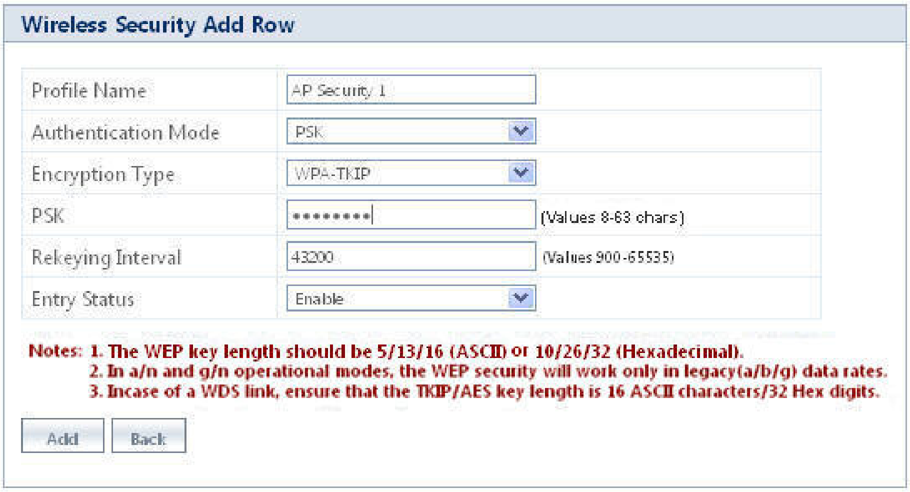
Parameter	Description
Profile Name	Specifies the name of the Security Profile created. To configure, enter a name in the **Profile Name** box.
Authentication Mode	Specifies the security mode for the wireless network. Select any of the following authentication modes for the wireless interface from the drop down menu: a. **None**: If you select this authentication mode, then no security exists on the wireless network. b. **WEP (Wired Equivalent Privacy)**: Select WEP from the authentication mode drop down menu and the configuration screen appears:  Wireless Security Add Row Profile Name: AP Security 1 Authentication Mode: WEP WEP Key: •••••• Entry Status: Enable Notes: 1. The WEP key length should be 5/13/16 (ASCII) or 10/26/32 (Hexadecimal). 2. In a/n and g/n operational modes, the WEP security will work only in legacy(a/b/g) data rates. 3. Incase of a WDS link, ensure that the TKIP/AES key length is 16 ASCII characters/32 Hex digits. **Figure 5-17 WEP Authentication Mode**

<table>
<tr>
<td>Authentication Mode</td>
<td>
Configure the following parameters in **WEP** authentication mode:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Key</td><td>This parameter allows you to configure the WEP key for the wireless security. Enter a WEP Key in the **Key** box.
– For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters. See ASCII Character Chart.
– For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.
– For 152-bit encryption, an encryption key is 32 hexadecimal characters or 16 ASCII characters.
: *Special characters* **- = \ " '? /** *space are not allowed while configuring the WEP key.*</td></tr>
</table>

: *When multiple VAPs are enabled on the AP device, then no two security profiles with WEP authentication, should be enabled at the same time.*

c. **PSK (Pre-Shared Key)**: Select PSK from the Authentication mode drop down menu and the configuration screen appears:



Wireless Security Add Row

<table>
<tr><td>Profile Name</td><td>AP Security 1</td><td></td></tr>
<tr><td>Authentication Mode</td><td>PSK</td><td></td></tr>
<tr><td>Encryption Type</td><td>WPA-TKIP</td><td></td></tr>
<tr><td>PSK</td><td>••••••••</td><td>(Values 8-63 chars)</td></tr>
<tr><td>Rekeying Interval</td><td>43200</td><td>(Values 900-65535)</td></tr>
<tr><td>Entry Status</td><td>Enable</td><td></td></tr>
</table>

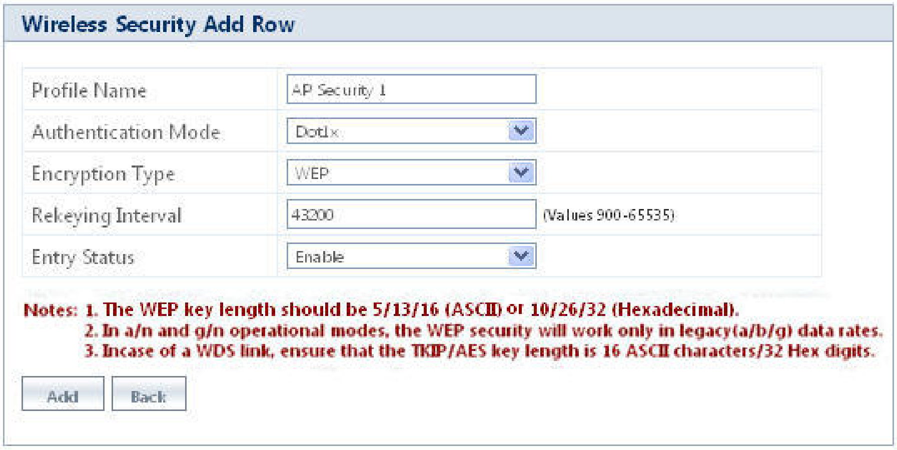
Notes: 1. The WEP key length should be 5/13/16 (ASCII) or 10/26/32 (Hexadecimal).
2. In a/n and g/n operational modes, the WEP security will work only in legacy(a/b/g) data rates.
3. Incase of a WDS link, ensure that the TKIP/AES key length is 16 ASCII characters/32 Hex digits.

Figure 5-18 PSK Authentication Mode

Configure the following parameters in **PSK Authentication Mode**:
</td>
</tr>
</table>

<table>
<tr>
<td>Authentication Mode</td>
<td>
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Encryption Type</td><td>Specifies the Encryption Type.
By default, it is taken as WPA-TKIP. To configure, select either WPA-TKIP, WPA2-AES or WPA-WPA2AES-TKIP from the drop down menu.
<i>:When the Encryption Type is set to WPA-WPA2AES-TKIP, the device supports clients with the encryption type of either WPA-TKIP or WPA2-AES.</i></td></tr>
<tr><td>PSK</td><td>Specifies the pass phrase that derives the PSK. To configure, enter a security key ranging from 8 to 63 characters in the <b>PSK</b> box.
<i>: Special characters <b>- = \ " '? /</b> space are not allowed while configuring the pass phrase.</i></td></tr>
<tr><td>Rekeying Interval</td><td>Specifies the time interval, for the device to send group keys to all its associated clients.
By default the <b>Rekeying Interval</b> value is set to 43200. To configure, enter a value ranging from 900 to 65535 seconds.</td></tr>
</table>

d. <b>802.1x</b>: Select 802.1x (Dot1x) from the Authentication mode drop down menu and the configuration screen appears:



Wireless Security Add Row

Profile Name: AP Security 1
Authentication Mode: Dot1x
Encryption Type: WEP
Rekeying Interval: 43200 (Values 900-65535)
Entry Status: Enable

Notes: 1. The WEP key length should be 5/13/16 (ASCII) or 10/26/32 (Hexadecimal).
2. In a/n and g/n operational modes, the WEP security will work only in legacy(a/b/g) data rates.
3. Incase of a WDS link, ensure that the TKIP/AES key length is 16 ASCII characters/32 Hex digits.

<b>Figure 5-19 802.1x Authentication Mode</b>

Configure the following parameters in <b>802.1x (Dot1x) Authentication Mode</b>:
</td>
</tr>
</table>

<table>
<tr>
<td>Authentication Mode</td>
<td>
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Encryption Type</td><td>Specifies the Encryption Type. By default, it is taken as WEP. To configure, enter the <b>Encryption Type</b> as either WEP, WPA-TKIP, WPA2-AES or WPA-WPA2AES-TKIP from the drop down menu.
<i>:When the Encryption Type is set to WPA-WPA2AES-TKIP, the device supports clients with the encryption type of either WPA-TKIP or WPA2-AES.</i></td></tr>
<tr><td>Rekeying Interval</td><td>Specifies the time interval, for the device to send group keys to all its associated clients.
By default, the <b>Rekeying Interval</b> value is set to 43200. To configure, enter a value ranging from 900 to 65535 seconds.</td></tr>
</table>
<i>: To configure the 802.1x authentication mode on RADIUS Server, please refer to the ‘AP11n - Reference Guide’.</i>
</td>
</tr>
<tr>
<td>Entry Status</td>
<td>Specifies the status for the security profile. By default, it is enabled. To configure, select the <b>Entry Status</b> from the drop down menu.</td>
</tr>
</table>

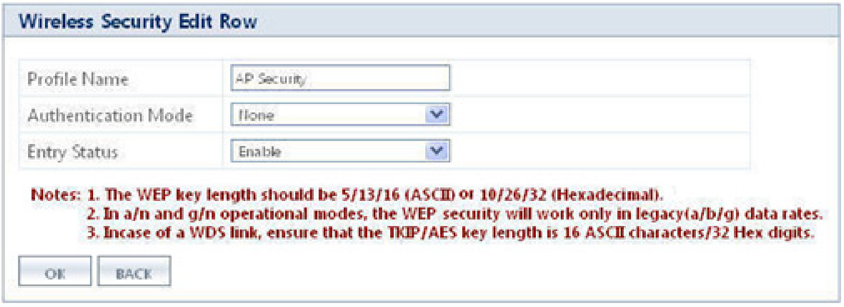
Click **Add**, to save the new profile with configured parameters.

:

- *You can add a maximum of 16 security profiles.*
- *In case of a WDS link, supported security keys and their respective key lengths are:*
  - *Key length should be (ASCII 5/13/16) (Hex 10/26/32), for WEP Encryption.*
  - *Key length should be 16 ASCII characters or 32 Hex digits, for AES or TKIP encryption.*
  - *WEP/TKIP Encryption will work only in Legacy (11 a/b/g) data rates, for 11na/11ng modes.*
- *If the PSK and WEP key passwords are not configured, then AP device uses the following default passwords:*
  - *WEP : 1234567890*
  - *PSK: 1234679890123456*
- *It is recommended not to use WEP/TKIP encryption type in 11n operational mode.*

5.5.1.2 Edit an Existing AP Security Profile

To edit an existing AP security profile, click the Edit icon in the **Wireless Security Configuration** screen. The **Wireless Security Edit Row** screen appears.



Profile Name: AP Security
Authentication Mode: None
Entry Status: Enable

Notes: 1. The WEP key length should be 5/13/16 (ASCII) or 10/26/32 (Hexadecimal).
2. In a/n and g/n operational modes, the WEP security will work only in legacy(a/b/g) data rates.
3. Incase of a WDS link, ensure that the TKIP/AES key length is 16 ASCII characters/32 Hex digits.

Figure 5-20 AP - Edit Wireless Security Profile

Configure the following parameters:

Parameter	Description
Profile Name	Specifies the name of the Security Profile that is being created. To configure, enter the desired **Profile Name**.
Authentication Mode	Specifies the security mode for the wireless network. The **Auth Mode** may vary between **None**, **WEP**, **PSK**, **802.1x**. (See Create a New Security Profile)
Entry Status	Specifies the status of the security profile selected. By default, it is enabled. To configure, select the **Entry Status** from the drop down menu.

Click **OK** and **COMMIT**, to save the configured parameters.

5.5.2 RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for nodes to connect and use a network service.

The AP device supports the following authentication and accounting mechanisms:

- **MAC Access Control Via RADIUS Authentication:** Allows only the MAC addresses that are registered on the RADIUS server to access the wireless network.
- **802.1x Authentication using RADIUS**: Refer 802.1x Authentication
- **RADIUS Accounting**: By using an external RADIUS server, the AP device can track and record the length of the client sessions by sending the RADIUS accounting messages per RFC2866. When a wireless client is successfully authenticated, RADIUS accounting is initiated by sending an "Accounting Start" request to the RADIUS server. When the wireless client session ends, an "Accounting Stop" request is sent to the RADIUS server.

: For the AP device to support the above authentication and accounting mechanisms, ensure to configure the RADIUS server. For more details on configuring a RADIUS server, please refer to 'AP11n - Reference Guide'.

5.5.2.1 Authentication Attributes

- **User-Name**: Specifies the name of the user that needs to be authenticated. It must be sent in Access-Request packets, if available.
- **User-Password**: Specifies the user password to be authenticated, or the user's input following an Access-Challenge. It is only used in Access-Request packets.

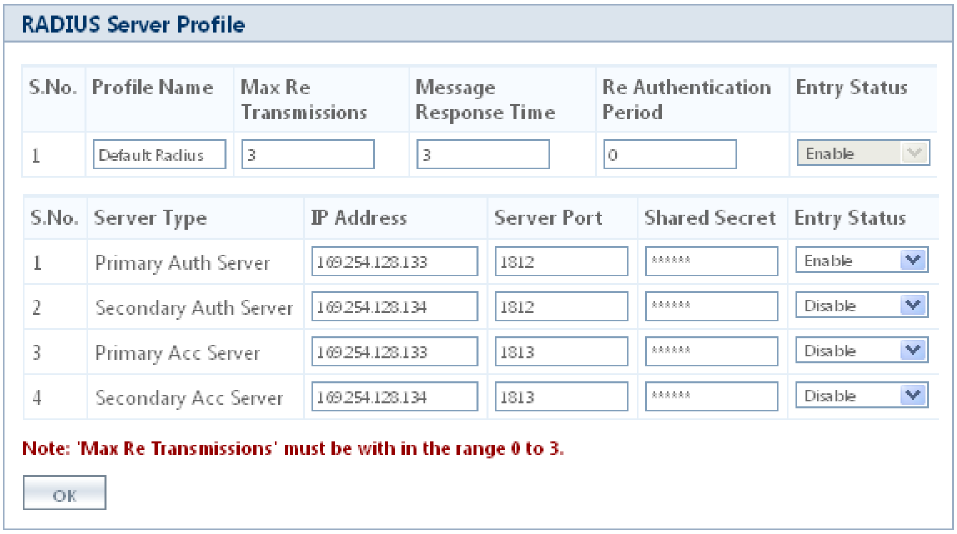
- **NAS-IP-Address**: Specifies the identifying IP Address of the NAS (AP device) which is requesting authentication of the user, and should be unique to the NAS (AP device) within the scope of the RADIUS server. NAS-IP-Address is only used in Access-Request packets.
- **State:** Specifies the attribute sent by the server to the client in an Access-Challenge and must be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any.
- **Class**: Specifies the attribute sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported.
- **Session-Time-out**: Specifies the attribute that sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. This attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge.
- **Termination-Action**: Specifies the action taken by the NAS (AP device) when the specified service is completed. It is only used in Access-Accept packets.
- **Called-Station-Id**: Specifies the MAC address of the AP device's wireless interface, with which the client gets authenticated.
- **Calling-Station-Id**: Specifies the MAC address of the wireless client being authenticated.
- **Acct-Interim-Interval**: Specifies the attribute obtained during the Authentication process and used for determining the time interval for sending Accounting-Update messages.

: If this attribute is not obtained from the RADIUS Server, the AP device uses default value (300 seconds) for updating the accounting messages.

5.5.2.2 Accounting Attributes

- **Acct-Status-Type**: Specifies whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
- **Acct-Input-Octets**: Specifies the number of octets that have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- **Acct-Output-Octets**: Specifies the number of octets that have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- **Acct-Session-Id**: Specifies a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop record for a given session will have the same Acct-Session-Id.
- **Acct-Authentic**: Specifies an attribute that is included in an Accounting-Request to indicate how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol.
- **Acct-Session-Time**: Specifies the total time in seconds, the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- **Acct-Input-Packets**: Specifies the number of packets that have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- **Acct-Output-Packets**: Specifies the number of packets that have been sent to the port in the course of delivering this service to a framed user, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- **Acct-Terminate-Cause:** Specifies the cause for which the session was terminated, and can only be present in Accounting- Request records where the Acct-Status-Type is set to Stop.

Navigate to **CONFIGURATION** > **Security** > **RADIUS**. The **RADIUS Server Profile** screen appears:



RADIUS Server Profile

S.No.	Profile Name	Max Re Transmissions	Message Response Time	Re Authentication Period	Entry Status
1	Default Radius	3	3	0	Enable

S.No.	Server Type	IP Address	Server Port	Shared Secret	Entry Status
1	Primary Auth Server	169.254.128.133	1812	******	Enable
2	Secondary Auth Server	169.254.128.134	1812	******	Disable
3	Primary Acc Server	169.254.128.133	1813	******	Disable
4	Secondary Acc Server	169.254.128.134	1813	******	Disable

Note: 'Max Re Transmissions' must be with in the range 0 to 3.

Figure 5-21 RADIUS Server Profile

Tabulated below are the 'RADIUS Server Profile' parameters and the method to configure the configurable parameters:

Parameter	Description
Profile Name	Specifies the RADIUS profile name which is used to identify a set of four RADIUS servers configured one per Accounting, Authentication, Secondary Accounting and Secondary Authentication.
Max Re Transmissions	Specifies the maximum number of times, an authentication request is retransmitted. By default, it is set to 3. To configure, enter the **Max ReTransmissions** in the range of 0 to 3.
Message Response Time	Specifies the response time, for the RADIUS server to acknowledge a request. By default, it is 3. To configure, enter the **Message Response Time** in the range of 3 to 12 seconds.
Re Authentication Period	Specifies the time period for the AP device to re-authenticate the client with the RADIUS server. By default, the **Re Authentication Period** is 0. To configure, enter the value in the range of 900 to 65535 seconds. : ***Re Authentication Period*** *is not applicable to wireless clients using 'RADIUS MAC Authentication' and is disabled if the value is set to "0".*
RADIUS Server Profile Table	
Server Type	A read-only parameter which displays the type of RADIUS Server. **Server Type** may vary between **Primary Accounting Server**, **Secondary Accounting Server**, **Primary Authentication Server** and **Secondary Authentication Server**.
IP Address	Specifies the IP address of the RADIUS server configured. To configure, enter the **IP Address** in the box.

Server Port	Specifies the number of the port, that the AP device and server use to communicate with each other. To configure, enter the **Server Port** number in the box.
Shared Secret	Specifies the password, shared by the RADIUS server and the AP device. To configure, enter a **Shared Secret** in the box, with a maximum of 64 characters. *: Special characters* **- = \ " '? /** *space are not allowed while configuring the pass phrase.*
Entry Status	Specifies the status of the RADIUS server. By default, the first RADIUS Server is enabled. To configure, select **Enable** or **Disable** from the drop down menu.

Click **OK** and **COMMIT**, to save the configured parameters.

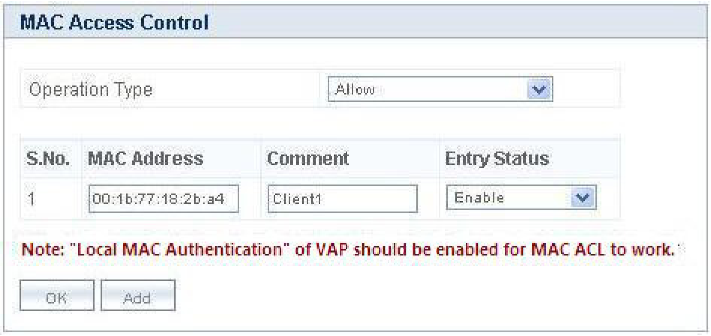
5.5.3 MAC Access Control

The MAC Access Control feature on AP device allows only the authorized wireless clients to access the network. MAC Authentication is supported only on the wireless interface. AP device supports two types of MAC authentication:

1. **RADIUS MAC Authentication:** Allows only the MAC addresses that are registered on the RADIUS server to access the wireless network. To configure **RADIUS MAC Authentication** on AP device, refer RADIUS MAC Authentication.

   : For information on RADIUS server configuration, please refer to the 'AP11n - Reference Guide'.

2. **Local MAC Authentication:** Allows only the MAC addresses that are registered on the AP device to access the wireless network. To configure, navigate to **CONFIGURATION** > **Security** > **MAC ACL**. The **MAC Access Control** screen appears.



MAC Access Control

Operation Type: Allow

S.No.	MAC Address	Comment	Entry Status
1	00:1b:77:18:2b:a4	Client1	Enable

Note: "Local MAC Authentication" of VAP should be enabled for MAC ACL to work.

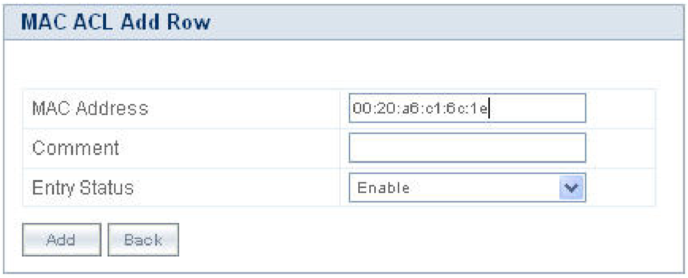
Figure 5-22 MAC Access Control

- Configure the '**Operation Type**' as **Allow** or **Deny**. While,
  - — **Allow:** AP device allows only the wireless clients in the MAC Access Control Table to access the wireless network.
  - — **Deny**: AP device does not allow the wireless clients in the MAC Access Control Table to access the wireless network.
- By default, it is **Deny.** To configure, select the **Operation Type** from the drop down menu.
- Click **OK** and **COMMIT**, to save the configuration.

: To enable MAC Access Control, you should enable Local MAC Authentication in VAP. Refer Local MAC Authentication.

5.5.3.1 Add Wireless Clients to MAC Access Control Table

To add a MAC address of a wireless client in the MAC Access Control Table, click **Add** in the **MAC Access Control** screen. The **MAC ACL Add Row** screen appears.



MAC ACL Add Row

MAC Address: 00:20:a6:c1:6c:1e

Comment:

Entry Status: Enable

Figure 5-23 MAC ACL Add Row

Configure the following parameters:

Parameter	Description
MAC Address	Specifies the MAC address of a wireless client. To configure, enter the **MAC address**.
Comment	Enter any comment in the **Comment** box.
Entry Status	Specifies the entry status of the wireless client. By default, the **Entry Status** of a wireless client is enabled. To configure, select **Enable** or **Disable** from the drop down menu.

Click **Add**, to add the new wireless client.

:

- *A maximum of 1024 MAC addresses can be added.*
- *Local MAC-ACL authentication and RADIUS MAC authentication cannot be enabled at the same time, for a single VAP.*

5.6 Quality of Service (QoS)

The AP device supports Wireless Multimedia Extensions (WME), which is a solution for QoS functionality based on the IEEE 802.11e specification. WME defines enhancements to the Media Access Control (MAC) for wireless LAN applications with Quality of Service requirements, which include transport of voice and video traffic over IEEE 802.11 wireless LANs.

The enhancements are in the form of changes in protocol frame formats (addition of new fields and information elements) addition of new messages, definition of new protocol actions, channel access mechanisms (differentiated control of access to medium), network elements (QoS/WME aware AP devices, wireless clients), and configuration management.

WME supports Enhanced Distributed Channel Access (EDCA) for prioritized QoS services. The QoS feature can be enabled or disabled per VAP.

The various QoS features supported by the AP device are described in the following sections:

- Enhanced Distributed Channel Access (EDCA)
- 802.1d to IP DSCP
- 802.1d to 802.1p

- QoS Profile
- QoS Policy

5.6.1 Enhanced Distributed Channel Access (EDCA)

EDCA is a prioritized 'Carrier Sense Multiple Access with Collision Avoidance (CSMA)/CA' access mechanism used by the clients/AP device in a WME enabled BSS to realize different classes of differentiated channel access.

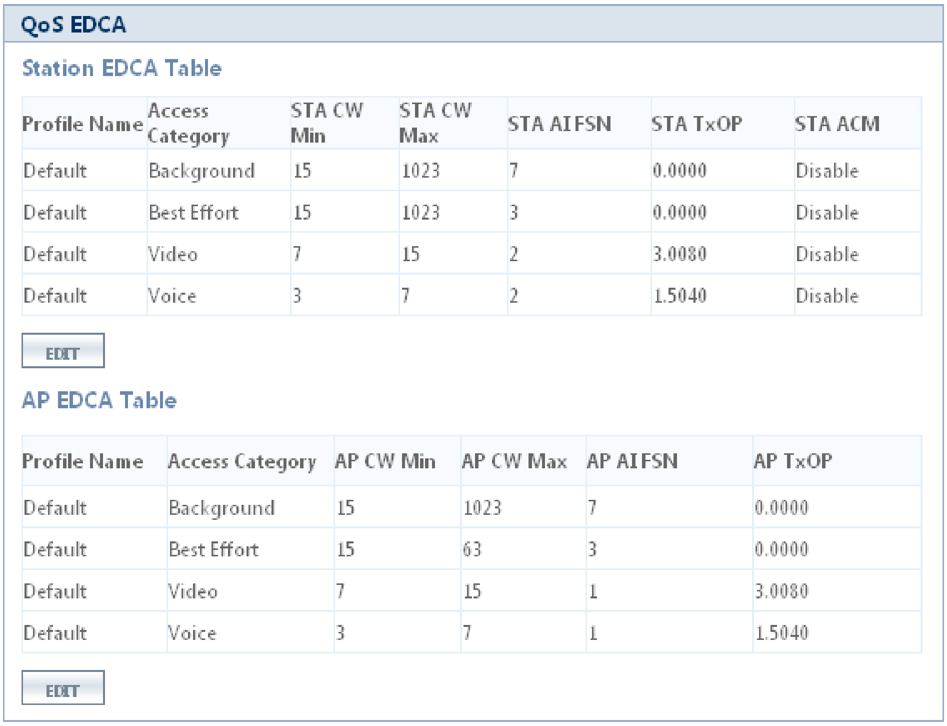
A wireless entity is defined as, all wireless clients and devices in the wireless medium contending for the common wireless medium. EDCA uses a separate channel access function for each of the access categories (Index), within a wireless entity. Each channel access function in a wireless entity contends for the wireless medium as if it were a separate client contending. Different channel access functions in a given wireless entity contend among themselves for access to the wireless medium in addition to contending with other clients.

Station EDCA Table and AP EDCA Table

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

: Proxim recommends you not to modify the default values of EDCA parameters defined in the web interface, unless strictly necessary.

Navigate to **CONFIGURATION > QoS > EDCA**. The **QoS EDCA** screen appears.



QoS EDCA

Station EDCA Table

Profile Name	Access Category	STA CW Min	STA CW Max	STA AIFSN	STA TxOP	STA ACM
Default	Background	15	1023	7	0.0000	Disable
Default	Best Effort	15	1023	3	0.0000	Disable
Default	Video	7	15	2	3.0080	Disable
Default	Voice	3	7	2	1.5040	Disable

AP EDCA Table

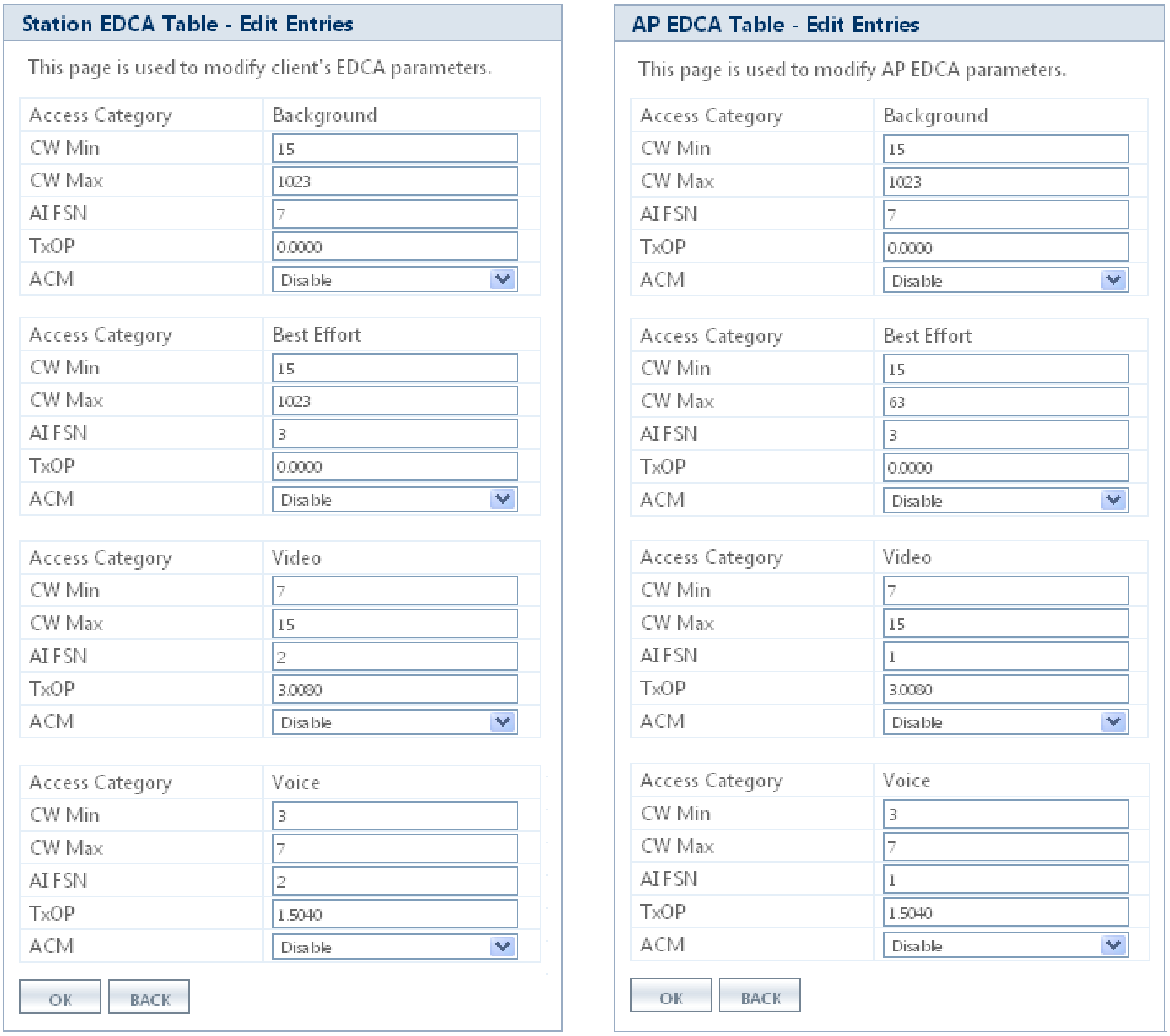
Profile Name	Access Category	AP CW Min	AP CW Max	AP AIFSN	AP TxOP
Default	Background	15	1023	7	0.0000
Default	Best Effort	15	63	3	0.0000
Default	Video	7	15	1	3.0080
Default	Voice	3	7	1	1.5040

Figure 5-24 QoS EDCA

The QoS EDCA screen is categorized under two headings, namely, **Station EDCA Table** and **AP EDCA Table**. The **Station EDCA** Table allows you to configure the EDCA parameters for the wireless client, and the **AP EDCA** Table allows you to configure the EDCA parameters for the AP device.

To modify the EDCA parameters of the wireless client (Station) or AP device, click **Edit** under the respective categories. The **Station EDCA Table - Edit Entries/AP EDCA Table - Edit Entries** screen appears.

*: The default EDCA Profile name is '**Default**' and it cannot be configured.*



Station EDCA Table - Edit Entries

This page is used to modify client's EDCA parameters.

Access Category	Background
CW Min	15
CW Max	1023
AIFSN	7
TxOP	0.0000
ACM	Disable

Access Category	Best Effort
CW Min	15
CW Max	1023
AIFSN	3
TxOP	0.0000
ACM	Disable

Access Category	Video
CW Min	7
CW Max	15
AIFSN	2
TxOP	3.0080
ACM	Disable

Access Category	Voice
CW Min	3
CW Max	7
AIFSN	2
TxOP	1.5040
ACM	Disable

AP EDCA Table - Edit Entries

This page is used to modify AP EDCA parameters.

Access Category	Background
CW Min	15
CW Max	1023
AIFSN	7
TxOP	0.0000
ACM	Disable

Access Category	Best Effort
CW Min	15
CW Max	63
AIFSN	3
TxOP	0.0000
ACM	Disable

Access Category	Video
CW Min	7
CW Max	15
AIFSN	1
TxOP	3.0080
ACM	Disable

Access Category	Voice
CW Min	3
CW Max	7
AIFSN	1
TxOP	1.5040
ACM	Disable

Figure 5-25 Station EDCA Table (left) /AP EDCA Table (right) - Edit Entries

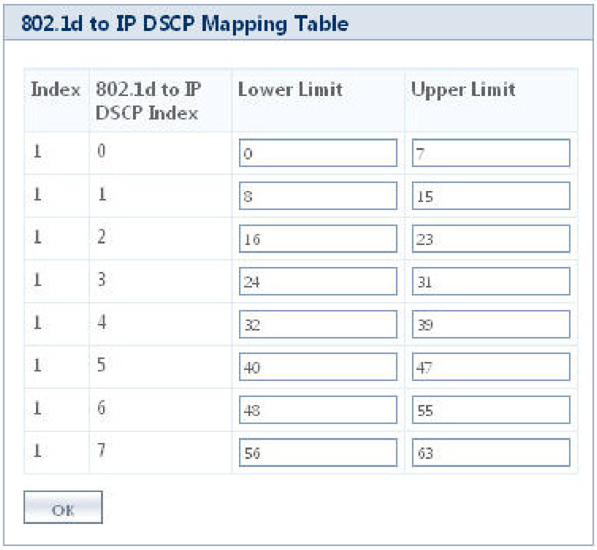
Tabulated below are the ‘QoS EDCA’ parameters and the method to configure the configurable parameters:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Access Category</td><td>Specifies a label for the common set of EDCA parameters that are used by a QoS Station/AP to contend for the channel in order to transmit MSDUs with certain priorities.Available access categories are:
– Background
– Best Effort
– Video
– Voice</td></tr>
<tr><td></td><td>Tabulated below are the default EDCA parameters for the wireless client (Station) and AP device, specific to each access category.
<table>
<tr><th rowspan="2">Access Category</th><th colspan="4">Default EDCA Parameters for Station</th><th colspan="4">Default EDCA Parameters for AP</th></tr>
<tr><th>CW Min</th><th>CW Max</th><th>AIFS</th><th>Tx OP (Unsigned Integer)</th><th>CW Min</th><th>CW Max</th><th>AIFS</th><th>Tx OP (Unsigned Integer)</th></tr>
<tr><td>Background</td><td>15</td><td>1023</td><td>7</td><td>0</td><td>15</td><td>1023</td><td>7</td><td>0</td></tr>
<tr><td>Best Effort</td><td>15</td><td>1023</td><td>3</td><td>0</td><td>15</td><td>63</td><td>3</td><td>0</td></tr>
<tr><td>Video</td><td>7</td><td>15</td><td>2</td><td>3.008 ms</td><td>7</td><td>15</td><td>1</td><td>3.008 ms</td></tr>
<tr><td>Voice</td><td>3</td><td>7</td><td>2</td><td>1.504 ms</td><td>3</td><td>7</td><td>1</td><td>1.504 ms</td></tr>
</table>
‘<b>Access Category</b>’ is a read-only parameter and cannot be configured.</td></tr>
<tr><td>CW Min</td><td>Specifies the minimum value for Contention Window (CW) for the wireless QoS EDCA profile. To configure, enter the <b>CW Min</b> in the range of 0 to 32767, for both wireless client and AP device.</td></tr>
<tr><td>CW Max</td><td>Specifies the maximum value for Contention Window (CW) for the wireless QoS EDCA profile. To configure, enter the <b>CW Max</b> in the range of 0 to 32767, for both wireless client and AP device.</td></tr>
<tr><td>AI FSN</td><td>Specifies the Arbitration Inter-Frame Space Number (AI FSN) per access category. To configure, enter the <b>AI FSN</b> in the range of 2 to 15 for Station and 1 to 15 for AP.</td></tr>
<tr><td>TxOP</td><td>The Transmission Opportunity Limit (TxOP) is a time interval for the QoS enhanced client to initiate a frame exchange on the wireless medium. The TxOP Limit defines the upper limit based on the TxOP value a wireless entity can obtain for a particular access category.
To configure, enter the <b>TxOP</b> in the range of 0 to 8160, for both Station and AP device.</td></tr>
<tr><td>ACM</td><td>The Admission Control Mandatory (ACM) defines, if an AP device accepts or rejects a request traffic stream with certain QoS specifications, based on available channel capacity and link conditions.
To configure ACM for each access category, select either <b>Enable</b> or <b>Disable</b> from the drop down menu</td></tr>
</table>

Click **OK** and **COMMIT**, to save the configured parameters.

5.6.2 802.1d to IP DSCP

Navigate to **CONFIGURATION > QoS > 802.1d to IP DSCP.** The **802.1d to IP DSCP Mapping Table** screen appears.



802.1d to IP DSCP Mapping Table

Index	802.1d to IP DSCP Index	Lower Limit	Upper Limit
1	0	0	7
1	1	8	15
1	2	16	23
1	3	24	31
1	4	32	39
1	5	40	47
1	6	48	55
1	7	56	63

Figure 5-26 802.1d To IP DSCP Mapping Table

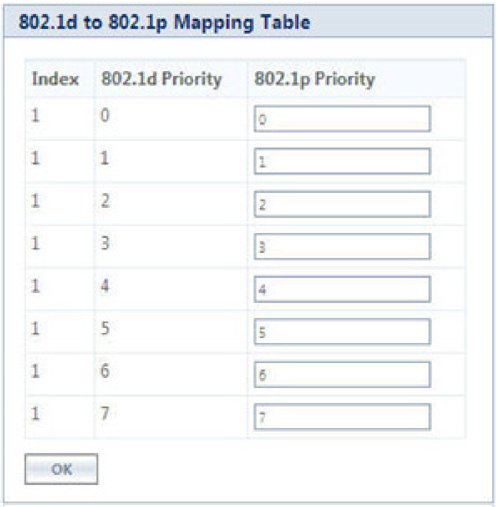
Tabulated below are the 'QoS 802.1d and IP DSCP (Differentiated Services Code Point) (for layer 3 policies)' parameters and the method to configure the configurable parameters:

Parameter	Description
802.1d to IP DSCP Index	Indicates the IP DSCP index corresponding to 802.1d priority. This parameter is a read-only and cannot be configured.
Lower Limit and Upper Limit	Specifies the IP DSCP range (lower and Upper limit) for each 802.1d priority. To configure, enter the **Lower Limit** and **Upper Limit** in the range of 0 to 63, respectively for each 802.1d priority.

Click **OK** and **COMMIT**, to save the configured parameters.

5.6.3 802.1d to 802.1p

Navigate to **CONFIGURATION > QoS > 802.1d to 802.1p**. The **802.1d to 802.1p Mapping Table** screen appears.



802.1d to 802.1p Mapping Table

Index	802.1d Priority	802.1p Priority
1	0	0
1	1	1
1	2	2
1	3	3
1	4	4
1	5	5
1	6	6
1	7	7

Figure 5-27 802.1d to 802.1p Mapping Table

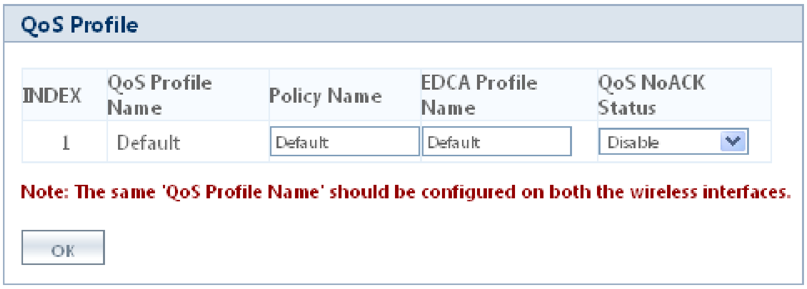
Tabulated below are the 'QoS 802.1d and 802.1p (for layer 2 policies) parameters and the method to configure the configurable parameters:

Parameter	Description
802.1d Priority	Represents the 802.1d priority. It is a read-only parameter and cannot be configured.
802.1p Priority	Specifies the 802.1p priority mapped to the corresponding 802.1d priority. To configure, enter the **802.1p Priority**, for the corresponding 802.1d priority, in the range of 0 to 7.

Click **OK** and **COMMIT**, to save the configured parameters.

5.6.4 QoS Profile

Navigate to **CONFIGURATION > QoS > QoS Profile.** The **QoS Profile** screen appears.



QoS Profile

INDEX	QoS Profile Name	Policy Name	EDCA Profile Name	QoS NoACK Status
1	Default	Default	Default	Disable

Note: The same 'QoS Profile Name' should be configured on both the wireless interfaces.

Figure 5-28 QoS Profile

Tabulated below are the ‘QoS Profile’ parameters and the method to configure the configurable parameters:

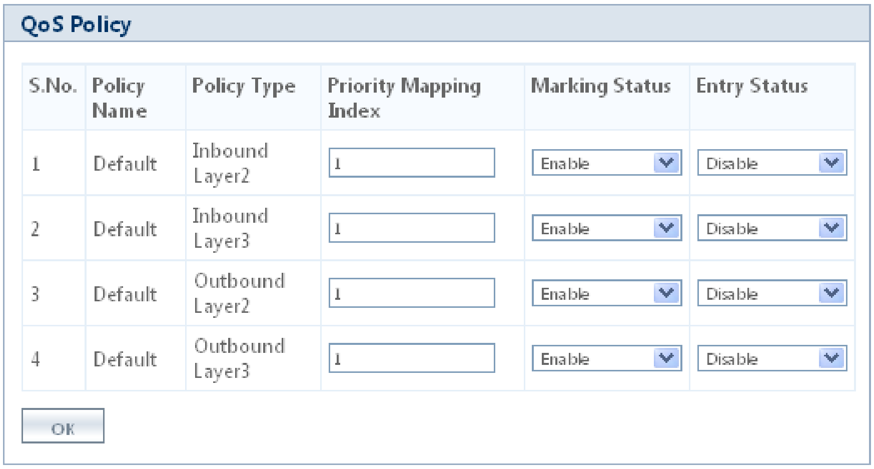
Parameter	Description
QoS Profile Name	Represents the QoS profile name. It is a read-only parameter and cannot be configured. *: By default, the available **QoS Profile Name** is ‘**Default’**.*
Policy Name	Specifies the QoS policy name. By default, the **QoS Policy Name** is **Default**.
EDCA Profile Name	Specifies the EDCA Profile Name. By default, the **EDCA Profile Name** is **Default**.
QoS NoACK Status	Specifies the QoS profile acknowledgement status. By default, the **QoS NoACK Status** is disabled. To configure, select either **Enable** or **Disable** from the drop down menu.

Click **OK** and **COMMIT**, to save the configured parameters.

: QoS Profile Name is applicable only to wireless interfaces.

5.6.5 QoS Policy

Navigate to **CONFIGURATION > QoS > QoS Policy.** The **Qos Policy** screen appears.



QoS Policy

S.No.	Policy Name	Policy Type	Priority Mapping Index	Marking Status	Entry Status
1	Default	Inbound Layer2	1	Enable	Disable
2	Default	Inbound Layer3	1	Enable	Disable
3	Default	Outbound Layer2	1	Enable	Disable
4	Default	Outbound Layer3	1	Enable	Disable

Figure 5-29 QoS Policy

Tabulated below are the ‘QoS Policy’ parameters and the method to configure the configurable parameters:

Parameter	Description
Policy Name	It represents the **QoS Policy Name**. It is a read-only parameter and cannot be configured.

Policy Type	It represents the **QoS Policy Type**. The available policy types are: – **Inbound Layer 2**: Represents inbound traffic direction with layer 2 traffic type. – **Outbound Layer 2**: Represents outbound traffic direction with layer 2 traffic type. – **Inbound Layer 3**: Represents inbound traffic direction with layer 3 traffic type. – **Outbound Layer 3**: Represents outbound traffic direction with layer 3 traffic type. It is a read-only parameter and cannot be configured.
Priority Mapping Index	By default, the priority mapping index is set to 1. While configuring this parameter, note that: – For layer 2 policies configuration, an index from the **802.1d** to **802.1p** mapping table should be specified. – For layer 3 policies configuration, an index from the **802.1d to IP DSCP** mapping table should be specified.
Marking Status	Specifies the **QoS Marking Status**. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu.
Entry Status	Specifies the **Entry Status**. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu. *: If you want to customize a particular policy type, then the entry status for that policy type should be enabled.*

Click **OK** and **COMMIT**, to save the configured parameters.

*: **Policy Name** and **EDCA Profile Name** are not configurable. They are always set to **Default**.*

5.7 Virtual Local Area Network (VLAN)

Virtual Local Area Network (VLAN) is a logical grouping of network hosts. The VLAN members appear (wireless clients) to be on the same physical segment as others, no matter where they are available on the logical LAN or WAN segment. They simplify traffic flow between clients and their frequently used or restricted resources.

In a BSS, clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A client can access the network by connecting to the AP device, configured to support its assigned SSID/VLAN.

The VLAN support is disabled by default. Before enabling VLAN support, certain network settings should be configured and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

Once enabled, VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
    - Improve network performance and reduce latency
- Increase security
    - Secure network restricts members to resources on their own VLAN
    - Clients roam without compromising security

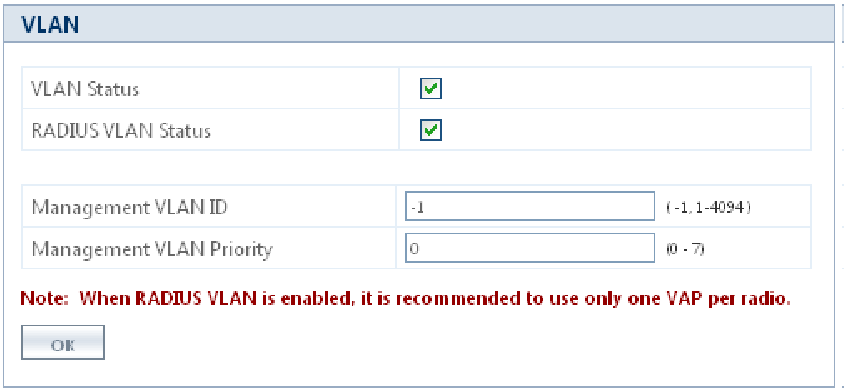
VLAN tagged data is collected and distributed through the AP device's wireless interface(s) based on their network names (SSID). Ethernet port on the AP device connects a wireless cell or network to a wired backbone. The AP device can communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports. On the wired network, a RADIUS server authenticates traffic and a DHCP server manages IP addresses for the VLAN(s). Resources like servers and printers may be present, and a hub may include multiple devices, extending the network over a larger area.

Access Points that are not VLAN-capable, typically transmit broadcast and multicast traffic to all the wireless Network Interface Cards (NICs). This process wastes wireless bandwidth and degrades throughput performance. In comparison, a VLAN-capable AP device is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP device assigns VLAN to the clients, based on a Network Name (SSID). Multiple SSIDs can have same VLAN ID. The device supports up to **8 SSIDs/VLAN** per radio.

The AP device matches the packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

Navigate to **CONFIGURATION > VLAN**. The **VLAN** screen appears.



VLAN

VLAN Status	☑
RADIUS VLAN Status	☑

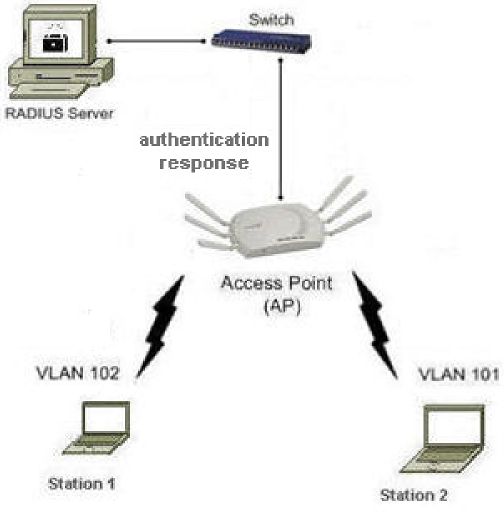
Management VLAN ID	-1	(-1, 1-4094)
Management VLAN Priority	0	(0 - 7)

Note: When RADIUS VLAN is enabled, it is recommended to use only one VAP per radio.

Figure 5-30 VLAN

Tabulated below are the 'VLAN' parameters and the method to configure the configurable parameters:

Parameter	Description
VLAN Status	Specifies the status of VLAN on the AP device. By default, it is disabled. To enable VLAN, check the **VLAN Status** box. : *To configure the Wireless (VAP) VLAN properties and Ethernet VLAN properties, **VLAN status** should be enabled.*

RADIUS VLAN Status	This parameter enables VLAN assignment to AP device's wireless clients through a RADIUS server. This way of RADIUS based VLAN assignment helps: – To reduce the task of manually configuring VLAN parameters on each wireless client connected to the AP device. – The wireless client to remain on the same VLAN as it moves across the network. – To maintain a maximum number of groups/wireless clients under a single VAP network. – To reduce the interference by sending the traffic to intended groups/wireless clients. By default, this parameter is disabled. To enable, check the **Radius VLAN Status** box. **VLAN Status** should also be enabled, failing which the AP device will not perform the VLAN assignment functionality. *: When RADIUS VLAN is enabled, it is recommended to use only one VAP (only for the first SSID) per radio. This will avoid interference between different VAPs with untagged broadcast traffic.* **RADIUS based VLAN Assignment**: When a wireless client tries to connect to an AP device, the AP device forwards the request to the RADIUS Server (a central storage of pre- configured user profiles). On receiving the request from the AP device, the RADIUS server authenticates the wireless client. On successful authentication, RADIUS Server sends an acknowledgment with three vendor specific attributes **Tunnel-Pvt-Group-ID**, **Tunnel-Medium-Type** and **Tunnel-Type**. Refer the *ORiNOCO® 802.11n Access Points - Reference Guide*, for details on how to configure the three vendor-specific attributes within the RADIUS Server.  Switch RADIUS Server authentication response Access Point (AP) VLAN 102 VLAN 101 Station 1 Station 2 **Figure 5-31 RADIUS based VLAN Assignment**

	⚠ **: It is recommended to configure the VLAN-Ethernet in Trunk mode, when RADIUS VLAN is enabled. This reduces the interference problems, by sending the VLAN traffic (broadcast/multicast) only to the intended wireless clients.**
Management VLAN ID	Specifies the Management VLAN ID. The wireless clients must tag the management frames sent to the AP device, along with the management VLAN ID. By default, the Management VLAN ID is set to -1; which indicates that no tag is added to the management frame. To enable, enter a value ranging from 1 to 4094. ✎ *: If a non-zero management VLAN ID is configured, then management access to the AP device is restricted to wired or wireless hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN, before attempting to manage the AP device.*
Management VLAN Priority	Specifies the IEEE 802.1p priority set for the management frames. By default, it is set to 0. To configure, set the VLAN priority in the range of 0 to 7.

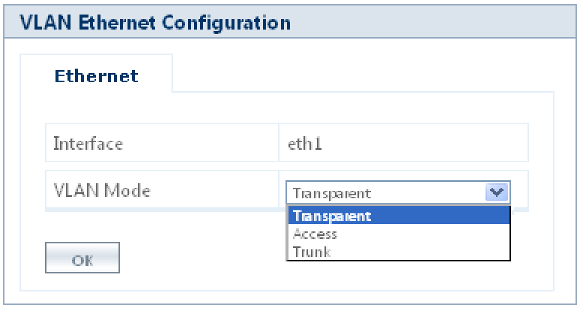
Click **OK** and **COMMIT**, to save the configured parameters.

✎ *:*

- *When VLAN is enabled, ensure that all nodes in the network share the same VLAN ID as this will ensure that all the access points are managed easily.*
- *In the case of RADIUS server authentication or EAP authentication, if the RADIUS server is present on any VLAN, then the RADIUS server should be member of the management VLAN ID of AP device.*

5.7.1 VLAN Ethernet Configuration

To enable VLAN on the ethernet interface, navigate to **CONFIGURATION** > **VLAN** > **Ethernet**. The **VLAN Ethernet Configuration** screen appears.



VLAN Ethernet Configuration

Ethernet

Interface eth1

VLAN Mode Transparent

Figure 5-32 VLAN Ethernet Configuration

Tabulated below are the 'VLAN Ethernet' parameters and the method to configure the configurable parameters:

Parameter	Description
Interface	A read-only parameter that represents the interface on which VLAN is configured.

<table>
<tr>
<td>VLAN Mode</td>
<td>

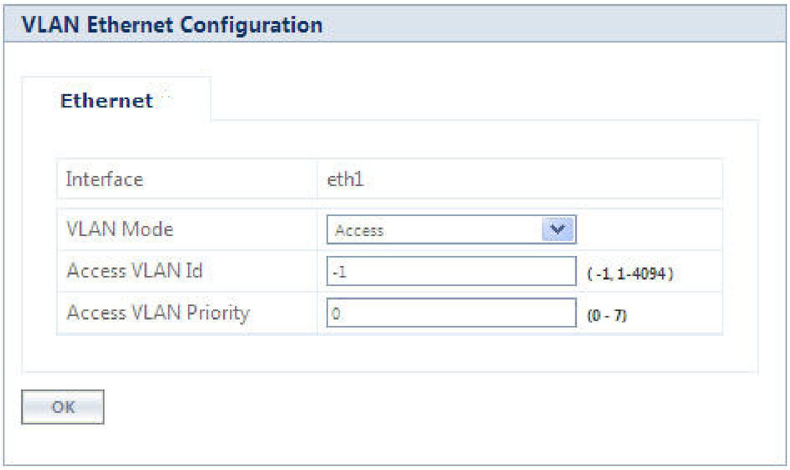
Specifies the VLAN mode to be configured on the ethernet interface. You can configure any of the following VLAN modes on the ethernet interface:

a. **Transparent Mode**: Transparent Mode is configurable on the ethernet interface of the AP device. It is equivalent to NO VLAN support and is the default mode. It is used to connect VLAN aware/unaware networks. An interface in transparent mode forwards both tagged and untagged frames.

To configure, select **Transparent Mode** from the **VLAN Mode** box and click **OK**.

b. **Access Mode**: Access Mode is configurable on the wireless, ethernet and management interfaces of the AP device. This mode is used to connect VLAN aware networks with VLAN unaware networks. In Access Mode, tagged frames with specified Access VLAN ID going out of the AP device through the interface are untagged and forwarded. The untagged frames coming into the AP device through the interface are tagged with specified Access VLAN ID and forwarded.

Select **Access Mode** from the **VLAN Mode** box and click **OK**. The configuration screen appears:



VLAN Ethernet Configuration

Interface: eth1

VLAN Mode: Access

Access VLAN Id: -1 (-1, 1-4094)

Access VLAN Priority: 0 (0 - 7)

Figure 5-33 VLAN Access Mode

Configure the following properties:

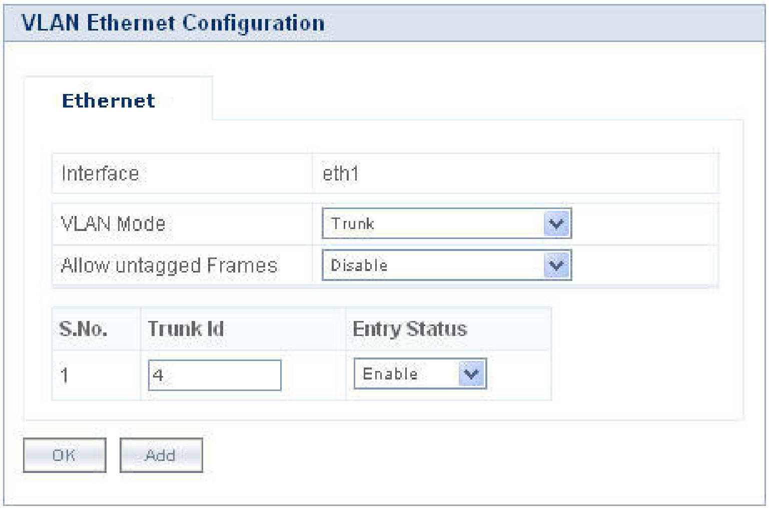
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Access VLAN ID</td><td>Specifies an access VLAN ID.
By default, it is -1, which indicates that no tag is added to the frame. To configure, enter the **Access VLAN ID** either as -1 or a value ranging from 1 to 4094.</td></tr>
<tr><td>Access VLAN Priority</td><td>Specifies the IEEE 802.1p priority set for the frames.
By default, it is 0. To configure, enter a value in the range of 0 to 7.</td></tr>
</table>

Click **OK** and **COMMIT**, to save the configured parameters.

</td>
</tr>
</table>

c. **Trunk Mode**: Trunk Mode is configurable on the ethernet interface of the AP device. It is mainly used to connect a VLAN aware network with an another VLAN aware network. An interface in the Trunk mode only forwards those tagged frames whose VLAN ID matches with a VLAN ID that is present in trunk table. All the other frames will be dropped.

Select **Trunk Mode** from the **VLAN Mode** box and click **OK**. The configuration screen appears:



VLAN Ethernet Configuration

Ethernet

Interface	eth1
VLAN Mode	Trunk
Allow untagged Frames	Disable

S.No.	Trunk Id	Entry Status
1	4	Enable

Figure 5-34 VLAN Trunk Mode

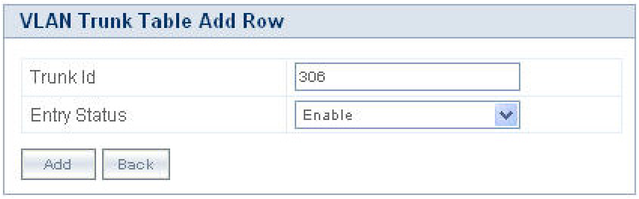
Configure the following parameters in Trunk Mode:

Parameter	Description
Allow Untagged Frames	To configure, either select **Enable** or **Disable** from the drop down menu. – If enabled, an interface in trunk mode forwards both tagged frames whose VLAN ID matches with one of the VLAN IDs in the trunk table and untagged frames. – If disabled, an interface in trunk mode forwards only tagged frames and drops untagged frames.

Click **OK** and **COMMIT**, to save the configured parameters.

VLAN Trunk Table

To add new entries, click **Add**. The **VLAN Trunk Table Add Row** screen appears:



VLAN Trunk Table Add Row

Trunk Id	306
Entry Status	Enable

Figure 5-35 VLAN Trunk Table - Add Row

Configure the following parameters to add a row:

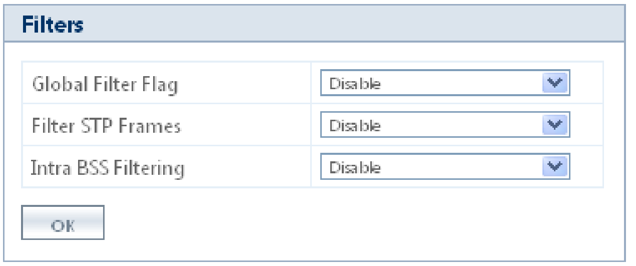
Parameter	Description
Trunk ID	Specifies the Trunk Id. To configure, enter the **Trunk Id** value in the range of 1 to 4094. The maximum Trunk Ids that you can create are 256.
Entry Status	Specifies the status of the entry being added. To configure, select either **Enable** or **Disable** from the drop down menu.

Click **Add**, to save the configured parameters and add a new row.

5.8 Filters

The Packet Filter feature helps you to control the amount of traffic exchanged between the wired and wireless networks. By using filters, you can restrict any unauthorized packets from accessing the network.

Navigate to **CONFIGURATION > Filters**. The **Filters** screen appears.



Filters

Global Filter Flag	Disable
Filter STP Frames	Disable
Intra BSS Filtering	Disable

Figure 5-36 Filters

Tabulated below are the ‘Filters’ and method to configure the configurable parameters:

Parameter	Description
Global Filter Flag	Specifies the global filter on the AP device. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu. *: If the Global Filter Flag is not enabled on the AP device, then none of the filters can be applied.*
Filter STP Frames	This feature helps to filter the STP frames and avoid loops that occur within a network. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu. – If enabled, the STP frames in the system are bridged. – If disabled, the STP frames encountered on a network are terminated at bridge. *: In case of AP-800 and AP-8000, this parameter is named as “STP Forward Frame Status”.*

Intra BSS Filtering	This parameter enables you to prevent the wireless clients within a BSS from exchanging traffic. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu.

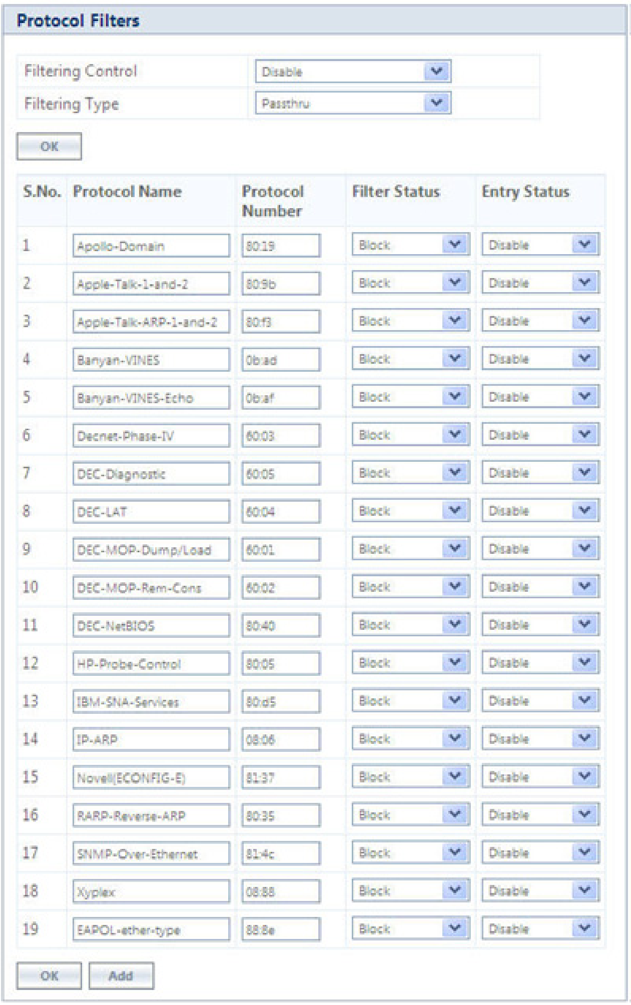
Click **OK** and **COMMIT**, to save the configured parameters.

AP device supports the following filters:

- Protocol Filters
- Static MAC Address Filters
- Advanced Filters
- TCP/UDP Port Filters
- Storm Threshold Filters
- Packet Forwarding

5.8.1 Protocol Filters

The Protocol Filter blocks or forwards the packets based on the protocols supported by the AP device. Navigate to **CONFIGURATION > Filters > Protocol Filters**. The **Protocol Filters** screen appears.



Protocol Filters

Filtering Control	Disable
Filtering Type	Passthru

S.No.	Protocol Name	Protocol Number	Filter Status	Entry Status
1	Apollo-Domain	80:19	Block	Disable
2	Apple-Talk-1-and-2	80:9b	Block	Disable
3	Apple-Talk-ARP-1-and-2	80:f3	Block	Disable
4	Banyan-VINES	0b:ad	Block	Disable
5	Banyan-VINES-Echo	0b:af	Block	Disable
6	Decnet-Phase-IV	60:03	Block	Disable
7	DEC-Diagnostic	60:05	Block	Disable
8	DEC-LAT	60:04	Block	Disable
9	DEC-MOP-Dump/Load	60:01	Block	Disable
10	DEC-MOP-Rem-Cons	60:02	Block	Disable
11	DEC-NetBIOS	80:40	Block	Disable
12	HP-Probe-Control	80:05	Block	Disable
13	IBM-SNA-Services	80:d5	Block	Disable
14	IP-ARP	08:06	Block	Disable
15	Novell(ECONFIG-E)	81:37	Block	Disable
16	RARP-Reverse-ARP	80:35	Block	Disable
17	SNMP-Over-Ethernet	81:4c	Block	Disable
18	Xyplex	08:88	Block	Disable
19	EAPOL-ether-type	88:8e	Block	Disable

Figure 5-37 Protocol Filters

Tabulated below are the ‘Protocol Filter’ parameters and the method to configure the configurable parameters:

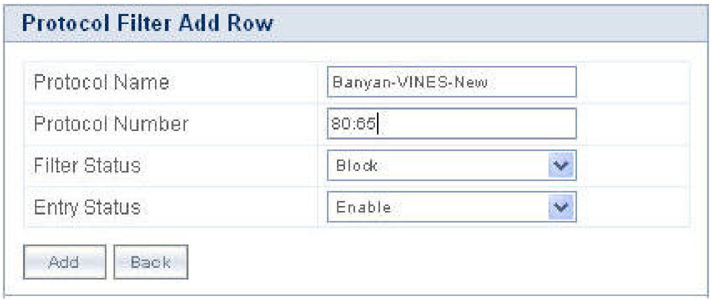
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Filtering Control</td><td>Specifies the interface on which filtering is applied. By default, it is disabled. It can be configured as:
– <b>Ethernet</b>: Packets are examined at the ethernet interface.
– <b>Wireless</b>: Packets are examined at the wireless interface.
– <b>All interfaces</b>: Packets are examined at both ethernet and wireless interface.
To configure, select an interface from the <b>Filtering Control</b> drop down menu.</td></tr>
<tr><td>Filtering Type</td><td>Specifies the action to be performed on the data packets whose protocol type is not defined in the protocol filter table (this table contains a list of default protocols supported by the AP device and the protocols defined by the user), or whose entry status is in <i>Disable</i> state. The available filtering types are:
– <b>Block</b>: The protocols with entry status <i>Disable</i> or the protocols which do not exist in the protocol filtering table are blocked.
– <b>Passthru</b>: The protocols with entry status <i>Disable</i> or the protocols which do not exist in the protocol filtering table are allowed through the interface.
To configure, select a <b>Filtering Type</b> from the drop down menu.</td></tr>
<tr><td colspan="2"><b>Protocol Filter Table</b>
The ‘Protocol Filters’ screen displays a list of default protocols supported by the AP device and the protocols created by the user. By default, the system generates 19 protocols entries. Each of the protocol contains the following information:</td></tr>
<tr><td>Protocol Name</td><td>Specifies the name of the protocol.
✎: <i>The system throws an error when you try to edit the name of a default protocol.</i></td></tr>
<tr><td>Protocol Number</td><td>Specifies the protocol number. It is in 4 digit hexadecimal format.
✎: <i>The system throws an error when you try to edit the protocol number of a default protocol.</i></td></tr>
<tr><td>Filter Status</td><td>Specifies the status of the filter. By default, it is <b>Block</b>. To configure, select the <b>Filter Status</b> as either <b>Block</b> or <b>Passthru</b> from the drop down menu.
– <b>Passthru</b>: When the filter status is set to <b>Passthru</b> and <b>Entry Status</b> is Enable, all packets whose protocol matches with the given protocol number are forwarded on the selected interface.
– <b>Block</b>: When the filter status is set to <b>Block</b> and <b>Entry Status</b> is Enable, all packets whose protocol matches with the given protocol number are dropped on the selected interface.</td></tr>
</table>

Entry Status	Specifies entry status of the protocol. By default, it is disabled. To configure, select either **Enable**/**Disable**/**Delete** from the drop down menu. – **Enable**: Enables the filter status on a protocol. – **Disable**: Disables the filter status on a protocol. – **Delete**: Deletes a protocol entry from the Protocol Filter Table. *: System-defined default protocols entries cannot be deleted.*

Click **OK** and **COMMIT**, to save the configured parameters.

Add New Entries to the Protocol Filter Table

To add user-defined protocols to the Protocol Filter Table, click **Add** in the **Protocol Filters** screen. The **Protocol Filter Add Row** screen appears.



Protocol Filter Add Row

Protocol Name	Banyan-VINES-New
Protocol Number	80:65
Filter Status	Block
Entry Status	Enable

Figure 5-38 Protocol Filter Add Row

Configure all the parameters and click **Add**.

: The maximum number of Protocol Filters that can be added are 64.

5.8.2 Static MAC Address Filters

The 'Static MAC Address Filter' optimizes the performance of a wireless (and wired) network. With this feature configured, the AP device can block traffic between wired devices and wireless devices based on the MAC address.

For example, you can set up a static MAC filter to prevent wireless clients from communicating with a specific server on the ethernet network. You can also use this filter to block unnecessary multicast packets from being forwarded to the wireless network.

Each MAC address or Mask comprises of 12 hexadecimal digits (0-9, A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (0 or 1)).

Taken together, a MAC address/Mask pair specifies an address or a range of MAC addresses that the AP device will look for when examining packets. The AP device uses Boolean logic to perform an "AND" operation between the MAC address and the Mask at the bit level. A Mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a Mask of FF:FF:FF:FF:FF:FF applies only to the specified MAC address.

For example, if the MAC address is 00:20:A6:12:54:C3 and the Mask is FF:FF:FF:00:00:00, the AP device will examine the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the Mask is FF:FF:FF:FF:FF:FF, the AP device will only look for the specific MAC address (in this case, 00:20:A6:12:54:C3).

You can configure the 'Static MAC address Filter' parameters depending on the following scenarios:

- To prevent entire traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC address and Wired Mask (leave the Wireless MAC address and Wireless Mask set to all zeros).
- To prevent entire traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC address and Wireless Mask (leave the Wired MAC address and Wired Mask set to all zeros).
- To prevent traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters. Configure the wired and wireless MAC address and set the wired and wireless mask to all Fs.
- To prevent all traffic from a specific wired group MAC address from being forwarded to the wireless network, configure only the Wired MAC address and Wired Mask (leave the Wireless MAC address and Wireless Mask set to all zeros).
- To prevent entire traffic from a specific wireless group MAC address from being forwarded to the wired network, configure only the Wireless MAC address and Wireless Mask (leave the Wired MAC address and Wired Mask set to all zeros).
- To prevent traffic between a specific wired group MAC address and a specific wireless group MAC address, configure all four parameters. Configure the wired and wireless MAC address and set the wired and wireless mask to all Fs.

5.8.2.1 Static MAC Filter Examples

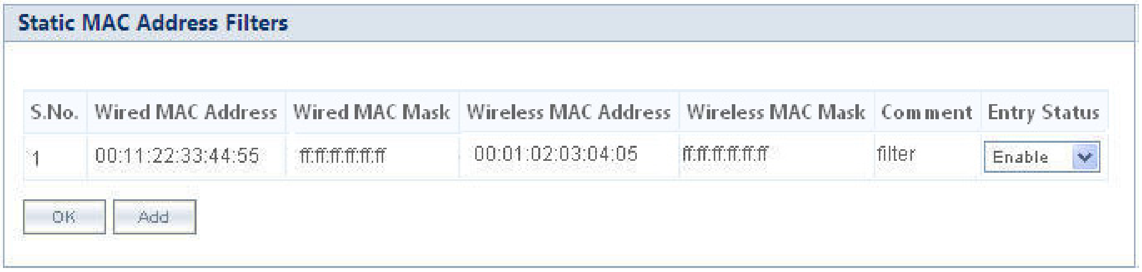
Consider a network that contains a wired interface and three wireless clients. The MAC address for each unit is as follows:

- Wired Interface: 00:40:F4:1C:DB:6A
- Wireless Client 1: 00:02:2D:51:94:E4
- Wireless Client 2: 00:02:2D:51:32:12
- Wireless Client 3: 00:20:A6:12:4E:38

Scenario	Example	Result
Prevent two specific devices from communicating	Configure the following settings to prevent the Wired Interface and Wireless Client 1 from communicating: Wired MAC address: 00:40:F4:1C:DB:6A Wired Mask: FF:FF:FF:FF:FF:FF Wireless MAC address: 00:02:2D:51:94:E4 Wireless Mask: FF:FF:FF:FF:FF:FF	Traffic between the Wired Interface and Wireless Client 1 is blocked. Wireless Clients 2 and 3 can still communicate with the Wired Interface.
Prevent multiple Wireless devices from communicating with a single wired device	Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Interface: Wired MAC address: 00:40:F4:1C:DB:6A Wired Mask: FF:FF:FF:FF:FF:FF Wireless MAC address: 00:02:2D:51:94:E4 Wireless Mask: FF:FF:FF:00:00:00	When a bitwise “AND” is performed on the Wireless MAC address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Interface and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Interface since it has a different prefix (00:20:A6).

Prevent all wireless devices from communicating with a single wired device	Configure the following settings to prevent all three Wireless Clients from communicating with Wired Interface 1: Wired MAC address: 00:40:F4:1C:DB:6A Wired Mask: FF:FF:FF:FF:FF:FF Wireless MAC address: 00:00:00:00:00:00 Wireless Mask: 00:00:00:00:00:00	The device blocks all traffic between Wired Interface 1 and all wireless clients.
Prevent a wireless device from communicating with the wired network	Configure the following settings to prevent Wireless Client 3 from communicating with any device on the ethernet: Wired MAC address: 00:00:00:00:00:00 Wired Mask: 00:00:00:00:00:00 Wireless MAC address: 00:20:A6:12:4E:38 Wireless Mask: FF:FF:FF:FF:FF:FF	The device blocks all traffic between Wireless Client 3 and the ethernet network.

Navigate to **CONFIGURATION > Filters > Static MAC Address Filters.** The **Static MAC Address Filters** screen appears:

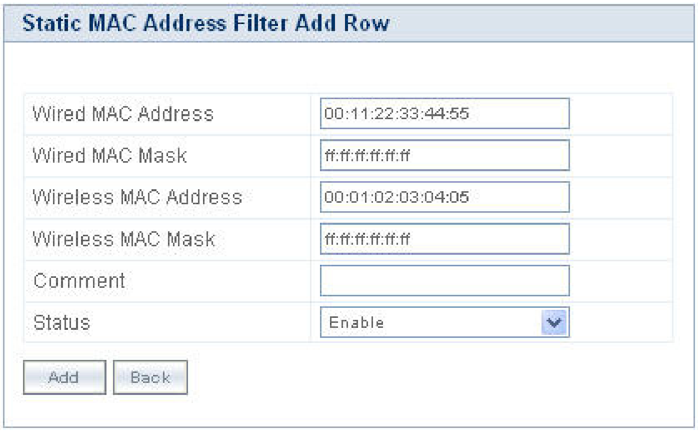


Static MAC Address Filters

S.No.	Wired MAC Address	Wired MAC Mask	Wireless MAC Address	Wireless MAC Mask	Comment	Entry Status
1	00:11:22:33:44:55	ff:ff:ff:ff:ff:ff	00:01:02:03:04:05	ff:ff:ff:ff:ff:ff	filter	Enable

Figure 5-39 Static MAC Address Filters

The **Static MAC Address Filters** screen contains a list of entries specifying the Wireless/Wired MAC addresses and Wireless/Wired MAC Mask to block the traffic between wired and wireless devices. To add an entry, click **Add**. The **Static MAC Address Filter Add Row** screen appears.



Static MAC Address Filter Add Row

Wired MAC Address	00:11:22:33:44:55
Wired MAC Mask	ff:ff:ff:ff:ff:ff
Wireless MAC Address	00:01:02:03:04:05
Wireless MAC Mask	ff:ff:ff:ff:ff:ff
Comment	
Status	Enable

Figure 5-40 Static MAC Address Filter - Add Entries

Tabulated below are the 'Static MAC Address Filter' parameters and the method to configure the configurable parameters:

Parameter	Description
Wired MAC Address	Specifies the MAC address of the device on the wired network that is restricted from communicating with a device on the wireless network. To configure, enter a **Wired MAC Address**.
Wired MAC Mask	Specifies the range of the wired MAC addresses to which the filter is applied. To configure, enter a Wired MAC Mask.
Wireless MAC Address	Specifies the MAC address of the device on the wireless network that is restricted from communicating with a device on the wired network. To configure, enter a **Wireless MAC Address**.
Wireless MAC Mask	Specifies the range of the wireless MAC addresses to which the filter is applied. To configure, enter a **Wireless MAC Mask**.
Comment	Specifies the user-comment on a Static MAC Filter table entry.
Status	Specifies the status of the filter added. **Enable** the status to apply filters between the wired and wireless devices. By default, it is enabled. To disable, click **Disable** from the **Status** box.

Click **Add**, to save the configured entry.

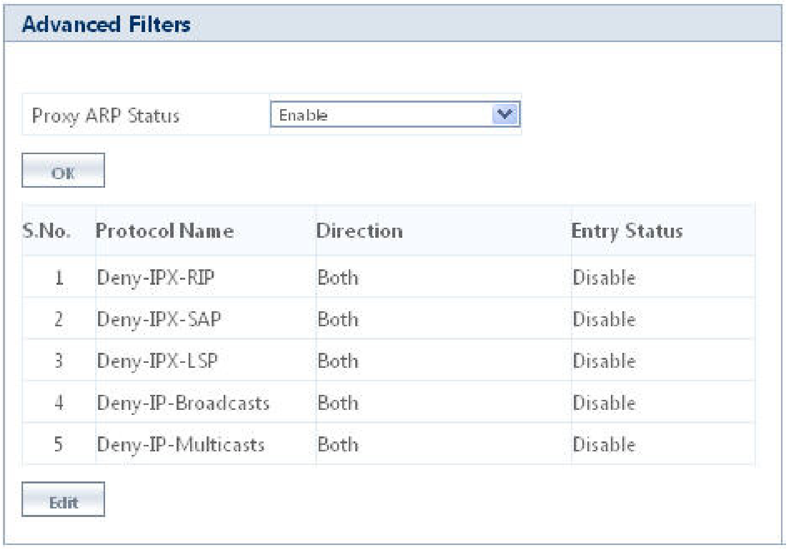
:

- *A maximum of 200 Static MAC Filters can be added.*
- *Wired and Wireless MAC address cannot have broadcast and multicast MAC address.*

5.8.3 Advanced Filters

The 'Advanced Filters' feature enables you to block the specific IP Protocol traffic on the network.

Navigate to **CONFIGURATION > Filters > Advanced Filters**. The **Advanced Filters** screen appears.



Advanced Filters

Proxy ARP Status: Enable

S.No.	Protocol Name	Direction	Entry Status
1	Deny-IPX-RIP	Both	Disable
2	Deny-IPX-SAP	Both	Disable
3	Deny-IPX-LSP	Both	Disable
4	Deny-IP-Broadcasts	Both	Disable
5	Deny-IP-Multicasts	Both	Disable

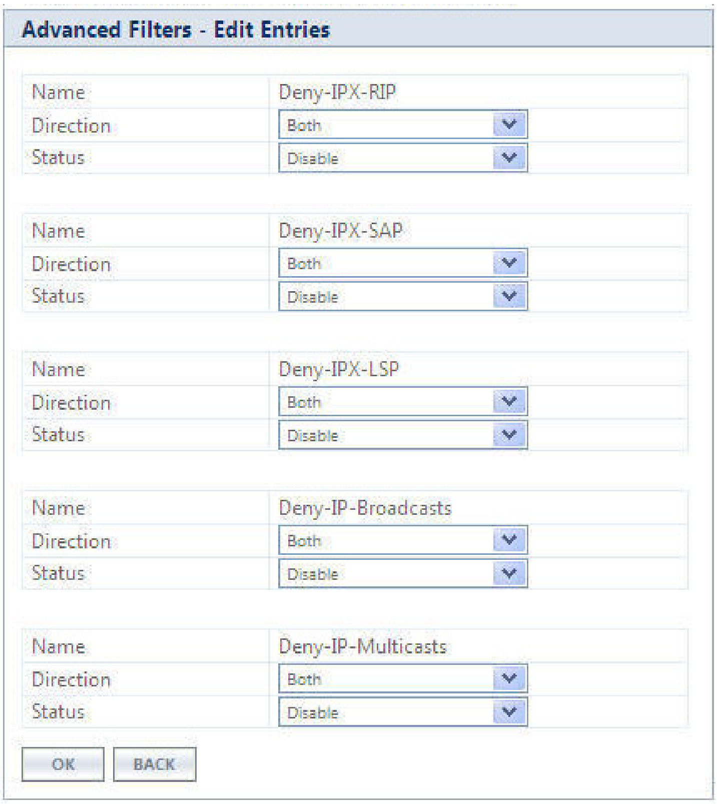
Figure 5-41 Advanced Filters

Tabulated below are the 'Advanced Filter' parameters and the method to configure the configurable parameters:

Parameter	Description
Proxy ARP Status	Specifies the status of the Proxy ARP feature on the AP device. By functioning as a **Proxy ARP,** the AP device helps: – To reduce unnecessary flow of broadcast traffic to all the wireless clients, without disturbing every wireless client on the network. – To power save the wireless clients as they need not wake up for ARP broadcasts. – The clients to learn the MAC addresses faster When two clients connected to an AP device try to communicate, they send an ARP request to get the MAC address of the destined client. AP device responds to this ARP request and looks for the MAC address of the destined client in its Proxy ARP table. On finding the MAC address, AP device forwards the MAC address to the client, without disturbing other wireless clients on the network. Wireless client updates its ARP table with the MAC address and forwards the ICMP packet to the destination via AP device. By default, **Proxy ARP Status** is disabled. To enable this feature, select **Enable** from the drop down menu.
Advanced Filter Table Advance Filter Table contains a list of all protocols to which Advanced Filters are applied.	
Protocol Name	Specifies the name of the protocol to be filtered. Following are the five default protocols, that support advanced filters: – Deny-IPX-RIP – Deny-IPX-SAP – Deny-IPX-LSP – Deny-IP-Broadcasts – Deny-IP-Multicasts
Direction	Specifies the direction of an IP Protocol traffic. The direction can be enabled either from ethernet to wireless, wireless to ethernet or both ways.
Entry Status	Specifies the status of the filter applied on the IP Protocol.

Click **OK** and **COMMIT**, to save the configured parameters.

To edit any protocol entry, click **Edit.** The **Advanced Filters - Edit Entries** screen appears.



Advanced Filters - Edit Entries

Name	Deny-IPX-RIP
Direction	Both
Status	Disable

Name	Deny-IPX-SAP
Direction	Both
Status	Disable

Name	Deny-IPX-LSP
Direction	Both
Status	Disable

Name	Deny-IP-Broadcasts
Direction	Both
Status	Disable

Name	Deny-IP-Multicasts
Direction	Both
Status	Disable

Figure 5-42 Advanced Filters - Edit Entries

Modify the **Direction** and **Status** of the desired IP Protocol. Click **OK** and **COMMIT**, to save the configured parameters.

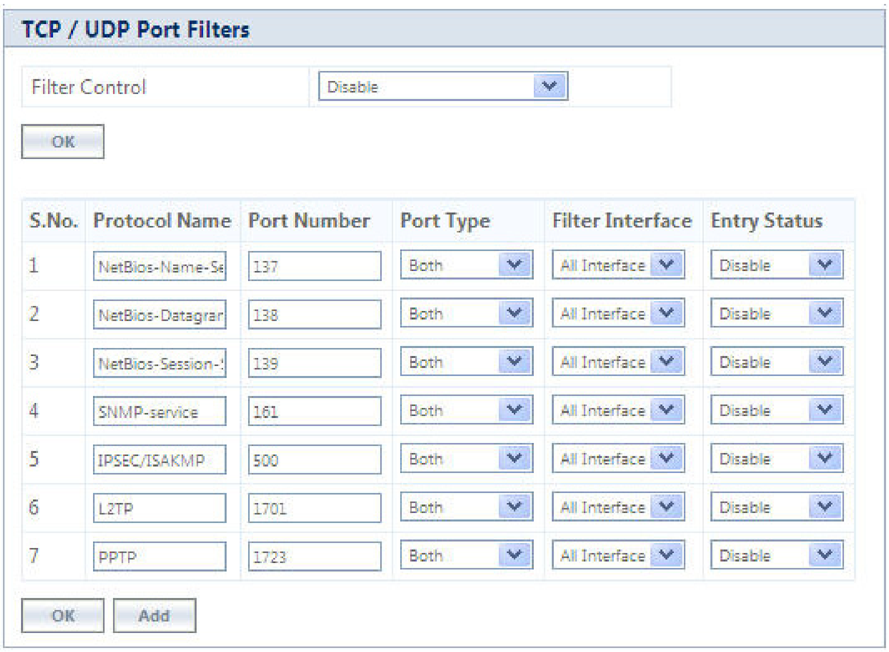
5.8.4 TCP/UDP Port Filters

Port-based filtering enables you to control wireless user access to network services by selectively blocking TCP/UDP protocols through the device. A user specifies a Protocol Name, Port Number, Port Type (TCP, UDP, or TCP/UDP), and filtering interfaces (Only Wireless, Only Ethernet or Both) in order to block access to services such as Telnet and FTP, and traffic such as NETBIOS and HTTP.

For example, a device with the following configuration would discard frames received on its ethernet interface with a UDP destination port number of 137, effectively blocking NETBIOS Name Service packets.

Protocol Name	Port Number	Port Type	Filter Interface	Entry Status (Enable/Disable)
NETBIOS Name Service	137	UDP	Ethernet	Enable

Navigate to **CONFIGURATION > Filters > TCP/UDP Port Filters**. The **TCP / UDP Port Filters** screen appears.



TCP / UDP Port Filters

Filter Control	Disable

S.No.	Protocol Name	Port Number	Port Type	Filter Interface	Entry Status
1	NetBios-Name-Se	137	Both	All Interface	Disable
2	NetBios-Datagrar	138	Both	All Interface	Disable
3	NetBios-Session-:	139	Both	All Interface	Disable
4	SNMP-service	161	Both	All Interface	Disable
5	IPSEC/ISAKMP	500	Both	All Interface	Disable
6	L2TP	1701	Both	All Interface	Disable
7	PPTP	1723	Both	All Interface	Disable

Figure 5-43 TCP/UDP Port Filters

Tabulated below are the 'TCP/UDP Port Filters' parameters and the method to configure the configurable parameters:

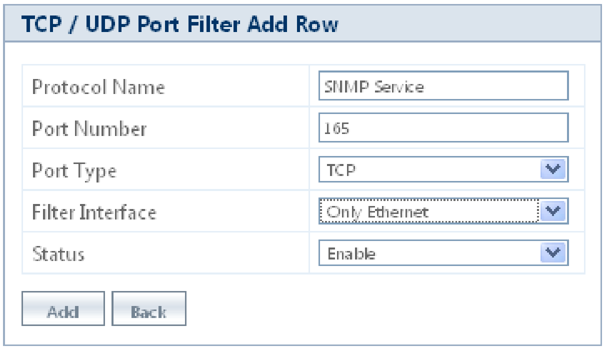
Parameter	Description
Filter Control	Specifies the *Filter Control* feature on the device. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu.
TCP/UDP Port Filter Table The TCP/UDP Port Filters screen displays a list of default protocols supported by the device and the protocols created by the user. By default, the system generates seven protocols entries. Each of the Protocol contains the following information:	
Protocol Name	Specifies the name of the Protocol. *: The system throws an error when you try to edit the name of a default protocol.*
Protocol Number	Specifies the TCP/UDP port number. *: The system throws an error when you try to edit the port number of a default protocol.*
Port Type	Specifies the type of the port. Select the port type as TCP or UDP or both from the **Port Type** box. By default, it is **Both** for the default entries and **TCP** for the newly added entries.
Filter Interface	Specifies the parameter used to configure the interface to which the filter is applied. Select the interface as either **Only Ethernet**, **Only Wireless**, or **All Interfaces** from the **Filter Interface** box.

Status	Set the entry status as Enable/Disable/Delete. – **Enable**: The device filters the TCP/UDP protocols. – **Disable**: The device allows all the TCP/UDP protocols. – **Delete**: The device deletes a protocol entry from the Filter Table. *: System-defined default protocols entries cannot be deleted.*

Click **OK** and **COMMIT**, to save the configured parameters.

5.8.4.1 Add New Entries to TCP/UDP Port Filter Table

To add user-defined protocols to the TCP/UDP Port Filter Table, click **Add** in the **TCP/UDP Port Filters** screen. The **TCP/UDP Port Filter Add Row** screen appears.



TCP / UDP Port Filter Add Row

Protocol Name	SNMP Service
Port Number	165
Port Type	TCP
Filter Interface	Only Ethernet
Status	Enable

Figure 5-44 TCP/UDP Port Filter Table - Add Entries

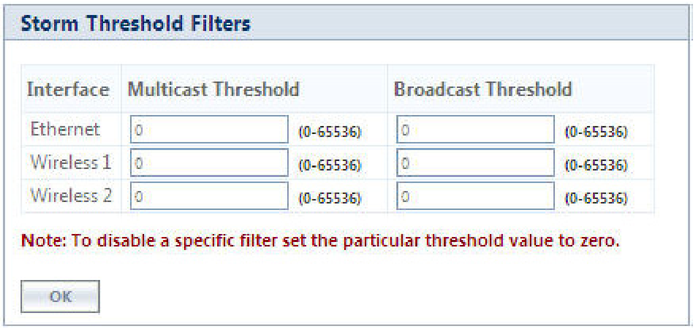
Configure all the parameters and click **Add**.

: A maximum of 64 TCP/IUDP Port Filters can be added.

5.8.5 Storm Threshold Filters

The Storm Threshold Filter restricts the excessive inbound multicast or broadcast traffic on layer two interfaces. This protects against broadcast storms resulting from spanning tree mis-configuration. A broadcast/multicast filtering mechanism needs to be enabled so that a large percentage of the wireless link remains available to the connected mobile terminals.

Navigate to **CONFIGURATION > Filters > Storm Threshold Filters**. The **Storm Threshold Filters** screen appears.



Storm Threshold Filters

Interface	Multicast Threshold		Broadcast Threshold	
Ethernet	0	(0-65536)	0	(0-65536)
Wireless 1	0	(0-65536)	0	(0-65536)
Wireless 2	0	(0-65536)	0	(0-65536)

Note: To disable a specific filter set the particular threshold value to zero.

Figure 5-45 Storm Threshold Filters

Tabulated below are the ‘Storm Threshold Filter’ parameters and the method to configure the configurable parameters:

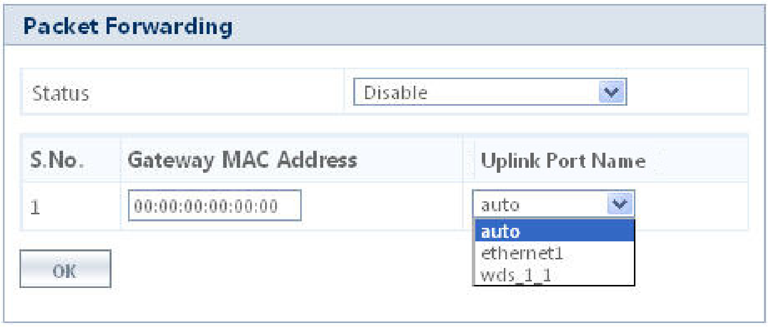
Parameter	Description
Interface	Represents the type of interface to which filters are applied. The Storm Threshold filter can be used to filter the traffic on either ethernet interface or wireless interface. By default, Storm Threshold filtering is disabled on both ethernet and wireless interfaces.
Multicast Threshold	Specifies the threshold value of the multicast packets to be processed for the ethernet or wireless interface. Packets more than threshold value are dropped. If threshold value for multicast packets is set to '0', filtering is disabled. The default **Multicast Threshold** value is 0 per second. To configure, enter a value ranging from 0 to 65536.
Broadcast Threshold	Specifies the threshold value of the broadcast packets to be processed for the ethernet or wireless interface. Packets more than threshold value are dropped. If threshold value for broadcast packets is set to '0', filtering is disabled. The default **Broadcast Threshold** value is 0 per second. To configure, enter a value ranging from 0 to 65536.

Click **OK** and **COMMIT**, to save the configured parameters.

5.8.6 Packet Forwarding

Packet Forwarding is the process of relaying the data packets, through a pre-configured gateway (connected to the AP device either through ethernet or WDS interface). On receiving the traffic (uplink) from the wireless clients, the AP device forwards the traffic to the destined gateway, by tagging it with the gateway MAC address. The gateway device (configured according to the user requirement) monitors the uplink traffic, for improved security.

Navigate to **CONFIGURATION** > **Filters** > **Packet Forwarding**. The **Packet Forwarding** screen appears.



Packet Forwarding

Status: Disable

S.No.	Gateway MAC Address	Uplink Port Name
1	00:00:00:00:00:00	auto

Figure 5-46 Packet Forwarding

Tabulated below are the ‘Packet Forwarding’ parameters and method to configure the configurable parameters:

Parameter	Description
Status	Specifies the status of **Packet Forwarding** on the AP device. By default, it is disabled. To configure, select **Enable** from the drop down menu.
Gateway MAC Address	Specifies the MAC address of the destined gateway device. To configure, enter the **Gateway MAC Address**.
Uplink Port Name	Specifies the port of the gateway, that should participate in **Packet Forwarding**. The **Uplink Port Name** can be configured as any of the following: – **Auto**: Configure the **Uplink Port Name** to **Auto**, when the interface of the destined gateway port is unknown. Based on the configured peer MAC address, the AP device automatically detects the gateway port by checking within its bridge table. – **Ethernet**: Configure the **Uplink Port Name** to **Ethernet**, when the destined gateway port is connected on ethernet interface of the AP device. – **WDS**: Configure the **Uplink Port Name** to **WDS**, when the destined gateway port is connected on WDS interface of the AP device. Based on the radio (interface 1 and interface 2) and the VAP enabled, the Uplink Port Name configured in WDS is represented as: **WDS_X_Y**; where **X** = the radio on which the VAP is enabled (interface 1 or interface 2) **Y** = the VAP enabled on a radio (VAP 1, VAP 2......VAP 8) For example, if Uplink Port Name is **WDS_1_2** then, **1** represents radio 1 (interface 1) and **2** represents VAP 2.

Click **OK** and **COMMIT**, to save the configured parameters.

📝:

- *Enabling Packet Forwarding within the same network, stops the communication between all the wireless clients and forwards data to the gateway.*
- *If the Uplink Port is enabled as ‘Auto’, then only unicast traffic is forwarded to the gateway. The multicast and broadcast traffic is forwarded to wireless clients.*
- *If the Uplink Port is enabled as ‘Ethernet’ or ‘WDS_X_Y’, then all the traffic (unicast, multicast and broadcast) between the wireless clients is forwarded to the gateway.*

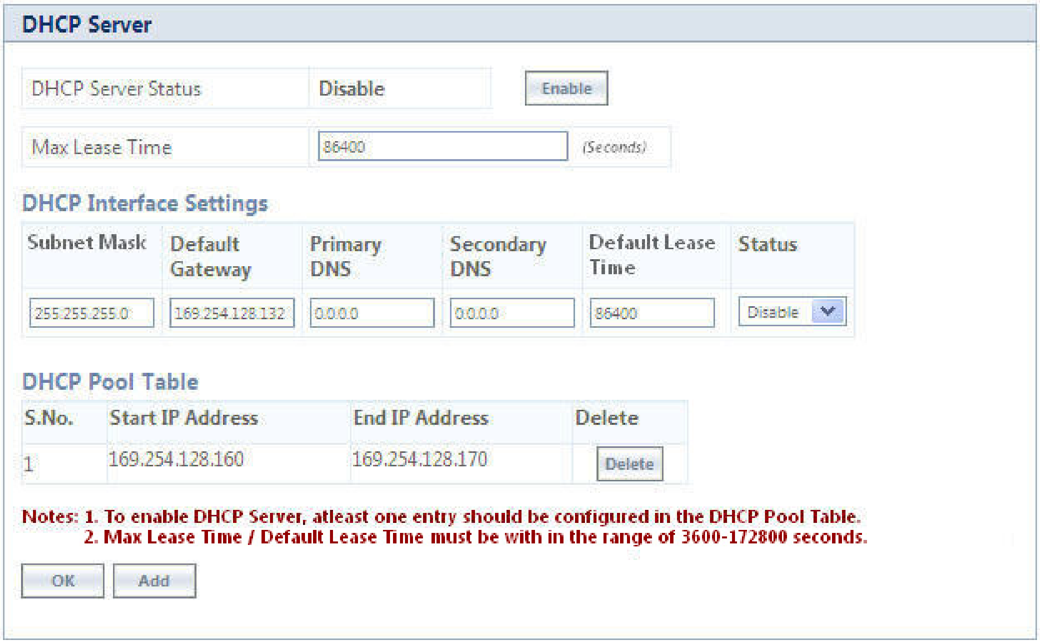
5.9 DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to assign an IP address to a device from a defined range of IP addresses configured for a given network. It allows you to distribute IP addresses from a central point to various hosts and simplifies the process of configuring the IP addresses to individual hosts.

5.9.1 DHCP Server

DHCP automatically allocates network addresses and also delivers configuration parameters dynamically to the clients from the DHCP Server. When DHCP server is enabled, it allows allocation of IP addresses to clients connected to the device.

Navigate to **CONFIGURATION** > **DHCP** > **DHCP Server.** The **DHCP Server** screen appears.



DHCP Server

DHCP Server Status	Disable	Enable
Max Lease Time	86400	(Seconds)

DHCP Interface Settings

Subnet Mask	Default Gateway	Primary DNS	Secondary DNS	Default Lease Time	Status
255.255.255.0	169.254.128.132	0.0.0.0	0.0.0.0	86400	Disable

DHCP Pool Table

S.No.	Start IP Address	End IP Address	Delete
1	169.254.128.160	169.254.128.170	Delete

Notes: 1. To enable DHCP Server, atleast one entry should be configured in the DHCP Pool Table.
2. Max Lease Time / Default Lease Time must be with in the range of 3600-172800 seconds.

Figure 5-47 DHCP Server

Tabulated below are the 'DHCP Server' parameters and method to configure the configurable parameters:

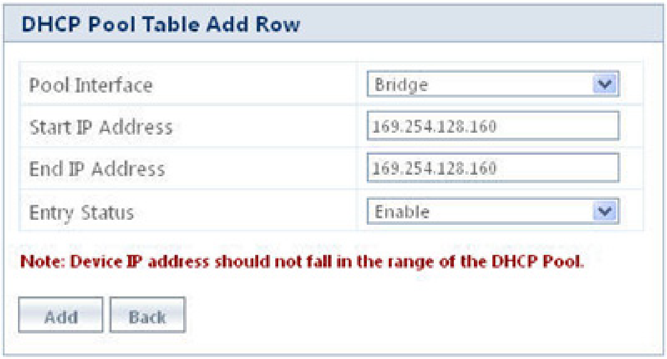
Parameter	Description
DHCP Server Status	Specifies the status of the DHCP Server functionality on the device. By default, it is disabled. To configure, select **Enable** or **Disable** from the drop down menu. : *If **DHCP Server Status** is enabled, it is recommended to set the IP address manually (Static IP Address). See* Assigning the IP Address Manually
Max Lease Time	The IP address assigned by the DHCP server is valid till the configured maximum lease time. By default, the **Max Lease Time** is 86400 seconds. To configure, enter a value in the range 3600-172800 seconds.
DHCP Interface Settings The DHCP Interface Settings Table contains the following information:	
Subnet Mask	Specifies the subnet mask forwarded to the client along with the assigned IP address. The netmask configured here should be greater than or equal to the netmask configured on the interface. To configure, enter the subnet mask.
Default Gateway	Specifies the default gateway address forwarded to the client along with the assigned IP address. Default Gateway is a node that serves as an accessing point to another network. To configure, enter the *Default Gateway* address.
Primary DNS	Specifies the primary DNS (Domain Name Server) IP address forwarded to the client. To configure, enter the Primary DNS address.
Secondary DNS	Specifies the secondary DNS IP address to be sent to the client. To configure, enter the Secondary DNS address.

Default Lease Time	Specifies the least time provided by the DHCP server, to the DHCP client on that interface. By default, it is 86400 seconds. To configure, enter a value in the range 3600 to 172800 seconds. : *If the 'Default Lease Time' value is greater than 'Max Lease Time', then the DHCP server assigns the **Max Lease Time** to the DHCP client.*
Status	Specifies the status of DHCP server functionality over the interface. By default, it is disabled. To configure, select Enable or Disable from the drop down menu.
DHCP Pool Table The DHCP Pool Table contains the following information:	
Start IP Address	Specifies the Start IP Address of the pool.
End IP Address	Specifies the End IP Address of the pool.
Delete	This parameter allows you to delete the added pool entry. : • *A pool entry can be deleted but not edited.* • *To enable DHCP Server, atleast one pool must be configured.*

Click **OK** and **COMMIT**, to save the configured parameters.

5.9.1.1 Add an Entry to DHCP Pool Table

To add an entry to the DHCP Pool Table, click **Add** in the **DHCP Server** screen. The **DHCP Pool Table Add Row** screen appears.



DHCP Pool Table Add Row

Pool Interface	Bridge
Start IP Address	169.254.128.160
End IP Address	169.254.128.160
Entry Status	Enable

Note: Device IP address should not fall in the range of the DHCP Pool.

Figure 5-48 DHCP Pool - Add an Entry

Configure the following parameters:

Parameter	Description
Pool Interface	Specifies the interface type (ethernet or wireless). The device supports only Bridge mode.
Start IP Address	See DHCP Pool Table

End IP address	See DHCP Pool Table
Entry Status	Specifies the status of the pool entry. By default, it is enabled. To configure, select **Enable** or **Disable** from the drop down menu.

Click **Add**, to save the added entry.

: You can add a maximum of five pool entries per interface.

Device Management 6

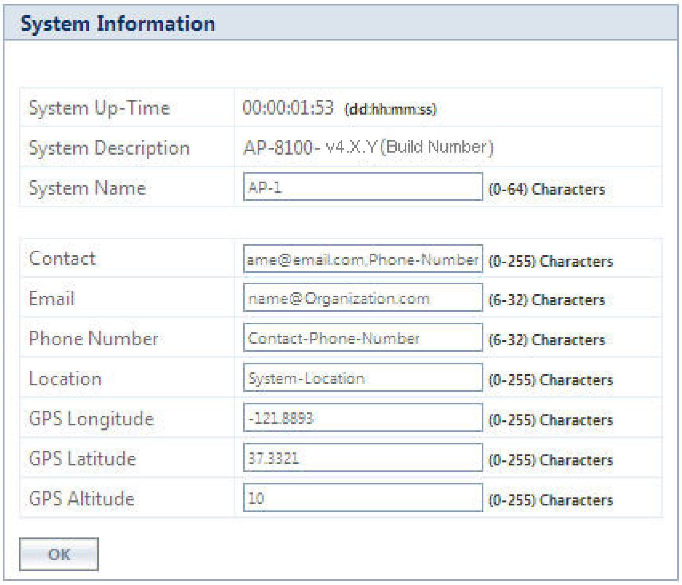
This chapter contains the following information, that helps you to manage the device by using Web Interface.

6.1 System

System tab enables you to view and configure the device information, Inventory Management information and licensed information.

6.1.1 Information

This section provides the basic system information such as System Name, System Description, Contact Details and so on. Navigate to **MANAGEMENT** > **System** > **Information**. The **System Information** screen appears.



System Information

System Up-Time	00:00:01:53 (dd:hh:mm:ss)	
System Description	AP-8100- v4.X.Y(Build Number)	
System Name	AP-1	(0-64) Characters
Contact	ame@email.com,Phone-Number	(0-255) Characters
Email	name@Organization.com	(6-32) Characters
Phone Number	Contact-Phone-Number	(6-32) Characters
Location	System-Location	(0-255) Characters
GPS Longitude	-121.8893	(0-255) Characters
GPS Latitude	37.3321	(0-255) Characters
GPS Altitude	10	(0-255) Characters

Figure 6-1 System Information

In the **System Information** screen, you can view and configure the following configurable parameters:

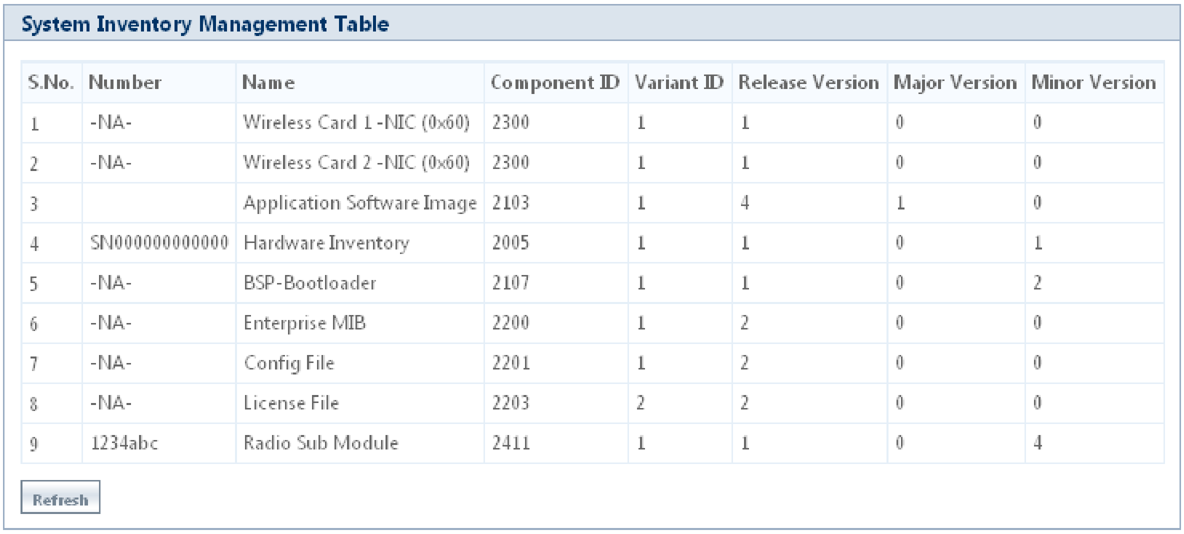
Parameter	Description
System Up-Time	Represents the operational time of the device since its last reboot. It is a read-only parameter and cannot be configured.
System Description	Specifies the system description including the device name, current version of the firmware and the current build number. System description cannot be configured.
System Name	Specifies the name assigned to the device. To configure, enter a **System Name** of maximum 64 characters.
Contact	Specifies the contact information (Email id, Phone number, Location) of the person administering the device. To configure, enter the **Contact** information of maximum 255 characters.
Email	Specifies the email address of the person administering the device. To configure, enter an email address of minimum 6 and maximum 32 characters in the **Email** box.
Phone Number	Specifies the phone number of the person administering the device. To configure, enter a phone number of minimum 6 and maximum 32 characters in the **Phone Number** box.
Location	Specifies the location where the device is installed. To configure, enter a location name of maximum 255 characters in the **Location** box.

GPS Longitude	Specifies the longitude at which the device is installed. To configure, enter a longitude value of maximum 255 characters (in the format required by your Network Management System) in the **GPS Longitude** box.
GPS Latitude	Specifies the latitude at which the device is installed. To configure, enter a latitude value of maximum 255 characters (in the format required by your Network Management System) in the **GPS Latitude** box.
GPS Altitude	Specifies the altitude at which the device is installed. To configure, enter an altitude value of maximum 255 characters (in the format required by your Network Management System) in the **GPS Altitude** box.

Click **OK**, to save the configured parameters.

6.1.2 Inventory Management

This section provides inventory information about the device. Navigate to **MANAGEMENT** > **System** > **Inventory Management**. The **System Inventory Management Table** appears.



System Inventory Management Table

S.No.	Number	Name	Component ID	Variant ID	Release Version	Major Version	Minor Version
1	-NA-	Wireless Card 1 -NIC (0x60)	2300	1	1	0	0
2	-NA-	Wireless Card 2 -NIC (0x60)	2300	1	1	0	0
3		Application Software Image	2103	1	4	1	0
4	SN000000000000	Hardware Inventory	2005	1	1	0	1
5	-NA-	BSP-Bootloader	2107	1	1	0	2
6	-NA-	Enterprise MIB	2200	1	2	0	0
7	-NA-	Config File	2201	1	2	0	0
8	-NA-	License File	2203	2	2	0	0
9	1234abc	Radio Sub Module	2411	1	1	0	4

Figure 6-2 System Inventory Management Table

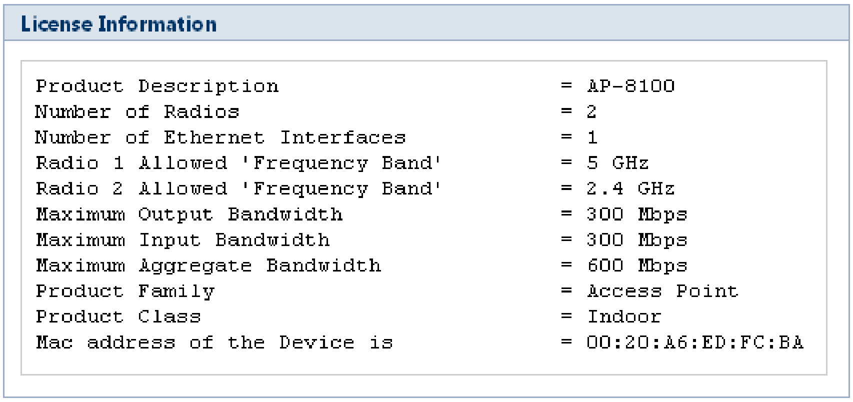
By default, the components information is auto-generated by the device. This information is standard and is used only for reference purpose. Click **Refresh**, to view the updated *System Inventory Management information*.

: Wireless Card 2 is applicable only to dual-radio device.

6.1.3 License Information

Licensing is considered to be the most important component of an enterprise-class device which typically has a feature-based pricing model. It is also required to prevent the misuse and tampering of the device by a wide-variety of audience whose motives may be intentional or accidental. Licensed Features are, by default, set by the company.

Navigate to **MANAGEMENT** > **System** > **License Information**. The **License Information** screen appears.



```
Product Description                     = AP-8100
Number of Radios                        = 2
Number of Ethernet Interfaces           = 1
Radio 1 Allowed 'Frequency Band'        = 5 GHz
Radio 2 Allowed 'Frequency Band'        = 2.4 GHz
Maximum Output Bandwidth                = 300 Mbps
Maximum Input Bandwidth                 = 300 Mbps
Maximum Aggregate Bandwidth             = 600 Mbps
Product Family                          = Access Point
Product Class                           = Indoor
Mac address of the Device is            = 00:20:A6:ED:FC:BA
```

Figure 6-3 License Information

: The above screenshot represents the licensed information of AP-8100. Licensed Features vary depending on your device.

You can view the following license information:

Parameter	Description
Product Description	Specifies the device description.
Number of Radios	Specifies the number of radios that the device is licensed to operate with.
Number of Ethernet Interfaces	Specifies the number of ethernet interfaces available on the device.
Radio 1 allowed 'Frequency Band'	Specifies the operational wireless frequency band supported by the device on Radio 1.
Radio 2 allowed 'Frequency Band'	Specifies the operational wireless frequency band supported by the device on Radio 2.
Maximum Output Bandwidth	Specifies the maximum output bandwidth limit of the device. It is represented in Mbps.
Maximum Input Bandwidth	Specifies the maximum input bandwidth limit of the device. It is represented in Mbps. *: The Input and Output Bandwidth features are referred with respect to the wireless interface. That is, input bandwidth refers to the data received on the wireless interface and output bandwidth refers to the data sent out of the wireless interface.*
Maximum Aggregate Bandwidth	Specifies the cumulative bandwidth of the device which is the sum of configured output and input.
Product Family	Specifies the product family of the device.
Product Class	Specifies the product class of the device. ORiNOCO® 802.11n Access Points are indoor devices.
Allowed Operational Modes of Radio 1	Specifies the operational modes allowed on the wireless interface (radio) 1.

Allowed Operational Modes of Radio 2	Specifies the operational modes allowed on the wireless interface (radio) 2.
MAC Address of the Device	Specifies the MAC address of the device.

6.2 File Management

The **File Management** tab enables you to upgrade the firmware and configuration files onto the device, and retrieve configuration and log files from the device through Hypertext Transfer Protocol (HTTP) and Trivial File Transfer Protocol (TFTP).

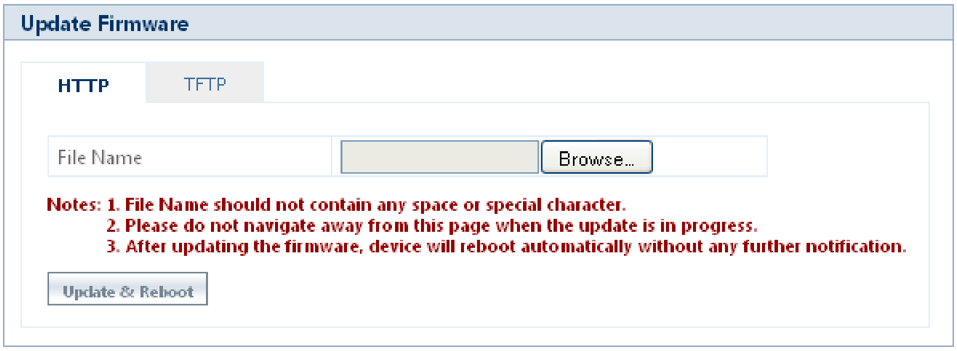
- HTTP file transfer can be performed with or without SSL enabled. HTTP file transfer with SSL requires enabling Secure Management and Secure Socket Layer. HTTP file transfer by using SSL may take extra time.
- A TFTP server must be running and configured to point in the desired directory path to copy the retrieved file.

6.2.1 Update Firmware

6.2.1.1 Update Firmware by Using HTTP

To update the firmware by using HTTP, follow the following steps:

1. Navigate to **MANAGEMENT** > **File Management** > **Update Firmware > HTTP.** The configuration screen appears:



Notes: 1. File Name should not contain any space or special character.
2. Please do not navigate away from this page when the update is in progress.
3. After updating the firmware, device will reboot automatically without any further notification.

Figure 6-4 Update Firmware by using HTTP

2. In the HTTP screen, click **Browse** to select the updated firmware file from the desired location.

   : The file name should not contain any spaces or special characters.

3. Click **Update & Reboot**, for the device to get uploaded with new firmware and reboot automatically.

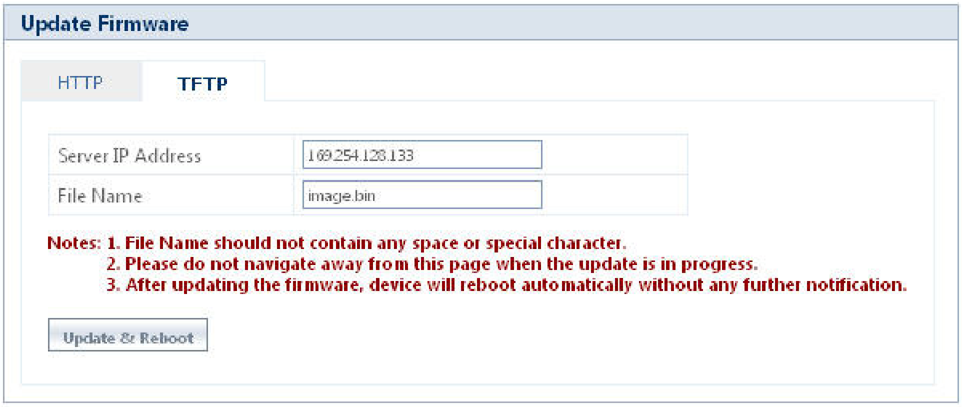
   :

   - ***Update & Reboot** is applicable only to AP-8100.*
   - *For AP-800 and AP-8000, click **Update** to load the firmware on to the device and then click **Reboot** to reboot the device.*

6.2.1.2 Update Firmware by Using TFTP

To update the firmware by using TFTP, follow the following steps:

1. Navigate to **MANAGEMENT** > **File Management** > **Update Firmware > TFTP**. The configuration screen appears:



Update Firmware

Server IP Address: 169.254.128.133

File Name: image.bin

Notes: 1. File Name should not contain any space or special character.
2. Please do not navigate away from this page when the update is in progress.
3. After updating the firmware, device will reboot automatically without any further notification.

Figure 6-5 Update Firmware by using TFTP

2. Configure the following parameters:

Parameter	Description
Server IP Address	Enter the TFTP server IP address.
File Name	Enter the name of the firmware file (including the file extension) to be downloaded onto the device.

3. Click **Update & Reboot**, for the device to get uploaded with new firmware and reboot automatically.

:

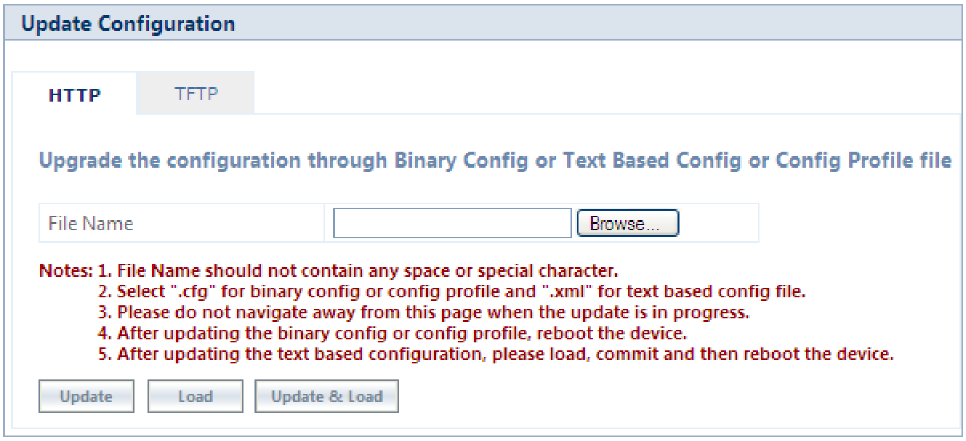
- *For AP-800 and AP-8000, click either **Update** or **Update & Reboot**, to update the device with new firmware.*
  - *If you click **Update**, then you should reboot the device after downloading the files.*
  - *If you click **Update & Reboot**, the system will automatically reboot the device after downloading the files.*
- ***Reboot** the device after upgrading it with the new firmware, else the device will continue to run with the old firmware.*
  - *For AP-8100, the device will automatically reboot after uploading the new firmware.*
- *It is recommended not to navigate away from the screen, while update is in progress.*

6.2.2 Update Configuration

6.2.2.1 Update Configuration by Using HTTP

To update the device with configuration files by using HTTP, follow the following steps:

1. Navigate to **MANAGEMENT** > **File Management** > **Update Configuration > HTTP**. The configuration screen appears.



Upgrade the configuration through Binary Config or Text Based Config or Config Profile file

Notes: 1. File Name should not contain any space or special character.
2. Select ".cfg" for binary config or config profile and ".xml" for text based config file.
3. Please do not navigate away from this page when the update is in progress.
4. After updating the binary config or config profile, reboot the device.
5. After updating the text based configuration, please load, commit and then reboot the device.

Figure 6-6 Update Configuration by using HTTP

2. In the HTTP screen, click **Browse** to locate the configuration file retrieved using Retrieve from Device option. Select
   - **'.cfg'** for binary configuration file and config profile file
   - **'.xml'** for text based configuration file

   : The file name should not contain any spaces or special characters.

3. Click **Update**, to update the device with new configuration file.
4. Click **Load**, to apply the updated changes.
5. Click **Update & Load**, to update and load the configuration file on the device in a single operation.

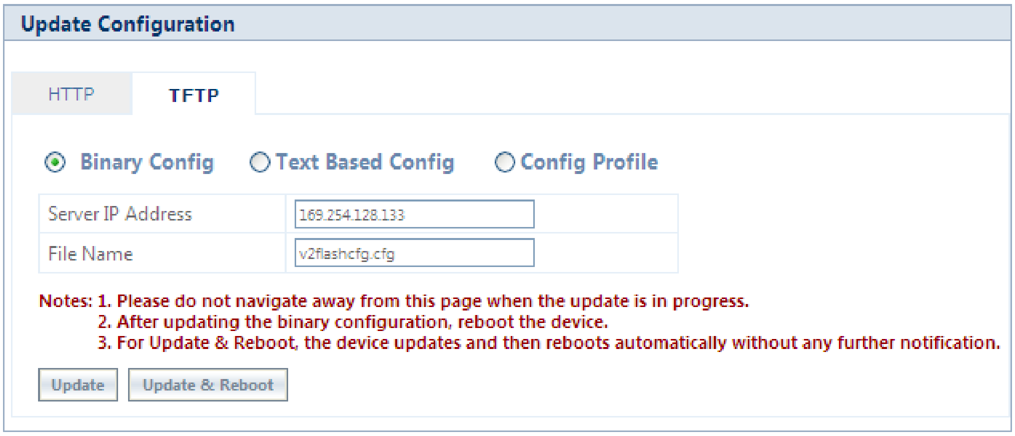
:

- ***Reboot** the device after updating it with the Binary Configuration file or the Config Profile file.*
- *For a Text Based Configuration File, either **Update** and **Load** the device or click **Update & Load**.*
- *It is recommended not to navigate away from the screen, while update is in progress.*

6.2.2.2 Update Configuration by Using TFTP

To update the device with configuration files by using TFTP, follow the following steps:

1. Navigate to **MANAGEMENT** > **File Management** > **Update Configuration > TFTP**.
2. You can update the device with two configuration files: **Binary Config** and **Text Based Config**.
3. To update the device with Binary Configuration file, select **Binary Config** radio button, the configuration screen appears.



Update Configuration

HTTP | TFTP

● Binary Config ○ Text Based Config ○ Config Profile

Server IP Address: 169.254.128.133

File Name: v2flashcfg.cfg

Notes: 1. Please do not navigate away from this page when the update is in progress.
2. After updating the binary configuration, reboot the device.
3. For Update & Reboot, the device updates and then reboots automatically without any further notification.

Figure 6-7 Update Configuration by using TFTP - Binary Config

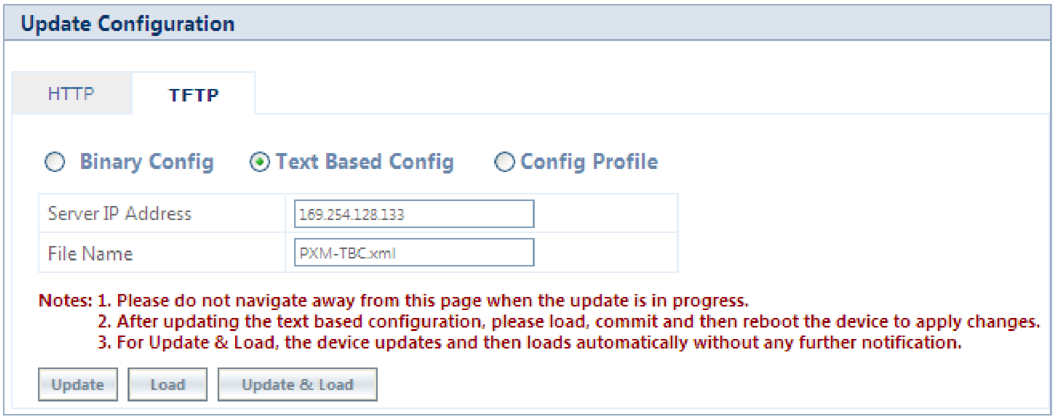
a. Configure the following parameters.

Parameter	Description
Server IP Address	Enter the TFTP server IP address.
File Name	Enter the Binary file (including the file extension) to be downloaded onto the device.

b. Click **Update**, to update the device with new configuration.

c. Click **Update & Reboot**, to update and automatically reboot the device.

4. To update the device with Text Based Configuration files, select **Text Based Config** and configuration screen appears.



Update Configuration

HTTP | TFTP

○ Binary Config ● Text Based Config ○ Config Profile

Server IP Address: 169.254.128.133

File Name: PXM-TBC.xml

Notes: 1. Please do not navigate away from this page when the update is in progress.
2. After updating the text based configuration, please load, commit and then reboot the device to apply changes.
3. For Update & Load, the device updates and then loads automatically without any further notification.

Figure 6-8 Update Configuration by using TFTP - Text Based Config

a. Configure the following parameters.

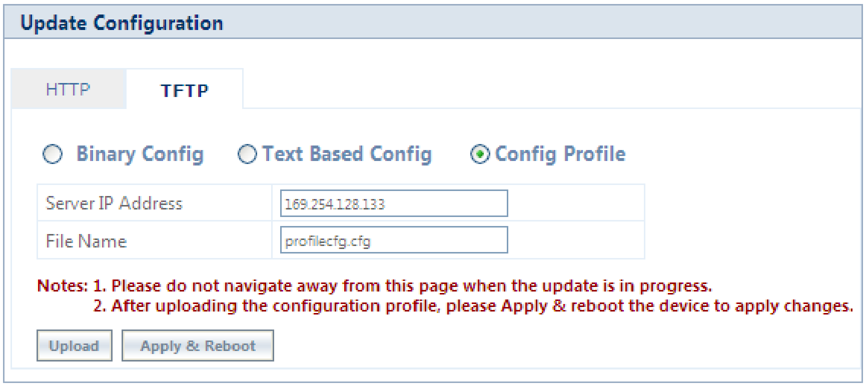
Parameter	Description
Server IP Address	Enter the TFTP server IP address.
File Name	Enter the Text based file (including the file extension) to be downloaded onto the device.

b. Click **Update**, to update the device with new configuration file.

c. Click **Load**, to apply the updated changes.

d. Click **Update & Load**, to update and load the configuration file onto the device.

5. To update the device with Config Profile files, select **Config Profile**.



○ Binary Config ○ Text Based Config ● Config Profile

Server IP Address	169.254.128.133
File Name	profilecfg.cfg

Notes: 1. Please do not navigate away from this page when the update is in progress.
2. After uploading the configuration profile, please Apply & reboot the device to apply changes.

Figure 6-9 Update Configuration by using TFTP - Config Profile

a. Configure the following parameters.

Parameter	Description
Server IP Address	Enter the TFTP server IP address.
File Name	Enter the config file name (along with the extension) to be updated onto the device.

b. Click **Upload**, to upload the device with new configuration.

c. Click **Apply & Reboot**, to upload and automatically reboot the device.

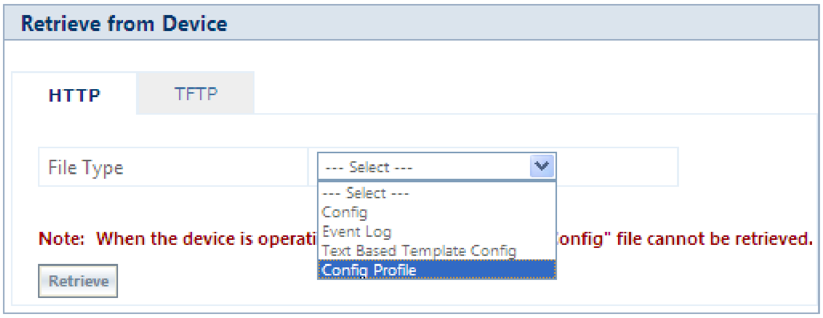
- ***Reboot*** *the device when you update the device with Binary Configuration file or Config Profile file.*
- ***Update & Load*** *the device when you update the device with Text Based Configuration file.*
- *It is recommended not to navigate away from the update screen while the update is in progress.*

6.2.3 Retrieve from Device

6.2.3.1 Retrieve from Device by using HTTP

To retrieve Configuration files, Event Logs and Text Based Templates from the device by using HTTP, follow the following steps:

1. Navigate to **MANAGEMENT** > **File Management** > **Retrieve from Device > HTTP**. The configuration screen appears.

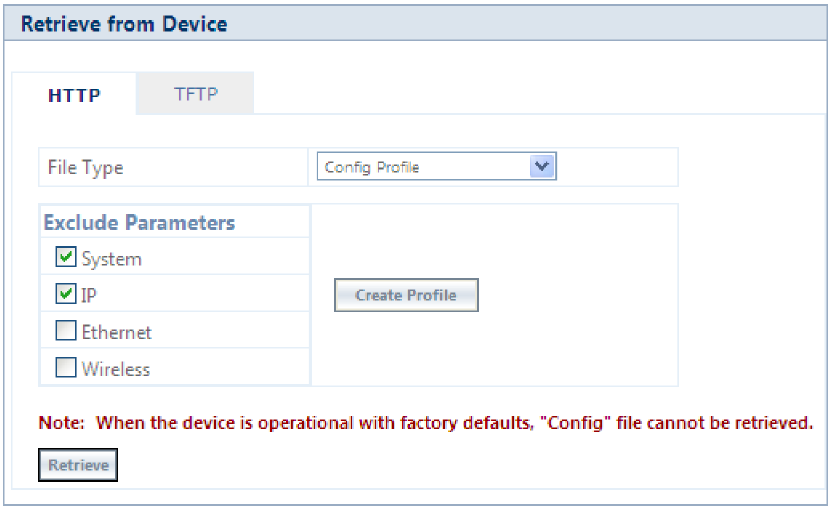


File Type

Note: When the device is operati onfig" file cannot be retrieved.

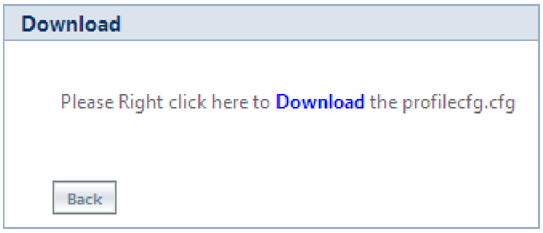
Figure 6-10 Retrieve From Device by using HTTP

2. Configure the following parameters:

Parameter	Description
File Type	Specifies the type of file that you want to retrieve from the device. To configure, select any of the following **File Type** from the drop down menu. – **Config**: Specifies the configuration files. – **Event Log**: Specifies the event logs. – **Text Based Template Config**: Specifies the text based template configuration files. – **Config Profile**: The Config Profile is used to replicate the configuration of a master device on similar devices. While replicating, you have an option to exclude unique device’s parameters such as System information, IP configuration, Ethernet configuration and Wireless configuration. By default, System Information and IP Configuration parameters are excluded. Select **Config Profile** from the **File Type.**  Retrieve from Device HTTP TFTP Create Profile Retrieve File Type: Config Profile Exclude Parameters ☑ System ☑ IP ☐ Ethernet ☐ Wireless Note: When the device is operational with factory defaults, "Config" file cannot be retrieved. **Figure 6-11 Retrieve Config Profile File via HTTP**

	Select the parameters to exclude and click **Create Profile**. Next, click **Retrieve**. See Update Configuration, to update the target device with the retrieved config profile. Once updated, the target device comes up with the configuration of the master device, by excluding the selected unique parameters. *: Config Profile is applicable only to the compatible devices.*

3. Click **Retrieve** after selecting the file type, the **Download** screen appears.



Download

Please Right click here to Download the profilecfg.cfg

Figure 6-12 Download

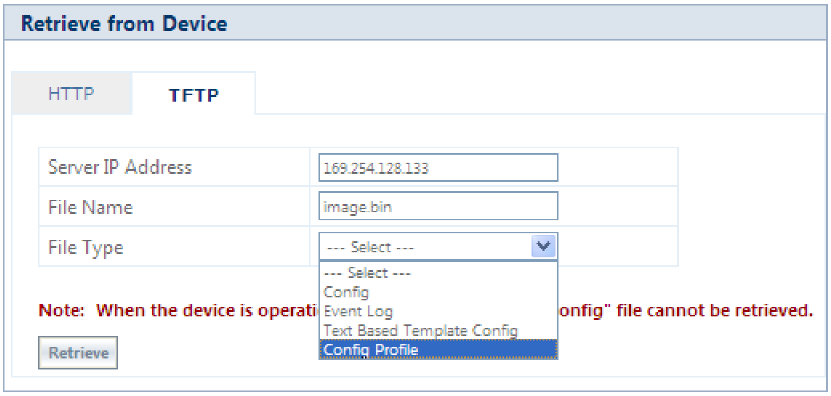
4. Right-click the **Download** link to save or retrieve the file to the desired location.

*: When the device is operational with factory default settings, there is no **Config** file present and hence it cannot be retrieved.*

6.2.3.2 Retrieve from Device by using TFTP

To retrieve Configuration files, Event Logs and Text Based Templates from the device by using TFTP, follow the following steps:

1. Navigate to **MANAGEMENT** > **File Management** > **Retrieve from Device > TFTP**. The configuration screen appears:



Retrieve from Device

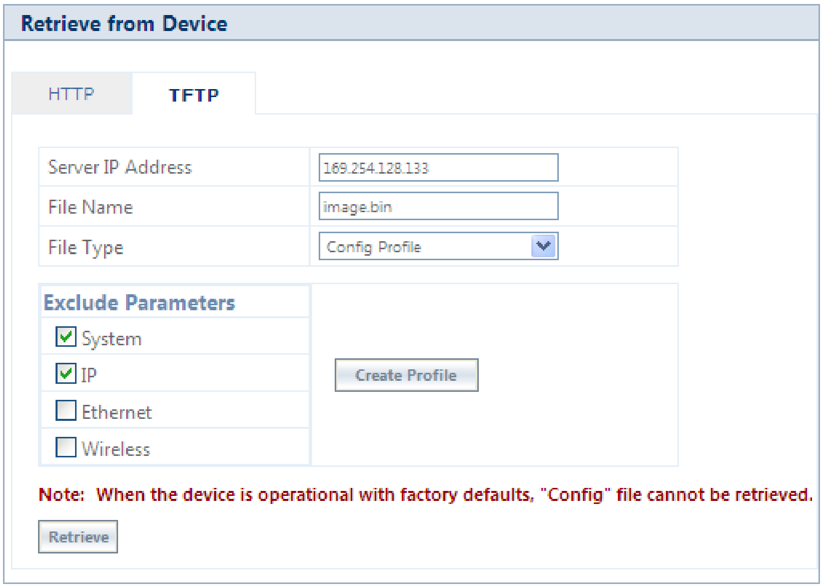
Server IP Address: 169.254.128.133
File Name: image.bin
File Type: --- Select ---

Note: When the device is operati onfig" file cannot be retrieved.

Figure 6-13 Retrieve From Device by using TFTP

2. Configure the following parameters:

Parameter	Description
Server IP Address	Enter the TFTP server IP address.
File Name	Enter the file (including the file extension) to be retrieved from the device.

File Type	Specifies the file type that you want to retrieve from the device. To configure, select any of the following **File Type** from the drop down menu. – **Config**: Specifies the configuration files of the device. – **Event Log**: Specifies the Event Logs from the device. – **Text Based Template Config**: Specifies the Text Based Template Configuration (TBC) files of the device. TBC template can be used to configure the parameters and retrieve the configuration to the device. – **Config Profile**: The Config Profile is used to replicate the configuration of a master device on similar devices. While replicating, you have an option to exclude unique device's parameters such as System information, IP configuration, Ethernet configuration and Wireless configuration. By default, System Information and IP Configuration parameters are excluded. Select **Config Profile** from the **File Type.**  Retrieve from Device HTTP | TFTP Server IP Address: 169.254.128.133 File Name: image.bin File Type: Config Profile Exclude Parameters ☑ System ☑ IP ☐ Ethernet ☐ Wireless Create Profile Note: When the device is operational with factory defaults, "Config" file cannot be retrieved. Retrieve **Figure 6-14 Retrieve Config Profile File via TFTP** Select the parameters to exclude and click **Create Profile**. Next, click **Retrieve**. See Update Configuration, to update the target device with the retrieved config profile. Once updated, the target device comes up with the configuration of the master device, by excluding the selected unique parameters. *: Config Profile is applicable only to the compatible devices.*

3. Click **Retrieve**.

*: When the device is operational with factory default settings, there is no **Config** file present and hence it cannot be retrieved.*

6.2.3.3 Text Based Configuration (TBC) File Management

Text Based Configuration (TBC) file is a simple text file that holds device template configurations. The device supports the TBC file in XML format which can be edited in any XML or text editors. You can generate the TBC file from the CLI session and manually edit the configurations and then load the edited TBC file onto the device so that the edited configurations are applied onto the device. It differs mainly from the binary configuration file in terms of manual edition of configurations. The generated TBC file is a template which has only the default and modified configurations on the live CLI session.

1. Generating TBC File

The TBC file is generated through CLI by executing generate command. While generating the TBC file from CLI, there is an option to generate it with or without all the *Management* and *Security* passwords. The management passwords include CLI/WEB/SNMP passwords. The security passwords include Network-Secret/Encryption-Key(s)/RADIUS-Shared-Secret. If included, these passwords become a part of the generated TBC file and are in a readable format. If excluded, all these passwords are not part of the generated TBC file.

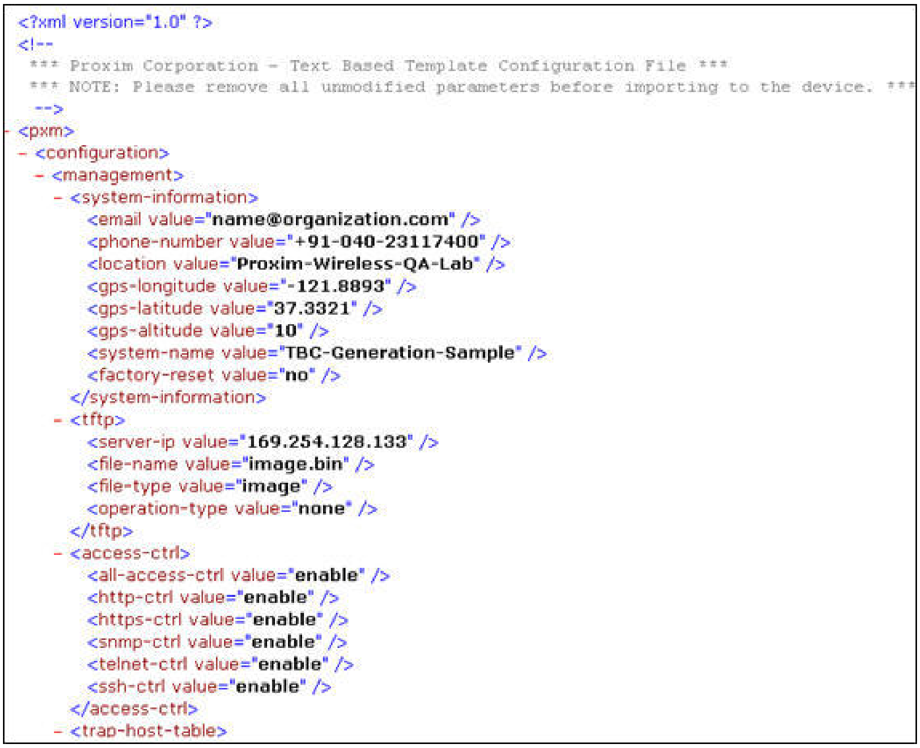
The commands used for the generation of TBC file are:

```
AP-00:7D:09>enable
AP-00:7D:09# generate ?
Possible completions:
tbc-with-pwds           Generate Text Based Template Config file with keys/passwords
tbc-without-pwds        Generate Text Based Template Config file without keys/passwords
```

The generated TBC file contains,

- Default configurations.
- Any user-added or edited configurations on current live CLI session.

The generated Text Based Template Configuration file appears as shown below:



```
<?xml version="1.0" ?>
<!--
 *** Proxim Corporation - Text Based Template Configuration File ***
 *** NOTE: Please remove all unmodified parameters before importing to the device. ***
  -->
- <pxm>
 - <configuration>
  - <management>
   - <system-information>
      <email value="name@organization.com" />
      <phone-number value="+91-040-23117400" />
      <location value="Proxim-Wireless-QA-Lab" />
      <gps-longitude value="-121.8893" />
      <gps-latitude value="37.3321" />
      <gps-altitude value="10" />
      <system-name value="TBC-Generation-Sample" />
      <factory-reset value="no" />
     </system-information>
   - <tftp>
      <server-ip value="169.254.128.133" />
      <file-name value="image.bin" />
      <file-type value="image" />
      <operation-type value="none" />
     </tftp>
   - <access-ctrl>
      <all-access-ctrl value="enable" />
      <http-ctrl value="enable" />
      <https-ctrl value="enable" />
      <snmp-ctrl value="enable" />
      <telnet-ctrl value="enable" />
      <ssh-ctrl value="enable" />
     </access-ctrl>
   - <trap-host-table>
```

Figure 6-15 TBC File in XML Format

2. **Editing the TBC File**

   The TBC file can easily be opened and edited in any standard Text-Editors like Wordpad, MS-Word, Notepad++, Standard XML Editors. Proxim recommends XML Notepad 7 editor for editing the TBC file. Do the following to edit the TBC file.

   - You can modify any value between the double quotes(“ ”) in the TBC file. It is recommended not to change the text outside the double quotes (“ ”) or XML tags in the TBC file.
   - Remove unchanged configurations from the TBC file before it loading onto the device.

3. **Loading the TBC file**

   The TBC file can be loaded onto the device by using either SNMP, Web Interface or CLI. You can either use TFTP or HTTP to load the TBC file. By using Web Interface, you can load the TBC file by navigating to **MANAGEMENT** > **File Management** > **Upgrade Configuration**. To load the TBC file, it should be generated or downloaded onto the device. While loading the TBC file onto the device, any file name is accepted. Once loaded, the TBC file name is renamed to **PXM-TBC.xml**.

   If the TBC file does not contain correct XML syntax, the file will be discarded with DOM error and no configurations will be loaded. All duplicate values entered are considered as errors while loading and syslogs will be generated accordingly. Therefore, it is recommended to delete all unchanged parameters from the TBC file during its edition. Commit is required to retain the configurations across reboots after loading the TBC file.

   : ***Commit*** *and* ***Reboot*** *the device to save the modifications done in the TBC File. To restore the device to factory default settings,* ***Reboot*** *the device.*

   Loading the TBC file is allowed only once in an active device session (that is, if TBC file is loaded, reboot is required to apply all configurations or to load another TBC file). All configurations in the TBC file are loaded to the device irrespective of their default or modified or added configurations. Loading the TBC file takes approximately 10-20 seconds depending on the number of configurations added.

:

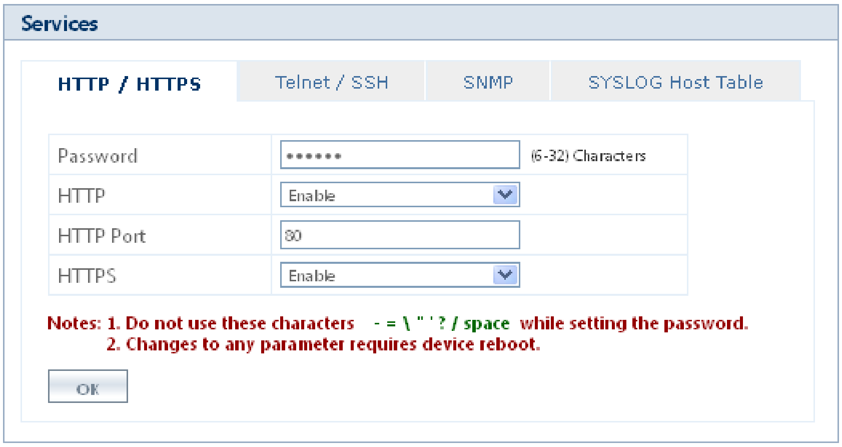
- *Remove any unmodified parameters from the TBC file, before loading it.*
- *If you get any time-out errors while loading TBC file from SNMP interface, increase the time-out value to more than 30 seconds in the MIB Browser.*

6.3 Services

The **Services** feature allows you to configure the management interface (HTTP/HTTPS, Telnet/SSH and SNMP) and SYSLOG host table parameters that prevent from unauthorized access to the device.

6.3.1 HTTP/HTTPS

Navigate to **MANAGEMENT** > **Services > HTTP/HTTPS**. The configuration screen appears.



Services

Password	••••••	(6-32) Characters
HTTP	Enable	
HTTP Port	80	
HTTPS	Enable	

Notes: 1. Do not use these characters - = \ " ' ? / space while setting the password.
2. Changes to any parameter requires device reboot.

Figure 6-16 HTTP/HTTPS

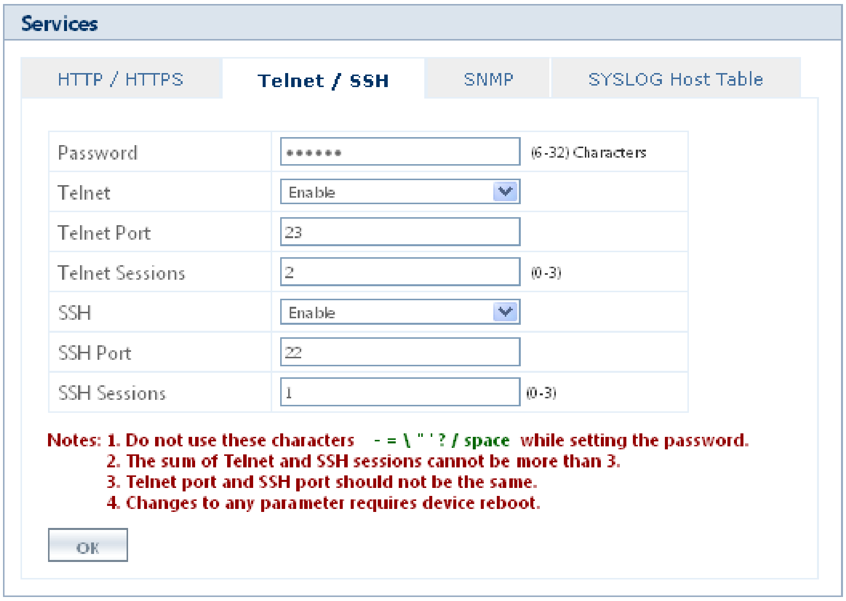
Configure the following parameters in the HTTP/HTTPS screen:

Parameter	Description
Password	Specifies the password that is required to log on to the web interface. By default, the password is set to **public**. To configure, enter a new alphanumeric password with a minimum of 6 and maximum of 32 characters in the **Password** box. *: Special characters like* **- = \ " ' ? /** ***space*** *are not allowed in the password.*
HTTP	Specifies the **HTTP** status. HTTP allows the user to access the device through a web interface. To configure, Select **Enable** or **Disable** from the drop down menu.
HTTP Port	Specifies the number of the port on the HTTP interface. By default, it is 80. To configure, enter a new **HTTP Port**.
HTTPS	Specifies the **HTTPS** status. HTTPS allows the user to access the device through a web interface. To configure, select **Enable** or **Disable** from the drop down menu. The password configuration for HTTPS is same as configured for HTTP.

Click **OK** and then **Reboot** the device for the changes to take effect.

6.3.2 Telnet/SSH

In the Web Interface, navigate to **MANAGEMENT** > **Services > Telnet/SSH**. The configuration screen appears.



Password	••••••	(6-32) Characters
Telnet	Enable	
Telnet Port	23	
Telnet Sessions	2	(0-3)
SSH	Enable	
SSH Port	22	
SSH Sessions	1	(0-3)

Notes: 1. Do not use these characters - = \ " ' ? / space while setting the password.
2. The sum of Telnet and SSH sessions cannot be more than 3.
3. Telnet port and SSH port should not be the same.
4. Changes to any parameter requires device reboot.

Figure 6-17 Telnet/SSH

Configure the following parameters in the Telnet/SSH screen:

Parameter	Description
Password	Specifies the password that is required to log on to the CLI. By default, the password is set to **public**. To configure, enter a new alphanumeric password with a minimum of 6 and maximum of 32 characters in the **Password** box. *: Special characters like* ***- = \ " ' ? / space*** *are not allowed in the password.*
Telnet	Select **Enable** or **Disable** from the **Telnet** drop down menu. If enabled, it allows the user to access the device via telnet interface.
Telnet Port	Specifies the number of the port on the telnet interface. By default, the **Telnet Port** number is 23. To configure, enter a new port.
Telnet Sessions	Specifies the number of Telnet sessions which controls the number of active telnet connections. By default, the number of **Telnet Sessions** are 2. To configure, enter a value ranging from 0 to 3.
SSH	Select **Enable** or **Disable** from the **SSH** drop down menu. If enabled, it allows the user to access the device via SSH Interface.

SSH Port	Specifies the number of the port on the SSH interface. By default, the **SSH Port** number is 22. To configure, enter a new port.
SSH Sessions	Specifies the number of SSH sessions which controls the number of active SSH connections. By default, the number of **SSH Sessions** allowed is 1. To configure, enter a value ranging from 0 to 3.

Click **OK** and then **Reboot** the device for the changes to take effect.

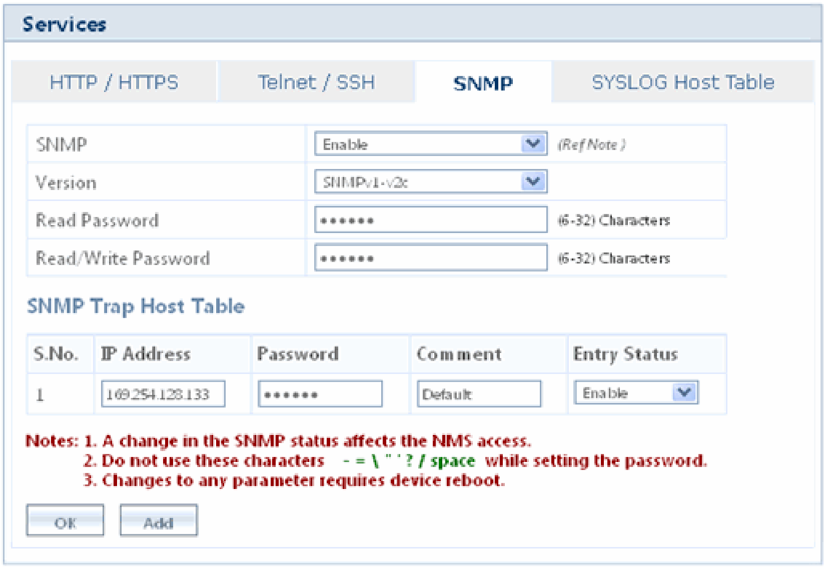
:

- *The sum of Telnet and SSH sessions cannot be more than 3.*
- *The Telnet and SSH Port should not be same.*

6.3.3 SNMP

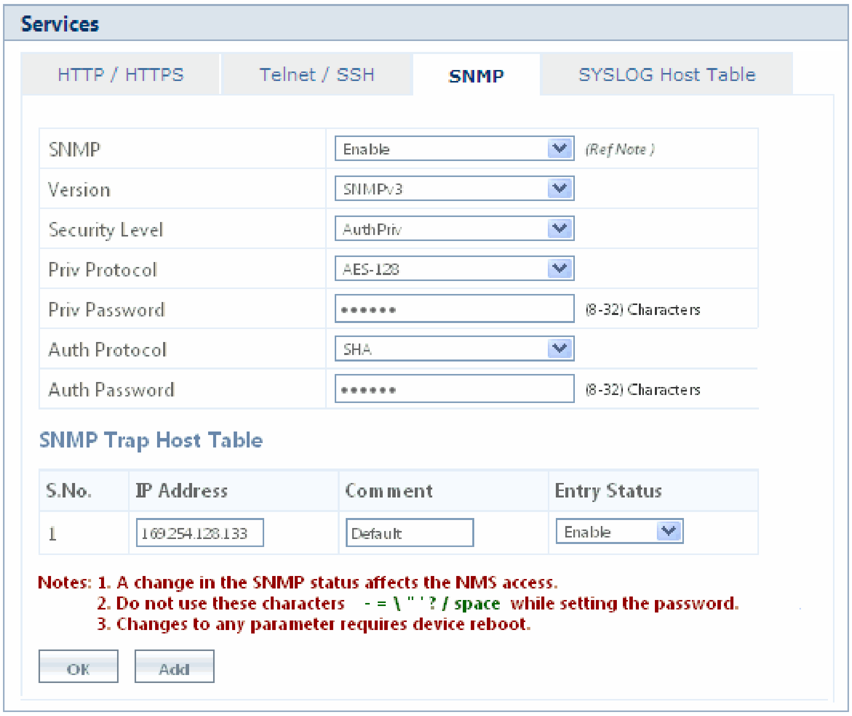
Navigate to **MANAGEMENT** > **Services > SNMP** and configure the following parameters:

Parameter	Description
SNMP	Select **Enable** or **Disable** from the drop down menu. – If enabled, it allows the user to access the device through SNMP Interface. *: Any change in the SNMP access will affect the NMS access.*

<table>
<tr>
<td>Version</td>
<td>
Specifies the SNMP versions v1-v2c or v3. By default, the SNMP version is v2c.
• If you select the SNMP version as <b>SNMP v1-v2c</b>, the following configuration screen appears:

Services
HTTP / HTTPS
Telnet / SSH
SNMP
SYSLOG Host Table
SNMP Trap Host Table
OK
Add

SNMP: Enable (Ref Note)
Version: SNMPv1-v2c
Read Password: •••••• (6-32) Characters
Read/Write Password: •••••• (6-32) Characters
S.No. 1 | IP Address 169.254.128.133 | Password •••••• | Comment Default | Entry Status Enable
Notes: 1. A change in the SNMP status affects the NMS access.
2. Do not use these characters - = \ " ' ? / space while setting the password.
3. Changes to any parameter requires device reboot.
<b>Figure 6-18 SNMP Version - SNMPv1-v2c</b>
Configure the following parameters:
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Read Password</td><td>Specifies the password that provides read access to device by using SNMP interface.
The default password is “<b>public</b>”. To configure, enter an alphanumeric password with a minimum of 6 and maximum of 32 characters in the <b>Read Password</b> box.</td></tr>
<tr><td>Read/Write Password</td><td>Specifies the password that provides read/write access to device by using SNMP interface.
The default password is “<b>public</b>. To configure, enter an alphanumeric password with a minimum of 6 and maximum of 32 characters in the <b>Read/Write Password</b> box.</td></tr>
</table>
</td>
</tr>
</table>

- If you select the SNMP version as **SNMP v3**, then following configuration screen appears:



Services

SNMP	Enable	(Ref Note)
Version	SNMPv3	
Security Level	AuthPriv	
Priv Protocol	AES-128	
Priv Password	••••••	(8-32) Characters
Auth Protocol	SHA	
Auth Password	••••••	(8-32) Characters

SNMP Trap Host Table

S.No.	IP Address	Comment	Entry Status
1	169.254.128.133	Default	Enable

Notes: 1. A change in the SNMP status affects the NMS access.
2. Do not use these characters - = \ " ' ? / space while setting the password.
3. Changes to any parameter requires device reboot.

Figure 6-19 SNMP Version - SNMPv3

Configure the following parameters:

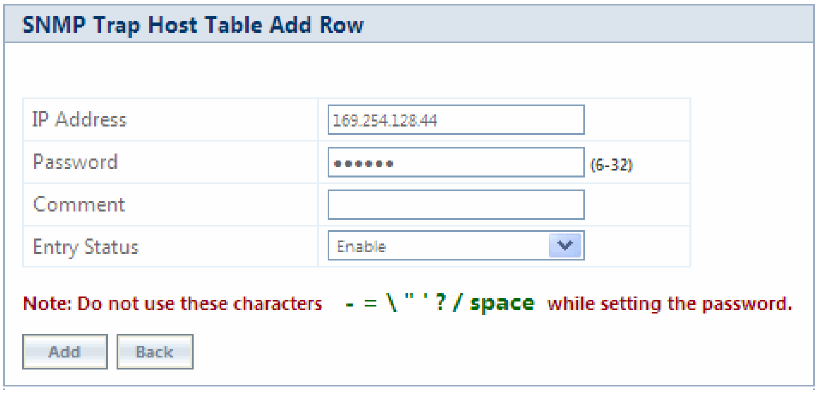
Parameter	Description
Security Level	Specifies the security level of the device. AP device supports the following security levels: – **None**: For no authentication – **AuthNoPriv**: For Extensible Authentication – **AuthPriv**: For both Authentication and Privacy (Encryption) By default, it is **AuthPriv**. To configure, select the security level from the drop down menu.
Priv Protocol	Specifies the type of privacy (or encryption) protocol. By default, **Priv Protocol** is AES-128. To configure, select the encryption standard as either AES-128 (Advanced Encryption Standard) or DES (Data Encryption Standard) from the drop down menu. : ***Priv Protocol*** *is applicable only when the security level is set to* ***AuthPriv****.*

<table>
<tr><td>Version</td><td>
<table>
<tr><td>Priv Password</td><td>Specifies the pass key for privacy protocol selected.
The default password is public123. To configure, enter a new password ranging from 8 to 32 characters.
<i>: <b>Priv Password</b> is applicable only when the security level is set to <b>AuthPriv</b>.</i></td></tr>
<tr><td>Auth Protocol</td><td>Specifies the type of Authentication protocol.
By default, it is SHA. To configure, select the encryption standard as either SHA (Secure Hash Algorithm) or MD5 (Message-Digest algorithm).</td></tr>
<tr><td>Auth Password</td><td>Specifies the pass key for privacy protocol selected.
The default password is public123. To configure, enter a new password ranging from 8 to 32 characters.</td></tr>
</table>
Click <b>OK</b> and <b>Reboot</b> the device, to save the configured parameters.</td></tr>
<tr><td colspan="2"><b>SNMP Trap Host Table</b>
The SNMP Trap Host Table contains the following information:</td></tr>
<tr><td>IP Address</td><td>Specifies the IP address to which SNMP traps will be delivered.</td></tr>
<tr><td>Password</td><td>Specifies the password set to access the SNMP Trap Host Table entry.
<i>: Applicable only to SNMP version v1-v2c.</i></td></tr>
<tr><td>Comment</td><td>Specifies the user-comment on the SNMP Trap Host Table entry.
To configure, enter any comment for the table entry.</td></tr>
<tr><td>Entry Status</td><td>Specifies the entry status set for each table entry.
To configure, select either <b>Enable</b>, <b>Disable</b> or <b>Delete</b>.
– If enabled, it allows the device to send SNMP traps to the specified IP address.
– Select <b>Delete</b>, if you want to delete any table entry from the SNMP Trap Host Table.</td></tr>
</table>

Click **OK** and **Reboot** the device, if you have changed the values in the SNMP Trap Host Table.

6.3.3.1 Add a new Entry to the SNMP Trap Host Table

To add new entries to the SNMP Trap Host Table, click **Add.** The **SNMP Trap Host Table Add Row** screen appears.



SNMP Trap Host Table Add Row

IP Address	169.254.128.44
Password	•••••• (6-32)
Comment	
Entry Status	Enable

Note: Do not use these characters - = \ " ' ? / space while setting the password.

Figure 6-20 SNMP Trap Host Table Add Row

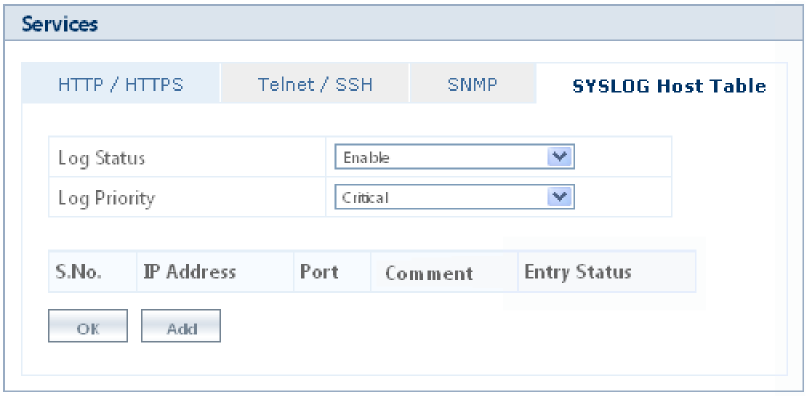
Configure the following parameters:

Parameter	Description
IP Address	Specifies the IP address to which SNMP traps will be delivered. To configure, enter the IP address in the **IP Address** box.
Password	To access SNMP traps, enter password in the **Password** box. A minimum of 6 and a maximum of 32 characters are allowed. *: Applicable only to SNMP version v1-v2c.*
Comment	Enter any comments in the **Comment** box.
Entry Status	Select the **Entry Status** as either **Enable** or **Disable** from the drop down menu.

Click **Add**, to add an entry to the SNMP Trap Host Table.

6.3.4 SYSLOG Host Table

System log messages are generated by the device by sending requests at various instances to the system log server. The system log messages are lost on device reboot. Navigate to **MANAGEMENT** > **Services > SYSLOG Host Table**, the configuration screen appears.



Services

Log Status	Enable
Log Priority	Critical

S.No.	IP Address	Port	Comment	Entry Status

Figure 6-21 SYSLOG Host Table

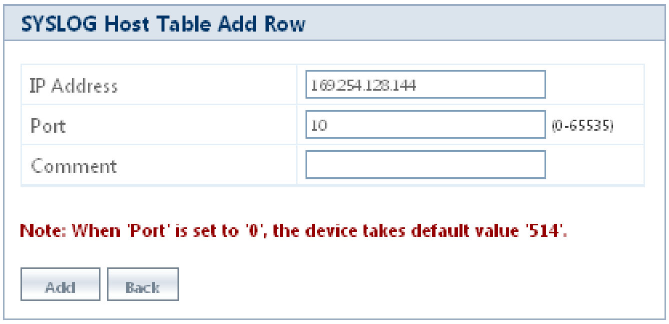
Configure the following parameters:

Parameter	Description
Log Status	Specifies the status of the system log. To configure, select either **Enable** or **Disable** from the drop down menu. If enabled, it allows the device to generate log messages.
Log Priority	Specifies the priority assigned to the log. The available log priorities are: – Emergency – Alert – Critical – Error – Warning – Notice – Info – Debug Please note that the priorities are listed in the order of their severity, where *Emergency* takes the highest severity and *Debug* the lowest. To configure, select the **Log Priority** from the drop down menu.
SYSLOG Host Table Entries The **S**YSLOG Host Entries Table contains the following information:	
IP Address	Specifies the IP address of the SYSLOG server.
Port	Specifies the host port number. The default port is 514. ✎ *: The user must configure the correct port number on which the SYSLOG server is running for the Host Port parameter. Choice of port number must be in line with the standards for port number assignments defined by Internet Assigned Numbers Authority (IANA).*
Host Comment	Specifies the user-comment on the SYSLOG Host Table entry. To configure, enter any comment for the table entry.
Entry Status	Specifies the entry status set for each table entry. To configure, select either **Enable**, **Disable** or **Delete**. – If enabled, it allows the device to send SysLog messages to the specified IP address of the SYSLOG server. – Select **Delete**, if you want to delete any table entry from the SYSLOG Host Table.

Click **OK** and **COMMIT**, to save the configured parameters.

6.3.4.1 Add a new Entry to the SYSLOG Host Table

To add new entries to the SYSLOG Host Table, click **Add.** The **SYSLOG Host Table Add Row** screen appears.



SYSLOG Host Table Add Row

IP Address	169.254.128.144	
Port	10	(0-65535)
Comment		

Note: When 'Port' is set to '0', the device takes default value '514'.

Figure 6-22 SYSLOG Host Table Add Row

Configure the following parameters:

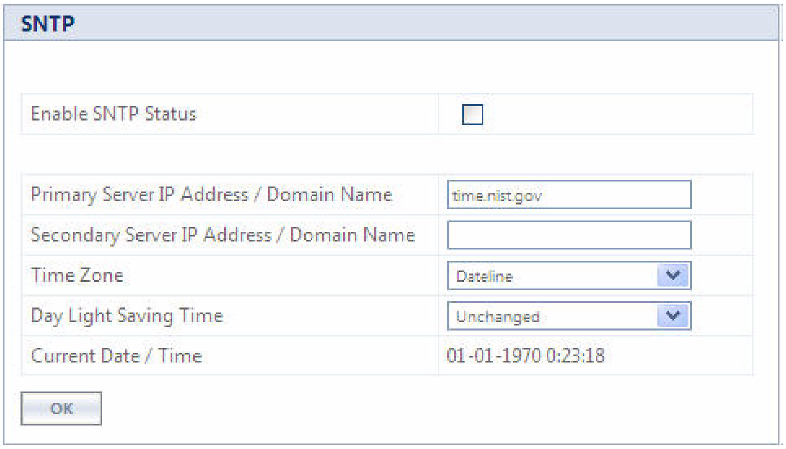
Parameter	Description
IP Address	Enter the IP address of the SYSLOG server in the **IP Address** box.
Host Port	Enter a Host Port in the range of 0 to 65535, in the **Host Port** box.
Comment	Enter any comments in the **Comment** box.

Click **Add**, to add an entry in the SYSLOG Host Table.

6.4 Simple Network Time Protocol (SNTP)

SNTP allows you to synchronize the date and time of the device with the configured time servers. When this feature is enabled, the device will attempt to retrieve the time of day information from the configured time servers (primary or secondary) and, if successful, will update the relevant time objects in the device.

Navigate to **MANAGEMENT > SNTP**. The **SNTP** screen appears.



SNTP

Enable SNTP Status	□

Primary Server IP Address / Domain Name	time.nist.gov
Secondary Server IP Address / Domain Name	
Time Zone	Dateline
Day Light Saving Time	Unchanged
Current Date / Time	01-01-1970 0:23:18

Figure 6-23 SNTP

You can view and configure the following configurable parameters:

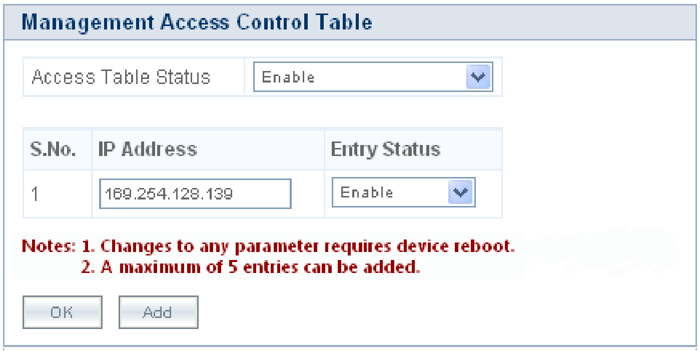
Parameter	Description
Enable SNTP Status	Specifies the status of the SNTP feature on the device. Select **Enable SNTP Status** checkbox to synchronize the date and time of the device with the SNTP time server.
Primary Server IP Address / Domain Name	Specifies the host name or the IP address of the primary SNTP server. To configure, enter the **Primary Server IP Address/Domain Name**.
Secondary Server IP Address / Domain Name	Specifies the host name or the IP address of the secondary SNTP server. To configure, enter the **Secondary Server IP Address/Domain Name**.
Time Zone	Specifies the time zone set for the SNTP. To configure, select the desired time zone from the drop down menu
Day Light Saving Time	Specifies the number of hours adjusted for the Daylight Saving Time. To configure, select the desired **Day Light Saving Time** from the drop down menu.
Current Date/Time	Specifies the system current date and time. It is read-only parameter and cannot be configured. – If SNTP is not enabled, the current date and time are automatically generated by the local system. – If SNTP is enabled, it displays the time, that the device has obtained from the SNTP server.

Click **OK** and **COMMIT**, to save the configured parameters.

*: Configure the parameters **Primary Server IP Address / Domain Name**, **Secondary Server IP Address / Domain Name** and **Time zone and Day Light Saving Time**, only when the SNTP status is enabled.*

6.5 Access Control

The Management Access Control feature allows you to manage the device from the specified host. Navigate to **MANAGEMENT > Access Control**. The **Management Access Control Table** screen appears.



Management Access Control Table

Access Table Status: Enable

S.No.	IP Address	Entry Status
1	169.254.128.139	Enable

Notes: 1. Changes to any parameter requires device reboot.
2. A maximum of 5 entries can be added.

Figure 6-24 Management Access Control Table

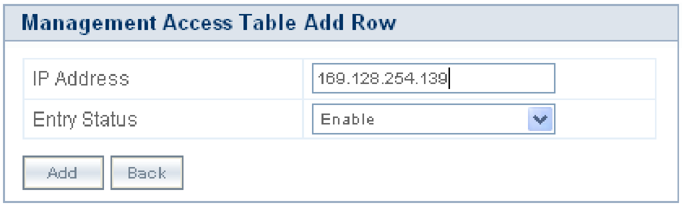
Configure the following parameters:

Parameter	Description
Access Table Status	Specifies the status of the Access Control on the AP device. By default, the Management Access Control is disabled on the device. To enable it, select **Enable** from the drop down menu.
IP Address	Specifies the IP address of the machine that would manage the device.
Entry Status	Specifies the status of the added entry. To configure, select Enable or Disable from the drop down menu.

Click **OK** and **Reboot** the device, if you have changed the values in the Access Control Table.

6.5.1 Add an Entry to the Access Control Table

To add new entries to the Access Control Table, click **Add** in the **Management Access Control Table** screen**.** The **Management Access Table Add Row** screen appears:



Management Access Table Add Row

IP Address: 169.128.254.139

Entry Status: Enable

Figure 6-25 Management Access Control - Add Row

Configure the following parameters:

Parameter	Description
IP Address	Specifies the IP address of the system that manages the AP device. To configure, enter the IP address in the **IP Address** box.
Entry Status	By default, the entry status is enabled. To configure, select the status form the drop down menu.

Click **Add**, to add an entry.

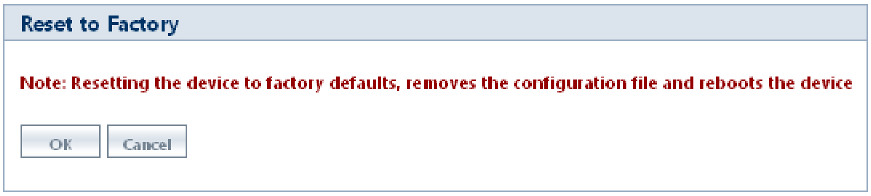
:

- *A maximum of five system IP addresses can be added to manage the AP device.*
- *You can add new entries only when the Access Table status is enabled.*

6.6 Reset to Factory

The ‘Reset to Factory’ feature allows you to reset the device to its factory default state. When this operation is performed, the device will reboot automatically and operates with the factory default configuration.

To reset the device to its factory defaults, navigate to **MANAGEMENT** > **Reset To Factory**. The **Factory Reset** screen appears.



Reset to Factory

Note: Resetting the device to factory defaults, removes the configuration file and reboots the device

Figure 6-26 Reset to Factory

Click **OK** for the device to restart with the default factory configuration.

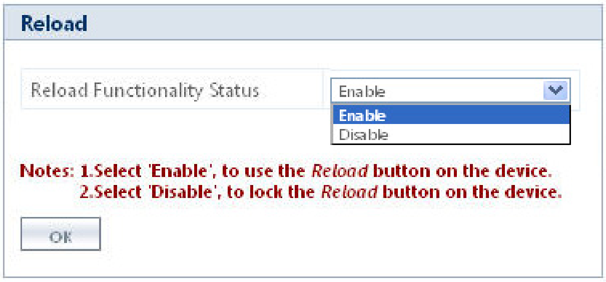
6.7 Reload

: Applicable only to AP-8100.

By default, the reload button on the device enables you to perform reload procedures when you cannot access the AP device. For details on reload procedures, refer Hard Reset to Factory Defaults (Reload) and Forced Reload. You can lock the reload button on the device, to avoid tampering with it.

To enable or disable the reload button functionality on the device, do the following:

- Navigate to **MANAGEMENT** > **Reload**, the **Reload** configuration screen appears.



Reload

Reload Functionality Status: Enable

Notes: 1.Select 'Enable', to use the *Reload* button on the device.
2.Select 'Disable', to lock the *Reload* button on the device.

Figure 6-27 Reload

- By default, the **Reload Functionality Status** is enabled. To configure, select **Enable** or **Disable** from the drop down menu.
  - — **Enable**: To use the reload button on the device and perform reload procedures.
  - — **Disable**: To lock and avoid tampering with the reload button on the device.
- Click **OK**.

❗: In case, the *'Reload Functionality Status'* is disabled and user cannot access the AP device, then follow the following steps to recover the device.

- Step-1: Unplug the power cable.
- Step-2: Press and hold the reload button on the device.
- Step-3: Plug in the power cable, with the reload button still pressed.
- Step-4: Once the power cable is plugged in, hold the reload button for:
  - 5 seconds to delete the configuration file. To load new configuration file onto the device, refer Update Configuration.
  - 12 seconds to delete the configuration file and firmware. To load new firmware onto the device, refer Update Firmware.

Device Monitoring 7

This chapter contains the step-by-step procedure to monitor the following features of the device, by using Web Interface:

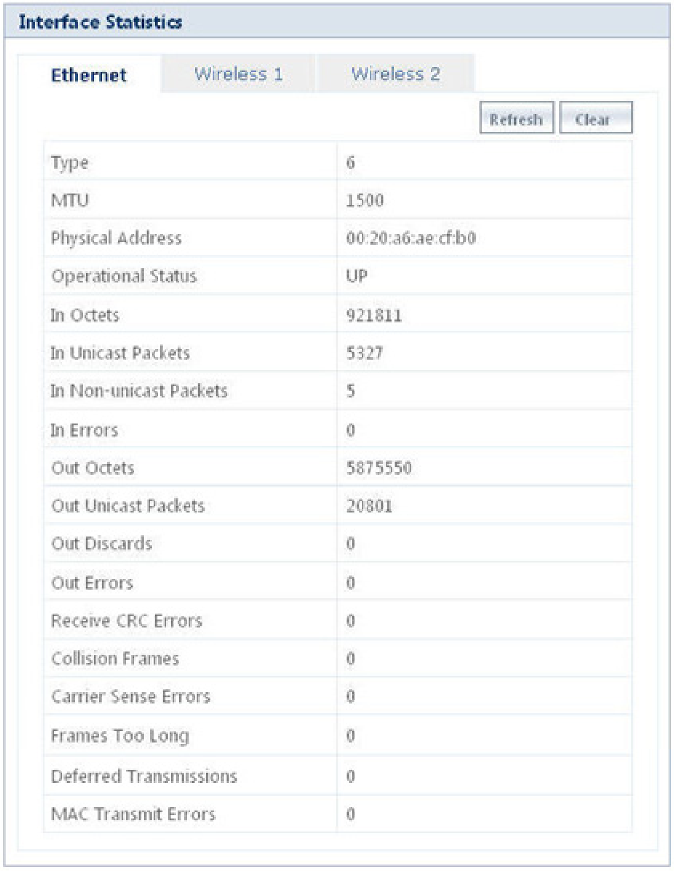
: All the interface (radio) 2 parameters discussed in this chapter are applicable only to a dual-radio device.

7.1 Interface Statistics

'Interface Statistics' allow you to monitor the status and performance of the ethernet and wireless interfaces of the device. To view interface statistics, navigate to **MONITOR > Interface Statistics**.

Ethernet Interface Statistics

To view the ethernet interface statistics, click **Ethernet** tab in the **Interface Statistics** screen. The ethernet interface statistics screen appears.



Type	6
MTU	1500
Physical Address	00:20:a6:ae:cf:b0
Operational Status	UP
In Octets	921811
In Unicast Packets	5327
In Non-unicast Packets	5
In Errors	0
Out Octets	5875550
Out Unicast Packets	20801
Out Discards	0
Out Errors	0
Receive CRC Errors	0
Collision Frames	0
Carrier Sense Errors	0
Frames Too Long	0
Deferred Transmissions	0
MAC Transmit Errors	0

Figure 7-1 Ethernet Interface Statistics

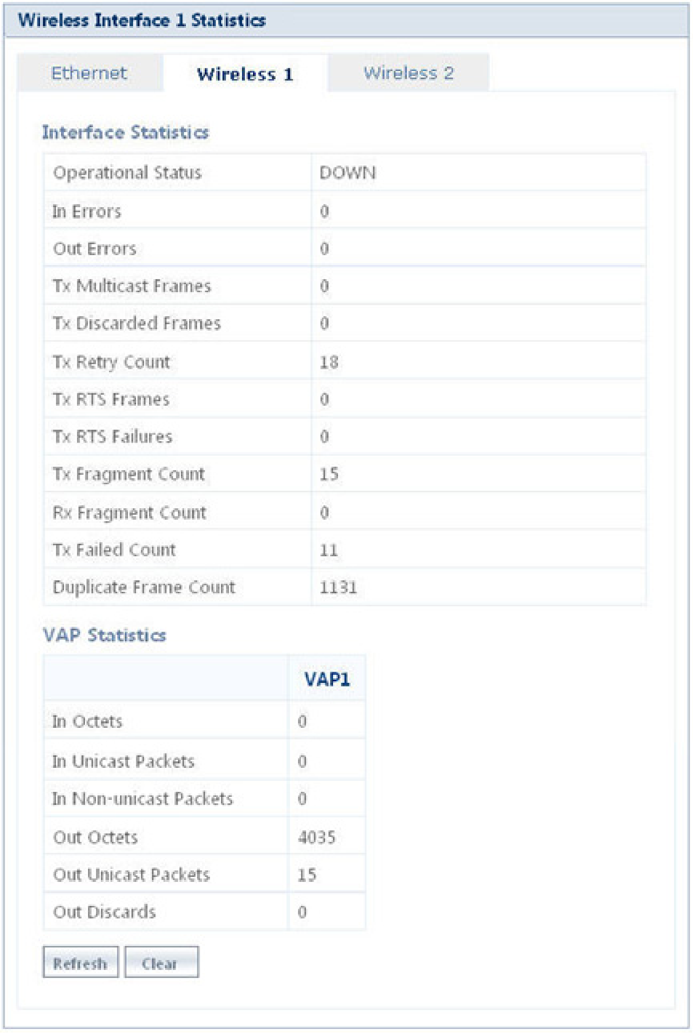
The Ethernet **Interface Statistics** screen contains the following information.

Ethernet Interface Statistics	
Parameter	**Description**
Type	Specifies the type of interface.
MTU	Specifies the largest size of the data packet transmitted on the bridge.
Physical Address	Specifies the MAC address of the interface
Operational Status	Specifies the current operational status of the ethernet interface.
In Octets	Specifies the total number of octets received on the interface.
In Unicast Packets	Specifies the number of unicast sub-network packets delivered to the higher level protocol.
In Non-Unicast Packets	Specifies the number of non-unicast sub-network packets delivered to the higher level protocol.
In Errors	Specifies the number of inbound packets with errors and that are restricted from being delivered.
Out Octets	Specifies the total number of octets transmitted out of the interface.

Out Unicast Packets	Specifies the total number of packets that are requested by the higher level protocol and transmitted to the non-unicast address.
Out Discards	Specifies the number of error-free outbound packets that are discarded to free up the buffer space.
Out Errors	Specifies the number of outbound error packets that are not allowed to transmit.
Receive CRC Errors	Specifies the total number of CRC errors occurred if the data transmitted is corrupted.
Collision Frames	Specifies the total number of collision frames.
Career Sense Errors	Specifies the total number of frames that are not transmitted.
Frames Too Long	Specifies the total number of frames, which are too long than the configured packet size.
Deferred Transmissions	Specifies the total number of times the interface fails to transmit a frame.
MAC Transmit Errors	Specifies the total number of frames that are not transmitted due to the MAC sub-layer transmit error.

Wireless Interface Statistics

To view wireless interface statistics, click the **Wireless1** or **Wireless2** tab in the **Interface Statistics** screen, the **Wireless Interface Statistics** screen appears.



Wireless Interface 1 Statistics

Interface Statistics

Operational Status	DOWN
In Errors	0
Out Errors	0
Tx Multicast Frames	0
Tx Discarded Frames	0
Tx Retry Count	18
Tx RTS Frames	0
Tx RTS Failures	0
Tx Fragment Count	15
Rx Fragment Count	0
Tx Failed Count	11
Duplicate Frame Count	1131

VAP Statistics

	VAP1
In Octets	0
In Unicast Packets	0
In Non-unicast Packets	0
Out Octets	4035
Out Unicast Packets	15
Out Discards	0

Figure 7-2 Wireless Interface Statistics

The **Wireless Interface Statistics** screen contains the following information.

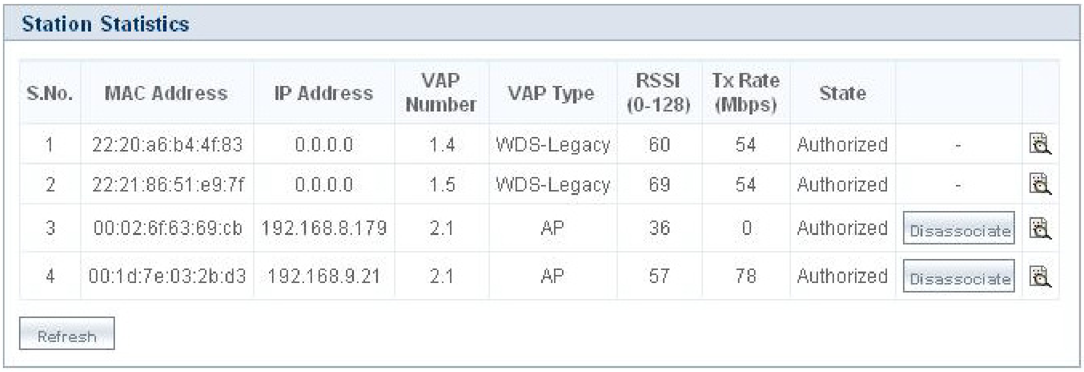
Wireless 1/Wireless 2 Interface Statistics	
Parameter	**Description**
Operational Status	Specifies the current operational status of the interface.
In Errors	Specifies the number of inbound packets with errors and that are restricted from being delivered. In Errors on the wireless interface include CRC errors.
Out Errors	Specifies the number of outbound error packets that are not allowed to transmit.
Tx Multicast Frames	Specifies the total number of multicast frames transmitted
Tx Discarded Frames	Specifies the total number of multicast frames discarded.
Tx Retry Count	Specifies the total number of frames delivered with one or more retransmissions.
Tx RTS Frames	Specifies the total number of requests for the RTS frames transmission.

Tx RTS Failures	Specifies the total number of RTS frames requests that receive no response.
Tx Fragment Count	Specifies the total number of fragments that are transmitted and acknowledged.
Rx Fragment Count	Specifies the total number of fragments that are transmitted and received successfully.
Tx Failed Count	Specifies the total number of undelivered frames.
Duplicate Frame Count	Specifies the total number of frames transmitted successfully, in a duplicate fragment.
VAP Statistics	
In Octets	Specifies the total number of octets received on the interface.
In Unicast Packets	Specifies the number of unicast sub-network packets delivered to the higher level protocol.
In Non - Unicast Packets	Specifies the number of non-unicast sub-network packets delivered to the higher level protocol.
Out Octets	Specifies the total number of octets transmitted out of the interface.
Out Unicast Packets	Specifies the total number of packets requested by the higher level protocol and then transmitted to the non-unicast address.
Out Discards	Specifies the number of error-free outbound packets that are discarded to free up the buffer space.

Click **Refresh** to view the updated Interface statistics (Ethernet/Wireless 1/Wireless 2) and click **Clear** to clear the interface statistics.

7.2 Station Statistics

'Station Statistics' allow you to monitor the wireless clients associated with the device. To view the station statistics, navigate to **MONITOR > Station Statistics**. The **Station Statistics** screen appears.



Station Statistics

S.No.	MAC Address	IP Address	VAP Number	VAP Type	RSSI (0-128)	Tx Rate (Mbps)	State		
1	22:20:a6:b4:4f:83	0.0.0.0	1.4	WDS-Legacy	60	54	Authorized	-	
2	22:21:86:51:e9:7f	0.0.0.0	1.5	WDS-Legacy	69	54	Authorized	-	
3	00:02:6f:63:69:cb	192.168.8.179	2.1	AP	36	0	Authorized	Disassociate	
4	00:1d:7e:03:2b:d3	192.168.9.21	2.1	AP	57	78	Authorized	Disassociate	

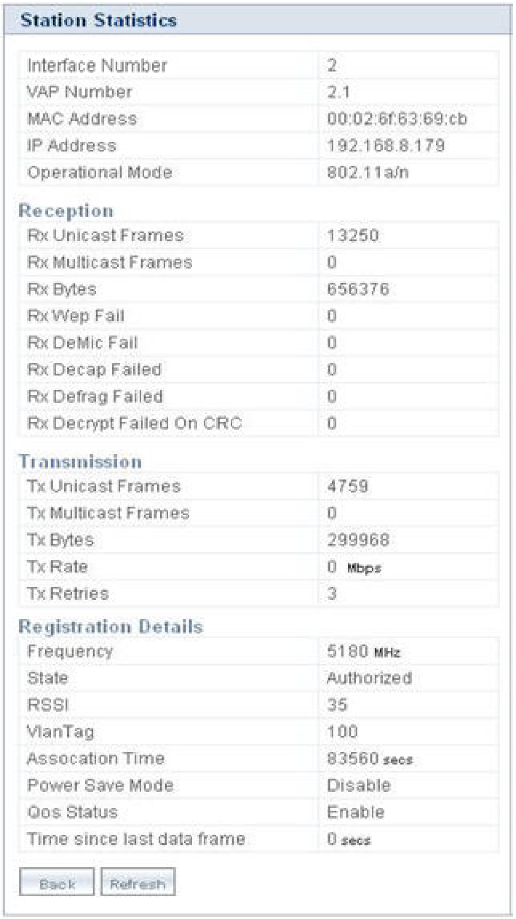
Figure 7-3 Station Statistics

The **Station Statistics** screen contains the following information:

Parameter	Description
MAC Address	Specifies the MAC address of the wireless client.

IP Address	Specifies the IP address of the wireless client. *:* • ***IP Address*** *is not applicable to a WDS enabled wireless client. By default, it is "0.0.0.0".* • ***IP Address*** *is not applicable, if Proxy ARP is disabled.*
VAP Number	Specifies the VAP number enabled on either interface 1 or interface 2.
VAP Type	Specifies the type of the VAP enabled.
RSSI	Specifies the strength of the signal received by the wireless client. The signal strength detected by the radio of the device, varies between the values 0 - 128. The higher the value, the greater is the received signal strength.
Tx Rate (Mbps)	Specifies the rate at which the last data packet is received.
State	Specifies the current status of the wireless client.
Disassociate	Specifies the parameter that disassociates a particular wireless client from the device. *: Disassociate option is not applicable to a WDS enabled wireless client.*

To view detailed station statistics, click Edit icon. The configuration screen appears:



Station Statistics

Interface Number	2
VAP Number	2.1
MAC Address	00:02:6f:63:69:cb
IP Address	192.168.8.179
Operational Mode	802.11a/n

Reception

Rx Unicast Frames	13250
Rx Multicast Frames	0
Rx Bytes	656376
Rx Wep Fail	0
Rx DeMic Fail	0
Rx Decap Failed	0
Rx Defrag Failed	0
Rx Decrypt Failed On CRC	0

Transmission

Tx Unicast Frames	4759
Tx Multicast Frames	0
Tx Bytes	299968
Tx Rate	0 Mbps
Tx Retries	3

Registration Details

Frequency	5180 MHz
State	Authorized
RSSI	35
VlanTag	100
Assocation Time	83560 secs
Power Save Mode	Disable
Qos Status	Enable
Time since last data frame	0 secs

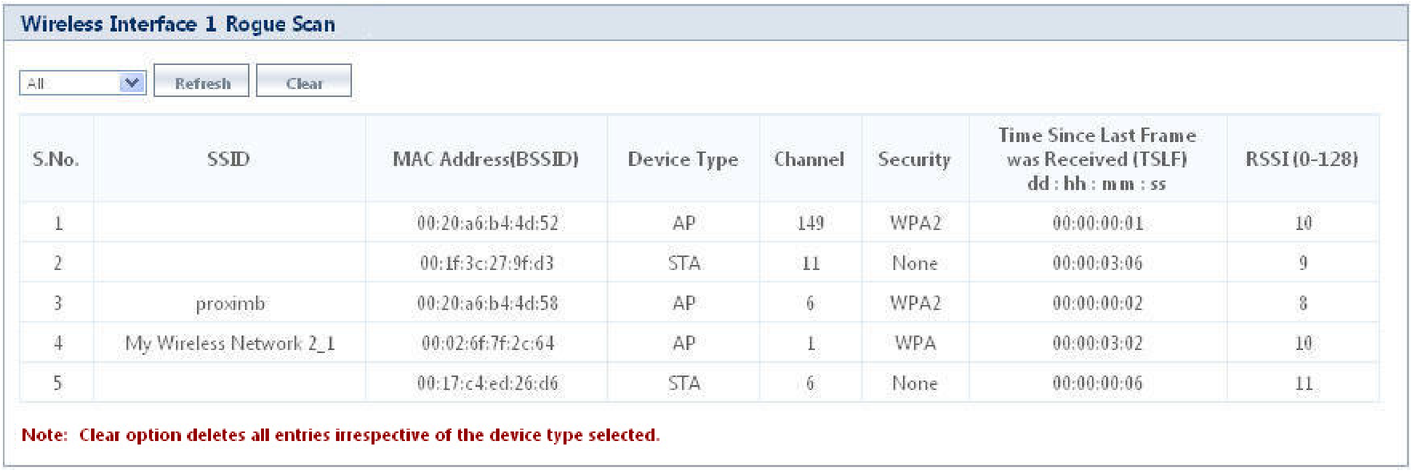
Figure 7-4 Station Statistics - Edit

Click **Refresh**, to view the updated Station Statistics.

7.3 Rogue Scan Statistics

Rogue Scan allows you to monitor all the wireless devices (AP/STA/WDS/ADHOC) and rogue AP devices detected, within the vicinity of your device. It provides with the statistics of all the devices detected under *Current Channel Scan Mode* or *All Channel Scan Mode*. Depending on the device type (AP, STA, Adhoc, WDS and Other devices) selected from the drop down menu, the Rogue Scan Statistics are displayed.

To view, navigate to **MONITOR > Rogue Scan > Interface 1**. The **Rogue Scan Statistics** screen appears.



S.No.	SSID	MAC Address(BSSID)	Device Type	Channel	Security	Time Since Last Frame was Received (TSLF) dd : hh : mm : ss	RSSI (0-128)
1		00:20:a6:b4:4d:52	AP	149	WPA2	00:00:00:01	10
2		00:1f:3c:27:9f:d3	STA	11	None	00:00:03:06	9
3	proximb	00:20:a6:b4:4d:58	AP	6	WPA2	00:00:00:02	8
4	My Wireless Network 2_1	00:02:6f:7f:2c:64	AP	1	WPA	00:00:03:02	10
5		00:17:c4:ed:26:d6	STA	6	None	00:00:00:06	11

Note: Clear option deletes all entries irrespective of the device type selected.

Figure 7-5 Wireless Interface 1 Rogue Scan Statistics

The **Rogue Scan Statistics** screen, contains the following information:

Parameter	Description
SSID	Specifies the SSID of the detected device.
MAC Address (BSSID)	Specifies the MAC address of the detected device.
Device Type	Specifies the device type (AP, STA, Adhoc, WDS and other devices) detected.
Channel	Specifies the channel of the detected device.
Security	Specifies the security applied on the detected device. Tabulated below are different **Security** types and the corresponding Authentication Modes / Encryption Types applied on the device.
TSLF	Specifies the time period since the last frame is received **(TSLF)** over the channel. It is recorded in **dd : hh : mm : ss** (days: hours: minutes: seconds)
RSSI	Specifies the strength of the signal received by the detected device. The signal strength detected by the device, varies between 0 - 128. The higher the value, the greater is the received signal strength.

Security	Encryption Type / Authentication Mode
None	No security
WEP	WEP / Dot1x
WPA	PSK-TKIP / Dot1x TKIP
WPA2	PSK-AES / Dot1x AES
Other / WEP	Other

Click **Refresh**, to view the updated Rogue Scan Statistics and click **Clear**, to clear the Rogue Scan Statistics.

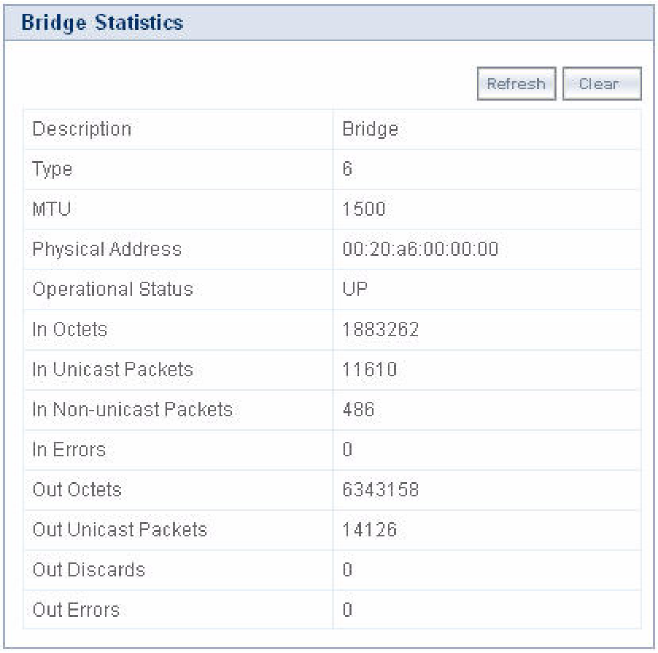
7.4 Bridge

The device serves as a bridge between the wired and the wireless networking devices.

7.4.1 Bridge Statistics

The Bridge Statistics allows you to monitor the statistics of the Bridge.

To view bridge statistics, navigate to **MONITOR > Bridge > Bridge Statistics**. The **Bridge Statistics** screen appears.



Description	Bridge
Type	6
MTU	1500
Physical Address	00:20:a6:00:00:00
Operational Status	UP
In Octets	1883262
In Unicast Packets	11610
In Non-unicast Packets	486
In Errors	0
Out Octets	6343158
Out Unicast Packets	14126
Out Discards	0
Out Errors	0

Figure 7-6 Bridge Statistics

The **Bridge Statistics** screen contains the following information:

Parameter	Description
Description	Specifies the interface type that is ‘Bridge’.
Type	Specifies the type of interface that is distinguished according to the physical/link protocol(s) below the network layer in the protocol stack.
MTU	Specifies the largest size of the data packet sent on the bridge.
Physical Address	Specifies the MAC address of the interface.
Operational Status	Specifies the current operational status of the bridge.
In Octets	Specifies the total number of octets received on the bridge.
In Unicast Packets	Specifies the number of unicast sub-network packets delivered to the higher level protocol.
In Non-Unicast Packets	Specifies the number of non-unicast sub-network packets delivered to the higher level protocol.
In Errors	Specifies the number of inbound packets with errors and that are restricted from being delivered. In Errors on the wireless interface include CRC errors.

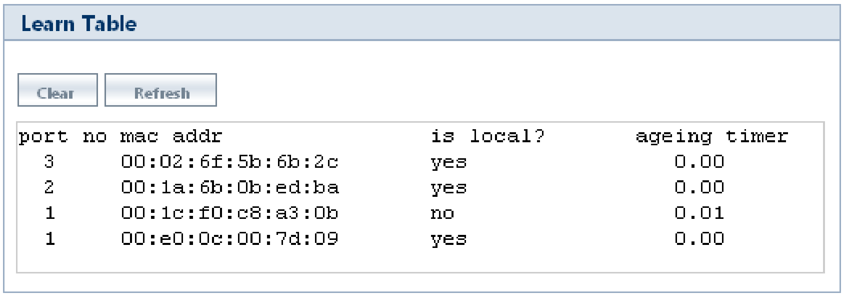
Out Octets	Specifies the total number of octets transmitted out of the bridge.
Out Unicast Packets	Specifies the total number of packets requested by the higher level protocol and then transmitted to the non-unicast address.
Out Discards	Specifies the number of error-free outbound packets which are discarded to free up buffer space.
Out Errors	Specifies the number of outbound error packets that are not allowed to transmit.

Click **Refresh**, to view updated Bridge statistics and click **Clear**, to clear the Bridge statistics.

7.4.2 Learn Table

'Learn Table' statistics allow you to view MAC address of the learnt device, the bridge port number, aging timer for each device learnt on an interface, and the local (DUT's local interfaces)/remote (learned entries through bridging) status of the learnt device. There can be up to 10,000 entries in the Learn Table.

To view learn table statistics, navigate to **MONITOR > Bridge > Learn Table**. The **Learn Table** screen appears.



```
port no mac addr                is local?       ageing timer
  3     00:02:6f:5b:6b:2c       yes                0.00
  2     00:1a:6b:0b:ed:ba       yes                0.00
  1     00:1c:f0:c8:a3:0b       no                 0.01
  1     00:e0:0c:00:7d:09       yes                0.00
```

Figure 7-7 Learn Table

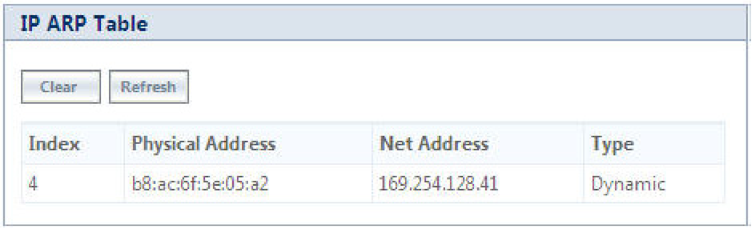
Click **Refresh**, to view updated Learn Table statistics and click **Clear**, to clear the Learn Table statistics.

7.5 Network Layer

7.5.1 IP Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address on the network. The IP ARP table is used to maintain a correlation between each IP address and its corresponding MAC address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

To view IP Address Resolution Protocol (ARP) statistics, navigate to **MONITOR > Network Layer > IP ARP**. The **IP ARP Table** screen appears.



Index	Physical Address	Net Address	Type
4	b8:ac:6f:5e:05:a2	169.254.128.41	Dynamic

Figure 7-8 IP ARP Statistics

The **IP ARP Table** contains the following information:

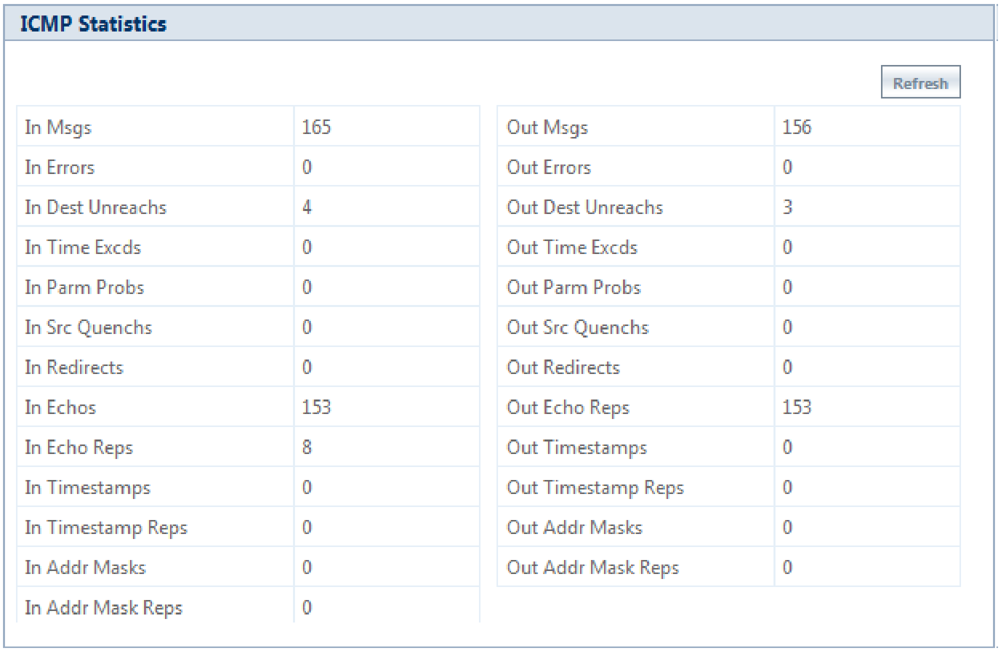
Parameter	Description
Index	Specifies the interface type.
Physical Address	Specifies the MAC address of a node on the network.
Net Address	Specifies the corresponding IP address of a node on the network.
Type	Specifies the type of mapping, that is dynamic or static.

Click **Refresh**, to view updated IP ARP Table statistics and click **Clear**, to clear the IP ARP Table statistics.

7.5.2 Internet Control Message Protocol (ICMP) Statistics

'ICMP Statistics' allow you to monitor the message traffic that is received and transmitted by the device.

To view ICMP statistics, navigate to **MONITOR > Network Layer > ICMP Statistics**. The **ICMP Statistics** screen appears.



In Msgs	165	Out Msgs	156
In Errors	0	Out Errors	0
In Dest Unreachs	4	Out Dest Unreachs	3
In Time Excds	0	Out Time Excds	0
In Parm Probs	0	Out Parm Probs	0
In Src Quenchs	0	Out Src Quenchs	0
In Redirects	0	Out Redirects	0
In Echos	153	Out Echo Reps	153
In Echo Reps	8	Out Timestamps	0
In Timestamps	0	Out Timestamp Reps	0
In Timestamp Reps	0	Out Addr Masks	0
In Addr Masks	0	Out Addr Mask Reps	0
In Addr Mask Reps	0		

Figure 7-9 ICMP Statistics

The **ICMP Statistics** screen contains the following information:

Parameter	Description
In Msgs/Out Msgs	Specifies the number of ICMP messages that are received or transmitted by the device.
In Errors/Out Errors	Specifies the number of ICMP messages that are received or transmitted by the device, but determined as having ICMP-specific errors such as Bad ICMP checksums, bad length, etc. In Errors on the wireless interface include CRC errors.
In Dest Unreachs/Out Dest Unreachs	Specifies the number of ICMP messages, received or transmitted by the device, that do not reach the destination.

In Time Excds/Out Time Excds	Specifies the number of ICMP time exceeded messages that are received or transmitted by the device.
In Parm Probs/Out Parm Probs	Specifies the number of ICMP parameter problem messages that are received or transmitted by the device.
In Src Quenchs/Out Src Quenchs	Specifies the number of ICMP source quench messages that are received or transmitted by the device.
In Redirects/Out Redirects	Specifies the rate at which the ICMP redirect messages are received or transmitted by the device.
In Echos	Specifies the rate at which the ICMP Echo messages are received.
In EchoReps/Out EchoReps	Specifies the rate at which the ICMP echo reply messages are received or transmitted by the device.
In Timestamps/Out Timestamps	Specifies the rate at which the ICMP timestamp (request) messages are received or transmitted by the device.
In Timestamp Reps/Out Timestamp Reps	Specifies the rate at which the ICMP timestamp reply messages are received or transmitted by the device.
In Addr Masks/Out Addr Masks	Specifies the number of ICMP address mask request messages that are received or transmitted by the device.
In Addr Mask Reps/Out Addr Mask Reps	Specifies the number of ICMP address mask reply messages that are received or transmitted by the device.

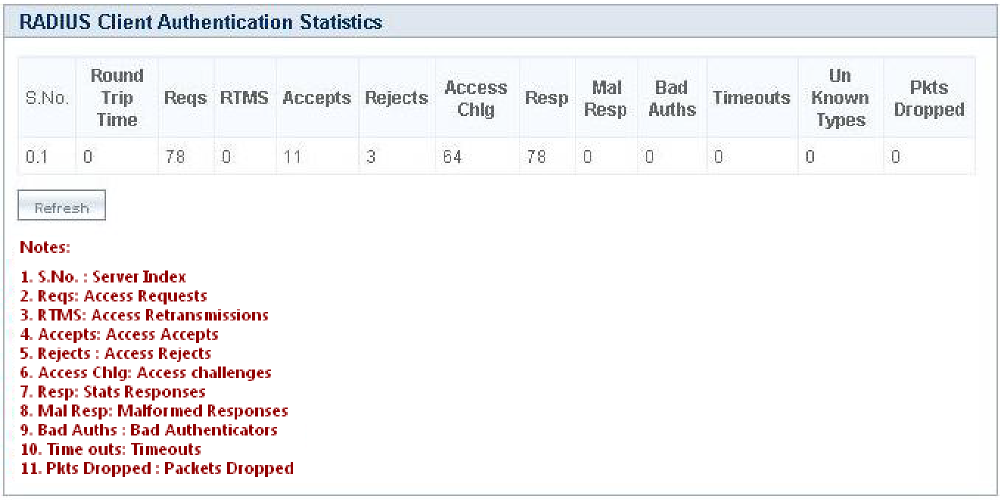
Click **Refresh**, to view updated ICMP statistics.

7.6 RADIUS

7.6.1 Authentication Statistics

Authentication statistics provide information on RADIUS Authentication for both the primary and backup servers for each RADIUS server profile.

To view authentication statistics, navigate to **MONITOR > RADIUS > Authentication Statistics**. The **RADIUS Client Authentication Statistics** screen appears.



RADIUS Client Authentication Statistics

S.No.	Round Trip Time	Reqs	RTMS	Accepts	Rejects	Access Chlg	Resp	Mal Resp	Bad Auths	Timeouts	Un Known Types	Pkts Dropped
0.1	0	78	0	11	3	64	78	0	0	0	0	0

Notes:

1. S.No. : Server Index
2. Reqs: Access Requests
3. RTMS: Access Retransmissions
4. Accepts: Access Accepts
5. Rejects : Access Rejects
6. Access Chlg: Access challenges
7. Resp: Stats Responses
8. Mal Resp: Malformed Responses
9. Bad Auths : Bad Authenticators
10. Time outs: Timeouts
11. Pkts Dropped : Packets Dropped

Figure 7-10 RADIUS Client Authentication Statistics

The **RADIUS Client Authentication Statistics** screen contains the following information:

Parameter	Description
Round Trip Time	Specifies the round trip time for messages exchanged between RADIUS client and authentication server since the client startup.
Reqs	Specifies the number of RADIUS access request messages transmitted from the RADIUS client to the authentication server since client startup.
RTMS	Specifies the number of times the RADIUS access requests are being re-transmitted to the server from the device since the client startup.
Accepts	Specifies the number of RADIUS access accept messages received by the device since client startup.
Rejects	Specifies the number of RADIUS access reject messages received by the device since client startup.
Access Chlg	Specifies the number of RADIUS access challenge messages received by the device since the client startup.
Resp	Specifies the number of RADIUS response packets received by the device since client startup.
Mal Resp	Specifies the number of malformed RADIUS access response messages received by the device since client startup.
Bad Auths	Specifies the number of malformed RADIUS access response messages containing invalid authenticators received by the device since client startup.

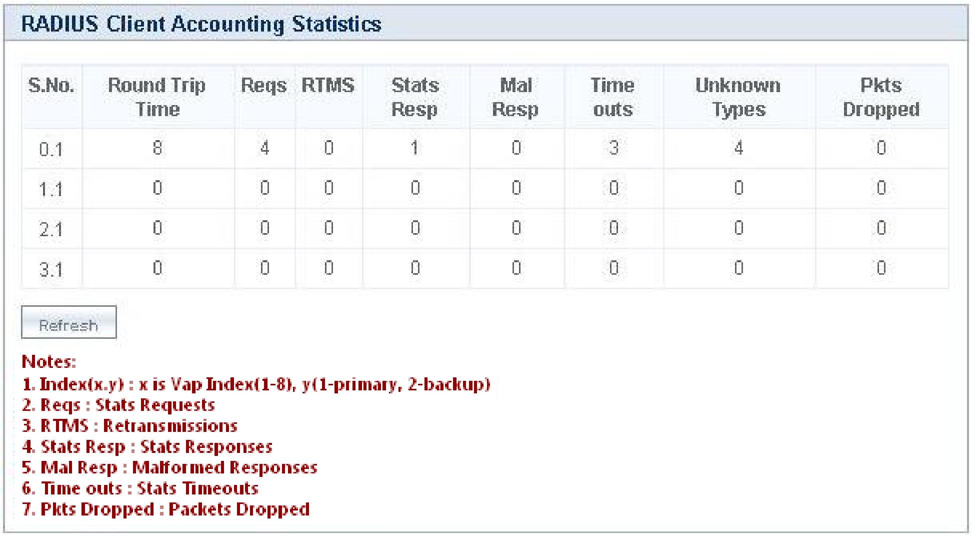
Timeouts	Specifies total number of time-outs for RADIUS access request messages since client startup.
Unknown Types	Specifies the number of messages with unknown RADIUS message code since client startup.
Pkts Dropped	Specifies the number of RADIUS packets dropped by the device.

Click **Refresh**, to view updated RADIUS Client Authentication statistics.

7.6.2 Accounting Statistics

Accounting statistics provide information on RADIUS Accounting for both the primary and backup servers for each RADIUS server profile.

To view accounting statistics, navigate to **MONITOR > RADIUS > Accounting Statistics**. The **RADIUS Client Accounting Statistics** screen appears.



RADIUS Client Accounting Statistics

S.No.	Round Trip Time	Reqs	RTMS	Stats Resp	Mal Resp	Time outs	Unknown Types	Pkts Dropped
0.1	8	4	0	1	0	3	4	0
1.1	0	0	0	0	0	0	0	0
2.1	0	0	0	0	0	0	0	0
3.1	0	0	0	0	0	0	0	0

Notes:
1. Index(x.y) : x is Vap Index(1-8), y(1-primary, 2-backup)
2. Reqs : Stats Requests
3. RTMS : Retransmissions
4. Stats Resp : Stats Responses
5. Mal Resp : Malformed Responses
6. Time outs : Stats Timeouts
7. Pkts Dropped : Packets Dropped

Figure 7-11 RADIUS Client Accounting Statistics

The **RADIUS Client Accounting Statistics** screen contains the following information:

Parameter	Description
Round Trip Time	Specifies the round-trip time for messages exchanged between RADIUS client and accounting server since client startup.
Reqs	Specifies the number of RADIUS accounting request messages transmitted from the RADIUS client to the accounting server since client startup.
RTMS	Specifies the number of times the RADIUS accounting requests are being re-transmitted to the accounting server from the device since the client startup.
Stats Resp	Specifies the total number of RADIUS accounting messages received by the device since system startup.
Mal Resp	Specifies the number of malformed RADIUS accounting response messages received by the device since client startup.
Timeouts	Specifies the total number of time-outs for RADIUS accounting request messages since client startup.

Unknown Types	Specifies the number of messages with unknown RADIUS message code since client startup.
Pkts Dropped	Specifies the number of RADIUS accounting packets dropped by the device.

Click **Refresh**, to view updated RADIUS Client Accounting statistics.

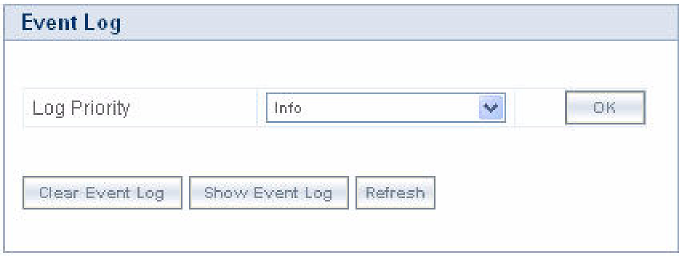
7.7 Logs

7.7.1 Event Log

Event Logs track all the events that occur during the operation of the device and display the event occurring time, event type, and the name of the error or the error message. Based on the priority, the event details are logged and can be used for any reference or troubleshooting.

To view Event Logs, do the following:

1. Navigate to **MONITOR > Logs > Event Log**. The **Event Log** screen appears.

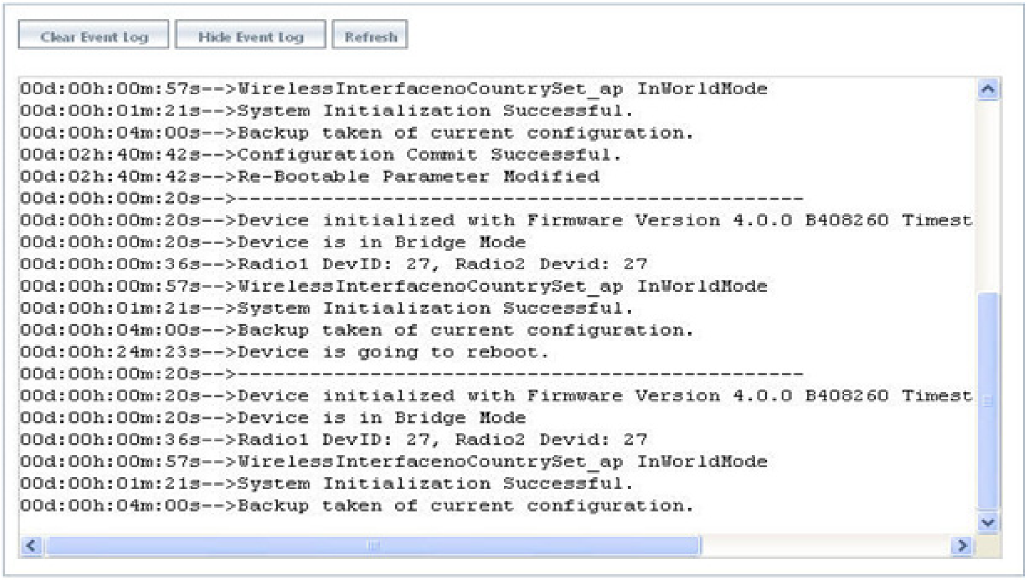


Event Log

Log Priority: Info

Figure 7-12 Event Log

2. Select the appropriate log priority from the **Log Priority** box and click **OK**. Log priority may vary between **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info and Debug**. (Refer SYSLOG Host Table)
3. To view the event logs for the selected log priority, click **Show Event Log**.



```
00d:00h:00m:57s-->WirelessInterfacenoCountrySet_ap InWorldMode
00d:00h:01m:21s-->System Initialization Successful.
00d:00h:04m:00s-->Backup taken of current configuration.
00d:02h:40m:42s-->Configuration Commit Successful.
00d:02h:40m:42s-->Re-Bootable Parameter Modified
00d:00h:00m:20s-->----------------------------------------------
00d:00h:00m:20s-->Device initialized with Firmware Version 4.0.0 B408260 Timest
00d:00h:00m:20s-->Device is in Bridge Mode
00d:00h:00m:36s-->Radio1 DevID: 27, Radio2 Devid: 27
00d:00h:00m:57s-->WirelessInterfacenoCountrySet_ap InWorldMode
00d:00h:01m:21s-->System Initialization Successful.
00d:00h:04m:00s-->Backup taken of current configuration.
00d:00h:24m:23s-->Device is going to reboot.
00d:00h:00m:20s-->----------------------------------------------
00d:00h:00m:20s-->Device initialized with Firmware Version 4.0.0 B408260 Timest
00d:00h:00m:20s-->Device is in Bridge Mode
00d:00h:00m:36s-->Radio1 DevID: 27, Radio2 Devid: 27
00d:00h:00m:57s-->WirelessInterfacenoCountrySet_ap InWorldMode
00d:00h:01m:21s-->System Initialization Successful.
00d:00h:04m:00s-->Backup taken of current configuration.
```

Figure 7-13 Event Logs for the Specified Log Priority

4. Click **Hide Event Log**, to hide the event logs.

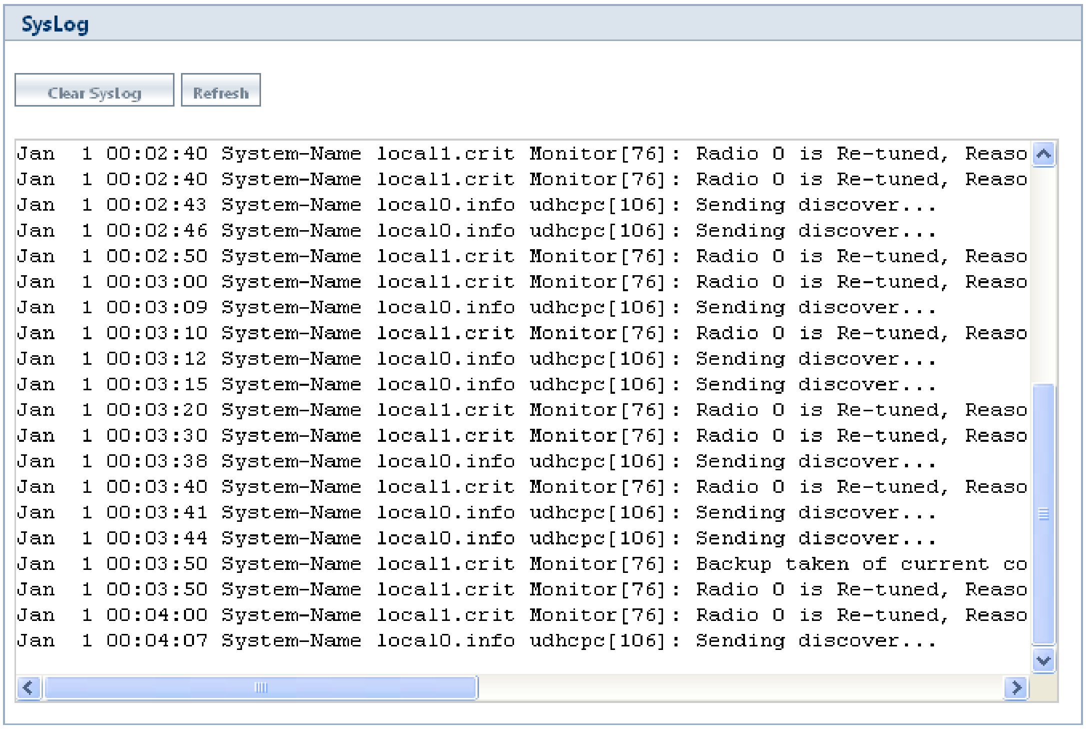
5. Click **Clear Event Log**, to clear the event logs.
6. Click **Refresh**, to view updated event logs.

: The recent event logs are stored in the flash memory.

7.7.2 SysLog

System log messages are generated by the system by sending requests at various instances to the system log server.

To view System Logs, navigate to **MONITOR > Logs > Syslog**. The **SysLog** screen appears.



```
Jan  1 00:02:40 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:02:40 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:02:43 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:02:46 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:02:50 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:03:00 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:03:09 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:03:10 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:03:12 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:03:15 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:03:20 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:03:30 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:03:38 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:03:40 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:03:41 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:03:44 System-Name local0.info udhcpc[106]: Sending discover...
Jan  1 00:03:50 System-Name local1.crit Monitor[76]: Backup taken of current co
Jan  1 00:03:50 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:04:00 System-Name local1.crit Monitor[76]: Radio 0 is Re-tuned, Reaso
Jan  1 00:04:07 System-Name local0.info udhcpc[106]: Sending discover...
```

Figure 7-14 System Logs

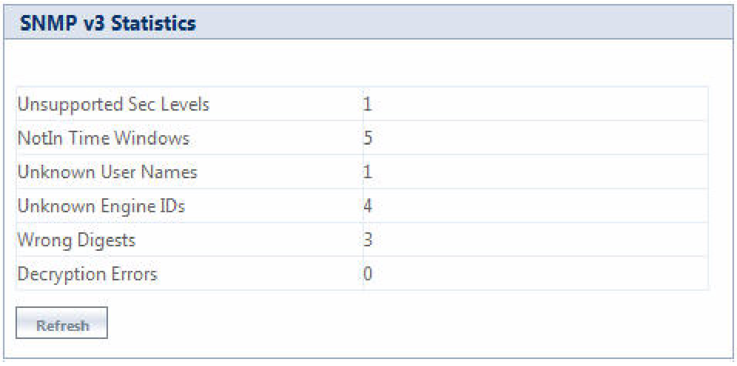
Click **Clear SysLog**, to clear the system logs and click **Refresh**, to view updated system logs.

7.8 Console Commands

The Console Commands feature helps Proxim's Technical Support team to debug field issues.

7.9 SNMP v3 Statistics

To view SNMP v3 Statistics, navigate to **MONITOR** > **SNMP V3 Statistics**. The **SNMP v3 Statistics** screen appears.



SNMP v3 Statistics

Unsupported Sec Levels	1
NotIn Time Windows	5
Unknown User Names	1
Unknown Engine IDs	4
Wrong Digests	3
Decryption Errors	0

Figure 7-15 SNMP V3 Statistics

The **SNMP v3 Statistics** screen contains the following information:

Parameter	Description
Unsupported Sec Levels	Specifies the total number of packets received by the SNMP engine which were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not In Time Windows	Specifies the total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	Specifies the total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.
Unknown Engine IDs	Specifies the total number of packets received by the SNMP engine which were dropped because they referenced an SNMP Engine ID that was not known to the SNMP engine.
Wrong Digests	Specifies the total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value.
Decryption Errors	Specifies the total number of packets received by the SNMP engine which were dropped because they could not be decrypted.

Click **Refresh**, to view the updated statistics.

*: ‘**SNMP v3 Statistics**’ is applicable only to the SNMP version v3. See* SNMP Version - SNMPv3*.*

Troubleshooting 8

This chapter helps you to address the following hardware and software issues, that might arise while using our device.

❗:

- **Before you start troubleshooting, ensure that all the guidelines detailed in the product documentation are satisfied. For details on RADIUS, TFTP, Terminal and Telnet Programs, and Web Browsers, refer to** Device Configuration **and** Device Management**.**
- **We recommend you to check our support site** http://support.proxim.com**, if the procedures discussed in this chapter do not provide a complete solution to your problem.**
- **In some cases, rebooting the device clears the problem. If nothing helps, consider** Soft Reset to Factory Defaults **or** Forced Reload**. Performing Forced Reload, you need to download a new firmware onto the device.**

8.1 Gigabit PoE Injector (Not supplied)

Problem	Solution
The Device Does Not Boot / Power ON / Initialize	• Make sure that you are using a standard UTP Category 5/Category6 foiled, twisted pair cable to power the device. • Try a different port on the same PoE Injector hub (remember to move the input port accordingly) – if it works then there is a problem in the previous RJ45 port or a bad RJ45 port connection. • Try to connect the device to a different PoE Injector hub. • Try using a different ethernet cable – if it works, there is probably a fault in the cable or its connection. • Check the power plug and hub. • If the ethernet link goes down, check the cable, cable type, switch and hub. • Make sure all the cables to the device are connected properly. • Make sure your power source is ON. • Try connecting the DC5v port of the device with a 110-220v worldwide power adapter, available at *Proxim Wireless Corporation,* on request.

There is No Data Link Established	• Verify that the indicator on the device port is “ON.” • Verify that the PoE Injector hub is properly connected to the ethernet port of the device. • Verify that the ethernet cable is Category 5 or better and is less than 100 meters (approximately 325 feet) in length from the ethernet port of the device to the PoE. • Try to connect a different device to the same port on the PoE Injector hub – if it works and a link is established then there is probably a fault in the data link of the device. • Try to re-connect the cable to a different output port (remember to move the input port accordingly) – if it works then there is a fault probably in the output or input port of the PoE Injector hub or a bad RJ45 connection.
Power Overload Indications	• Connect the device to a PoE Injector. • Ensure that there is no short over on any of the connected cables. • Move the device into a different output port (remember to move the input port accordingly) - if it works then there is a fault probably in the previous RJ45 port or bad RJ45 port connection.

8.2 Connectivity Issues

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

<table>
<tr><th>Problem</th><th>Solution</th></tr>
<tr><td>Device Does Not Boot / No LED Activity</td><td>See The Device Does Not Boot / Power ON / Initialize</td></tr>
<tr><td>Ethernet Link Does Not Work</td><td>Check the ethernet LED. The color of the Ethernet LED indicates the speed of the Ethernet traffic:
<table>
<tr><th colspan="2">Ethernet LED Color</th><th>Speed</th></tr>
<tr><td>🟥</td><td>Red</td><td>100 Mbps</td></tr>
<tr><td>🟩</td><td>Green</td><td>1000 Mbps</td></tr>
<tr><td></td><td>OFF</td><td>No link is available or Ethernet is not connected</td></tr>
</table>
Try connecting the device:
• To a different port on the PoE and/or a switch.
• Through a different Ethernet Category 5/Category6 cable.</td></tr>
</table>

Serial Link Does Not Work	• Double-check the physical network connections. • Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values: – **Com Port**: (COM1, COM2 and so on depending on your computer); – **Baud rate**: 115200; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None; – Line Feeds with Carriage Returns – (In HyperTerminal select: **File > Properties > Settings > ASCII Setup > Send Line Ends with Line Feeds**) *: Not applicable to AP-8100.*
The Wireless LED does not glow on the device	• For AP-800 and AP-8000, the device might be in Bootloader Mode. Refer Download a New Image using the Bootloader CLI. If the device is not in the Bootloader mode, please perform a Forced Reload operation on the device. *: Not applicable to AP-8100.* • The wireless interface might be down. Ensure, the wireless interface is enabled and all the wireless properties are configured properly.
Cannot Access the Web Interface	• The **Speed and TX mode** configured is different at both the ends of a wired link. Ensure that the same Tx mode is configured at both the ends and same ethernet speed is maintained. See Ethernet. • Open a command prompt window and type the Ping command along with the IP address of the device. For example, **ping 10.0.0.1**. If the device does not respond, check if you have the correct IP address. If the device responds then it means the ethernet connection is working properly. • Double-check the physical network connections. Use a well-known device to ensure the network connection is functioning properly. • Ensure that you are using Microsoft Internet Explorer 7.0 (or later) or Mozilla Firefox 10.0 (or later). • Ensure that you are not using a proxy server for the network connection with your Web browser. • Use CLI, to check the IP Access Table which can restrict access to Telnet and HTTP. • Ensure that you have not exceeded the maximum number CLI sessions. • Troubleshoot the network infrastructure (check switches, routers, and so on). • Also, ensure that the Management VLAN ID is enabled. Refer Virtual Local Area Network (VLAN) • Ensure that the ***Reload Functionality Status is*** *enabled to perform reload procedures. Else, refer to the recovery procedure explained in Reload.* *: At any point of time, if your device is unable to connect to your network, reset the device by unplugging and plugging the cables from the PoE (if using a PoE).*

Connection to the host is lost	When you try to access the AP Device through HTTP interface (169.254.128.132) during its initialization, you might receive an error saying “*Could not open connection to the host, on port 23: Connect failed*” Hence, it is recommended to wait for two minutes, until the device is completely initialized and then try to access the device through HTTP interface.

8.3 Setup and Configuration Problems

Problem	Solution
Device Reboots Continuously	One of the reason for the device to reboot continuously is that the radio card is not properly placed in the mini-PCI slot. When you power on the device and you do not see the “**WIRELESS NETWORK1 PASSED**” message in the POST message in the Serial Console, please contact Proxim’s support site at http://support.proxim.com. 📝*: Not applicable to AP-8100.*
Lost Telnet or SNMP Password	Perform Soft Reset to Factory Defaults procedure. This procedure resets system and network parameters, but does not affect the image of the device. The default HTTP, Telnet, and SNMP username is **“admin”** and password is **“public”** for the device.
Device Responds Slowly	If the device takes a long time to respond, it could mean that: • The **Speed and TX mode** configured is different at both the ends of a wireless link. Ensure that the same Tx mode is configured at both the ends and same ethernet speed is maintained. See Ethernet • The IP address of the device is already in use. Verify that the IP address is assigned only to the device. Do this by switching off the device and then pinging the IP address. • The network traffic is high.
Incorrect Device IP Address	• The default IP address assignment mode is dynamic. The device contacts a DHCP server during boot-up. If the DHCP server is not available on your network while the device is booting, then the fall back IP address (**169.254.128.132)** of the device is used. • Use ScanTool, to find the current IP address of the device. Once you have the current IP address, use Web Interface or CLI Interface to change the device IP settings, if necessary. • If you are using static IP address assignment, and cannot access the device over ethernet, refer to Initializing the IP Address by using CLI. • Perform the Soft Reset to Factory Defaults procedure. This will reset the device to dynamic mode. If there is a DHCP Server on the network, the DHCP Server will assign an IP address automatically to the device.

HTTP Interface / Telnet Interface Does Not Work	• Make sure you are using a compatible browser: — Microsoft Internet Explorer 7.0 or later — Mozilla Firefox 3.0 or later • Make sure you have the proper IP address of device. Enter the device IP address in the address bar of the browser, for example **http://169.254.128.132**. • When the **Enter Network Password** window appears, enter the **User Name** and enter the HTTP password in the **Password** field. The default HTTP username is **admin** and password is **public**. • Use CLI, to check the IP Access Table which can restrict access to Telnet and HTTP.
Not able to login into the CLI, after the unit is rebooted	Though the CLI prompts for the username and password, the device will take two minutes to get initialized and accept the login credentials, after rebooting it.
Telnet CLI Does Not Work	• Make sure you have the proper IP address. Enter the device IP address in the Telnet connection dialog, from a DOS prompt: **C:\> telnet <Device IP Address>** • Use HTTP, to check the IP Access Table which can restrict access to Telnet and HTTP. *: Please enable Telnet in Vista or Windows 7 as it is by default disabled.*
TFTP Server Does Not Work	With TFTP, you can transfer files to and from the device. If a TFTP server is not properly configured and running, you cannot upload and download files. The TFTP server: • Can be situated either local or remote • Must have a valid IP address • Must be set for send and receive without time-out • Must be running only during file upload and download If the TFTP server does not upload or download files, it could mean: • The TFTP server is not running • The IP address of the TFTP server is invalid • The upload or download directory is not correctly set • The file name is not correct *:* • *Ensure, the firewall on the Ethernet PC is disabled until the TFTP process is completed.* • *Also ensure that the IP Address configured on the server and the wireless client are the same, by checking the IP Address at the bottom right corner of the TFTP Server.*
Unable to Retrieve Event Logs through HTTPS	If using Internet Explorer 7 and are not able to retrieve event logs through HTTPS, do the following: 1. Open Internet Explorer 2. Navigate to **Tools** > **Internet Options** > **Advanced** 3. Go to **Security** and uncheck/deselect **Do not save encrypted pages to disk** Alternatively, use Mozilla Firefox 3.5 or later.

Uploading Older Version Configuration Files	If you are trying to upload the configuration files of the older versions below AP 3.0 on AP 4.0, the device hangs and does not perform the normal AP functionality. This issue can be recovered by just deleting the uploaded configuration file and resetting the factory values, by using soft and hard reload functionality of the device. See Soft Reset to Factory Defaults and Hard Reset to Factory Defaults (Reload)
Not able to initialize the device in bootloader mode, using CLI	This could be due to one of following errors: **TFTP Error** • Ensure, that the firewall on the Ethernet PC is disabled until the TFTP process is completed. • Ensure, that the firmware image loaded is located in the corresponding TFTP folder. • Use a different TFTP server like '*tftpd32*' **Bad Magic Number**: • You get this error when a wrong or invalid firmware image is loaded on to the AP device. • Ensure, that a firmware image is loaded on to the AP device and is located in the corresponding TFTP folder.
Client Connectivity Issues	
Problem	**Solution**
Wireless Station / Client's Not Connected	• Client computers should have the same Network Name (VAP SSID) and security settings as the device. (Network Names and WEP Keys are typically allocated and maintained by your Network Administrator.) • Network Names (VAP SSIDs) should be allocated and maintained by the Network Administrator. • For additional troubleshooting tips, see the documentation that comes with your client card. • Check, if other wireless clients within the coverage area of same Access Point are able to detect the SSID.
Intermittent Loss of Connection	• Make sure you are within the range of an active device. • You can check the signal strength by using the signal strength gauge on the client software.
Wireless Client Does Not Receive any IP Address	• Check the IP configuration of the device by logging on to the web interface. • Check whether the DHCP server can be reached from the device. This can be verified by pinging the DHCP server from a wired station connected to the same switch as that of the device. • If VLAN is configured for the SSID, check whether the DHCP server is available in that VLAN. • If WEP or WPA-PSK/WPA2-PSK Security mechanisms are used, then ensure that pass-phrase configured in security profile and the client are the same. • If WPA or WPA2 Security mechanisms are used, then ensure the EAP settings are proper in the client and the RADIUS server

Clients connect at legacy rates but not higher rates	• Check the security modes. – WEP and WPA-TKIP will make the unit to operate at legacy rates. • Check the Channel bandwidth: Should be set to 40MHz • Check the Operating mode: It should be either 802.11gn or 802.11an
VLAN Related Issues	
Problem	**Solution**
Verifying VLAN Functionality on the Device	The correct VLAN configuration can be verified by using ping command in both wired and wireless hosts from both sides of the device and the network switch. Traffic can be “sniffed” on the wired (ethernet), if configured. Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the device.
VLAN Workgroups	The correct VLAN assignment can be verified by pinging the device to ensure connectivity, by pinging the switch to ensure VLAN properties, and by pinging hosts past the switch to confirm the switch is functional. Ultimately, traffic can be “sniffed” on the ethernet using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the user’s assigned network name. ⚠ ***: The** Forced Reload **procedure disconnects all the users and resets all values to factory defaults.***
What if network traffic is being directed to a non-existent host?	All sessions are disconnected, traffic is lost, and a Forced Reload is necessary. • You can configure the switch to mimic the non-existent host.
I have just configured the Management ID and now I can't manage the device?	Check to ensure your password is correct. If your password is incorrect or all inbound packets do **NOT** have the correct tag, then a Forced Reload is necessary. – Ensure if the Ethernet PC, through which you are managing the AP device, belongs to the same Management VLAN ID.

8.4 Recovery Procedures

8.4.1 Soft Reset to Factory Defaults

Use this procedure to reset the network configuration values, including the Password, IP Address, and Subnet Mask. This procedure resets configuration settings, but does not change the current device Image.

- To use this procedure, in the web interface navigate to **MANAGEMENT** > **Reset to Factory**.
- The DHCP Server gets the default IP address (169.254.128.132) for the device. You can change the IP address by using Web Interface or CLI. If you do not have access to the HTTP or CLI interfaces, use Hard Reset to Factory Defaults (Reload) procedure.

: If you are not able to access and configure the device by using web interface, then enter the ***username*** *and* ***password*** *as* ***reload****, in terminal emulator (serial) interface (not applicable for AP-8100), after the device is initialized. This soft reset procedure will set the device to factory defaults.*

8.4.2 Hard Reset to Factory Defaults (Reload)

If you cannot access the device or you have lost its password, you can reset the device to its factory default settings by using the **Reload** button available on the device.

Press the Reload button on the AP device for 10 seconds, that will reset the device configuration parameters to default factory settings.

:

- *You need to use a pin or the end of a paperclip to press the Reload button.*
- Ensure that the ***Reload Functionality Status is*** *enabled to perform reload procedure. Else, refer to the recovery procedure explained in* Reload.

If you are not using DHCP, use the ScanTool or CLI to set the IP Address, Subnet Mask, and other IP parameters. Please see *ORiNOCO® 802.11n Access Points - Reference Guide* for CLI information.

: For AP-8100, the Power LED will glow amber as you press the Reload button, indicating that the Reload functionality is applied on the device.

: If you hold the Reload button for long, you may go into Forced Reload mode. See Forced Reload for ***details.***

8.4.3 Forced Reload

With Forced Reload, you bring the device into bootloader mode which erases the firmware. Use this procedure only as a last option if the device does not boot, and the Soft and Hard reset to Factory Defaults procedure does not help.

- **For AP-800 and AP-8000**: To go to forced reload mode, press and release the reset button for the device to initialize and press the reload button for longer than 12 seconds to reset the device to factory defaults, deleting the firmware.
- **For AP-8100**: To go to forced reload mode, follow any of the following procedures:
  - Reset the device by unplugging and plugging in the power cable and then press the Reload button for longer than 12 seconds as soon as you power on the device. The device is reset to factory defaults, deleting the firmware.
  - Press the Reload button for 30 seconds, the device is reset to factory defaults and deletes the firmware.

The device will try to load the image using the default factory configuration parameters. If this fails, then it will enter either CLI mode or ScanTool mode as per the user's choice, with a message on the serial console "Starting ScanTool interface, press any key to enter CLI 5".

Follow one of the procedures below to load a new image to the device:

- Download a New Image using ScanTool
- Download a New Image using the Bootloader CLI

As the CLI requires a physical connection to the device serial port, Proxim recommends you to use the ScanTool option.

:

- *Forced Reload using serial interface (Bootloader CLI) is not applicable for AP-8100.*
- Ensure that the ***Reload Functionality Status is*** *enabled to perform forced reload procedure. Else, refer to the recovery procedure explained in* Reload.

: With Forced Reload, the firmware in the device will be erased. You will need to reload the software before the device is operational.

8.4.3.1 Download a New Image using ScanTool

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

ScanTool automatically detects the device that does not have a valid software image. The **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's ***Change*** screen so that you can download a new image to the device. (These fields are disabled, if ScanTool does not detect a software image problem).

Follow the following steps, to download a new image using ScanTool.

Step 1: Preparing to Download the Device Image

Before starting the download process, you need to know the device IP Address, Subnet Mask, the TFTP Server IP Address, and the Image file name. Make sure the TFTP server is running and properly configured to point to the folder containing the image to be downloaded.

Step 2: Download Procedure

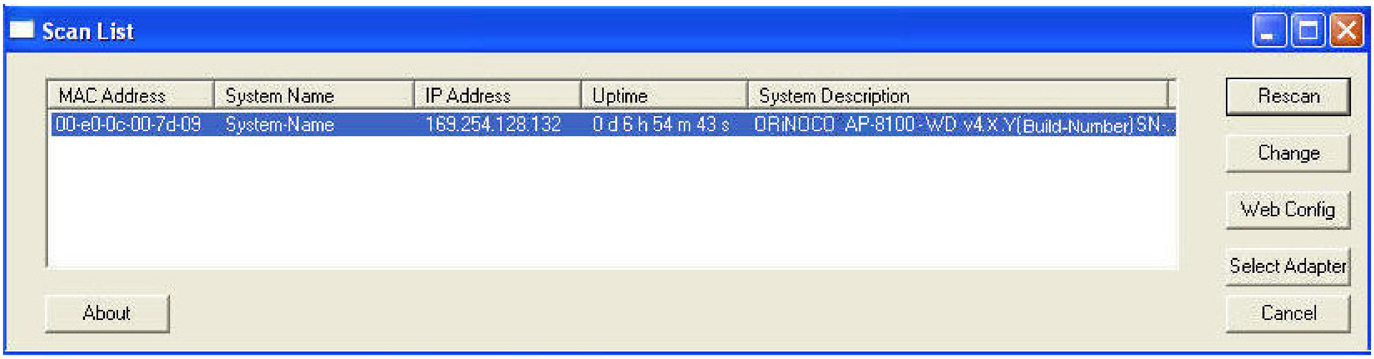
Follow these steps to download a software image to the device by using ScanTool:

1. Download the latest software from http://support.proxim.com.
2. Copy the latest software updates to your TFTP server.
3. Launch Proxim's ScanTool.
4. Highlight the entry for the device that you want to update and click **Change**.
5. Set **IP Address Type** to **Static**.

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

6. Enter an unused IP address that is valid on your network in the **IP Address** field. You may need to contact your Network Administrator to get this address.
7. Enter the network's **Subnet Mask**.
8. Enter the network's **Gateway IP Address**, if necessary. You may need to contact your Network Administrator to get this address. You need to enter the default gateway address (169.254.128.133) only if the device and the TFTP server are separated by a router.
9. By default, the IP address of the TFTP server is provided.
10. By default, the image file name is provided.
11. Click **OK**. The device will reboot and the download starts automatically.

12. Click **OK** when prompted to return to the ***Scan List*** screen after the device has been updated successfully.



MAC Address	System Name	IP Address	Uptime	System Description
00-e0-0c-00-7d-09	System-Name	169.254.128.132	0 d 6 h 54 m 43 s	ORiNOCO AP-8100-WD v4.X.Y(Build-Number) SN-..

Figure 8-16 Device in Bootloader Mode - ScanTool

13. Click **Cancel** to close the ScanTool.

When the download process is complete, start configuring the device.

8.4.3.2 Download a New Image using the Bootloader CLI

: Downloading new image using Bootloader CLI (via a serial interface), is not applicable for AP-8100.

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

You must also connect the device to a computer with a standard serial cable and use a terminal client. From the terminal, enter the CLI commands to set the IP address of the device and to download the device image. Follow the following steps, to download a new image using the Bootloader CLI.

Step 1: Preparing to Download the device image

Before starting, you need to know the device IP Address, Subnet Mask, the TFTP Server IP Address, and the device image file name. Make sure the TFTP server is running and configured to point to the default directory containing the image to be downloaded.

Step 2: Download Procedure

1. Download the latest software from http://support.proxim.com.
2. Copy the latest software updates to your TFTP server's default directory.
3. Connect the device serial port to your computer's serial port.
4. Open your terminal emulator program and set the following connection properties:
   - **Com Port:** COM1, COM2 and so on, depending on your computer
   - **Baud Rate:** 115200
   - **Data Bits:** 8
   - **Stop Bits:** 1
   - **Flow Control:** None
   - **Parity:** None
5. The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Starting ScanTool interface, press any key to enter CLI 5".** After this message appears, press any key. Now the bootloader prompt appears as below:

   ```
   Bootloader=>
   ```

: *Optionally, you can enable* **Send line ends with line feeds (CTRL+F)** *under* **File** > **Properties** > **Settings** > **ASCII Setup***, to allow the Terminal Emulator program send a line return at the end of each line of code.*

Enter the following CLI commands:

```
Bootloader=> show(to view configuration parameters and values)
Bootloader=> set ipaddr <Access Point IP Address>
Bootloader=> set serverip <TFTP Server IP Address>
Bootloader=> set filename <Device Image File Name, including file
             extension>
Bootloader=> set gatewayip <Gateway Ip Address>
Bootloader=> set netmask <Network Mask>
Bootloader=> set ipaddrtype static
Bootloader=> show (to confirm your new settings)
```

Example:

```
Bootloader=> show
Bootloader=> set ipaddr 169.254.128.132
Bootloader=> set serverip 169.254.128.133
Bootloader=> set filename apimage_proxim.sei
Bootloader=> set gatewayip 169.254.128.133
Bootloader=> set netmask 255.255.255.0
Bootloader=> set ipaddrtype static
Bootloader=> show
Bootloader=> reboot
```

6. The device will reboot and then download the image file.
7. When the download process is complete, configure the device.

8.4.4 Setting IP Address by Using a Serial Port

: *'Setting IP Address by using a Serial Port', is not applicable for AP-8100.*

Use the following procedure to set an IP address for the device by using the CLI. The Network Administrator typically provides the device IP address.

- **Hardware and Software Requirements**
  - Standard serial (RS-232) cable (not included in the Product Package).
  - ASCII Terminal software.
- **Attaching the Serial Port Cable**
  - Connect one end of the serial cable to the device and the other end to a serial port on your computer.
  - Power on the computer and the device.
- **Initializing the IP Address by using CLI**

  After connecting the cable to the serial port, you can use the CLI to communicate with the device. CLI supports the most-generic terminal emulation programs. In addition, many web sites offer shareware or commercial terminal programs that you can download. Once the IP address has been assigned, you can use the HTTP interface or the Telnet to complete the configuration.

Follow the following steps to assign an IP address to the device:

1. Open your terminal emulation program and set the following connection properties:
   - **Com Port**: COM1, COM2 and so on depending on your computer
   - **Baud Rate:** 115200
   - **Data Bits**: 8
   - **Stop Bits:** 1
   - **Flow Control:** None
   - **Parity:** None
2. The terminal display shows Power On Self Tests (POST) activity, and then displays the software version. It prompts you to enter the CLI username and password. The commands to enter the username and password are as follows.

   ```
   Username: admin
   Password:
   ```

   This process may take up to 90 seconds.
3. Enter the CLI Username and password (By default username is **admin** and password is **public**). The terminal displays a welcome message and then the CLI Prompt.
4. Enter the following CLI command for the current IP Address of the device.

   ```
   AP-00:7D:09>show ip
   ```

5. Change the IP address and other network values by using the following CLI commands (use your own IP Address and Subnet Mask)

   ```
   AP-00:7D:09>enable
   AP-00:7D:09#configure
   AP-00:7D:09(config)# network
   AP-00:7D:09(config-net)# ip
   AP-00:7D:09(config-net-ip)# ethernet-ip-table rowedit 1
   Possible completions:
   <[Enter]>     Execute this command
   address-type  Configure the Address type
   ipaddress     IP Address of the network interface
   mask          subnet mask of the network interface

   AP-00:7D:09(config-net-ip-etherip)# rowedit 1 ipaddress <IP Address>
   Changes in Ethernet IP Address requires reboot.
   AP-00:7D:09(config-net-ip-etherip)# rowedit 1 mask <Subnet Mask>
   Changes in Ethernet Subnet mask requires reboot.
   AP-00:7D:09(config-net-ip-etherip)# rowedit 1 address-type <static/dynamic>
   Changes in Ethernet IP Address Type requires reboot.
   AP-00:7D:09(config-net-ip-etherip)#exit
   AP-00:7D:09(config-net-ip)# default-gateway <IP Gateway>
   AP-00:7D:09(config-net-ip)#exit
   AP-00:7D:09(config-net)#exit
   ```

   For Commit and Reboot,

```
AP-00:7D:09(config)#commit 1
Committing in progress, may take few seconds....
Configuration Applied Successfully.

AP-00:7D:09(config)#reboot 1
```

6. After the device reboots, verify the new IP address by reconnecting to the CLI. Alternatively, you can ping the device from a network computer to confirm that the new IP address has taken effect.
7. When a proper IP address is set, use the HTTP interface or Telnet to configure, rest of the operating parameters of the device.

: For AP-8100, accessing CLI thorough serial interface is not applicable as it does not have a serial port. However, you can access the CLI via your LAN (switch, hub and so on), internet, or with an ethernet cable connected directly to your computer's ethernet Port.

8.5 Application Specific Troubleshooting

8.5.1 RADIUS Authentication Server

If you have enabled RADIUS Authentication on the device, make sure that your network's RADIUS servers are operational. Otherwise, clients will not be able to log onto the device. There are several reasons for the authentication server's services to be unavailable. To make it available,

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

Make sure the RADIUS authentication server RAS setup matches the device.

8.5.2 TFTP Server

The "Trivial File Transfer Protocol" (TFTP) server allows you to transfer files across a network. You can upload configuration files from the device for backup and you can download configuration files or new software images.

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

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the device Image.
- Make sure you have the proper TFTP server IP Address, the proper device image file name, and that the TFTP server is connected.

Make sure the TFTP server is configured to both Transmit and Receive files (on the TFTP server's **Security** tab), with no automatic shutdown or time-out (on the **Auto Close** tab).

Frequency Domains and Channels

A

This chapter lists the available channels for the following frequencies, supported by the AP device for specific country codes:

Available Channels

Available channels vary based on radio, country, and frequency band. To verify which channels are available for your product locate the product model number on the underside of the device or on the unit box. Tabulated below are the details on the available channels of channel bandwidths 2.4 GHz and 5 GHz, for different country codes.

2.4 GHz CHANNELS				
Region (SKU)	**Country**	**20 MHz**	**40 PLUS MHz**	**40 MINUS MHz**
NORTH AMERICA	**Canada** **United States**	1 to 11 (2412 ~ 2462)	1 to 7 (2412 ~ 2442)	5 to 11 (2432 ~ 2462)
WORLD	**Taiwan**	1 to 11 (2412 ~ 2462)	1 to 7 (2412 ~ 2442)	5 to 11 (2432 ~ 2472)
	Belarus **Egypt** **Israel** **Russia** **Serbia** **Montenegro**	1 to 13 (2412 ~ 2472)	1 to 9 (2412 ~ 2452)	5 to 13 (2432 ~ 2472)
	Mexico	1 to 13 (2412 ~ 2472)	1 to 9 (2412 ~ 2452)	5 to 13 (2432 ~ 2472)
	India	1 to 11 (2412 ~ 2462)	1 to 7 (2412 ~ 2442)	5 to 11 (2432 ~ 2472)
	Australia **New Zealand**	1 to 13 (2412 ~ 2472)	1 to 9 (2412 ~ 2452)	5 to 13 (2432 ~ 2472)

2.4 GHz CHANNELS				
Region (SKU)	**Country**	**20 MHz**	**40 PLUS MHz**	**40 MINUS MHz**
	Argentina **Austria** **Belgium** **Brazil** **Bulgaria** **China** **Cyprus** **Czech Republic** **Denmark** **Estonia** **Finland** **France** **Germany** **Greece** **Hong Kong** **Hungary** **Iceland** **Ireland** **Italy** **Korea** **Latvia** **Liechtenstein** **Lithuania** **Luxembourg** **Malaysia** **Malta** **Netherlands** **Norway** **Poland** **Portugal** **Romania** **Singapore** **Slovakia** **Slovenia** **South Africa** **Spain** **Sweden** **Switzerland** **UK**	1 to 13 (2412 ~ 2472)	1 to 9 (2412 ~ 2452)	5 to 13 (2432 ~ 2472)
	United States	1 to 11 (2412 ~ 2472)	1 to 7 (2412 ~ 2452)	5 to 11 (2432 ~ 2472)
JAPAN	**Japan**	1 to 13 (2412 ~ 2472)	1 to 9 (2412 ~ 2452)	5 to 13 (2432 ~ 2472)

2.4 GHz CHANNELS				
Region (SKU)	**Country**	**20 MHz**	**40 PLUS MHz**	**40 MINUS MHz**
Europe	**Austria** **Belgium** **Bulgaria** **Cyprus** **Czech Republic** **Denmark** **Estonia** **Finland** **France** **Germany** **Greece** **Hungary** **Iceland** **Ireland** **Italy** **Latvia** **Liechtenstein** **Lithuania** **Luxembourg** **Malta** **Netherlands** **Norway** **Poland** **Portugal** **Romania** **Slovakia** **Slovenia** **Spain** **Sweden** **Switzerland** **United Kingdom**	1 to 13 (2412 ~ 2472)	1 to 9 (2412 ~ 2452)	5 to 13 (2432 ~ 2472)

5 GHz CHANNELS				
Region (SKU)	**Country**	**20 MHz**	**40 PLUS MHz**	**40 MINUS MHz**
NORTH AMERICA	**Canada** **United States***	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660)* 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660)* 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680)* 153 (5765) 161 (5805)
	** AP-8100 does not support the channels 132 (20 and 40 Plus MHz) and 136 (40 Minus MHz) of United States.*			
WORLD	**Argentina**	52 (5260) 56 (5280) 60 (5300) 64 (5320) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	52 (5260) 60 (5300) 149 (5745) 157 (5785)	56 (5280) 64 (5320) 153 (5765) 161 (5805)

	Brazil	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680) 153 (5765) 161 (5805)
	Belarus	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680)
	China	149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	149 (5745) 157 (5785)	153 (5765) 161 (5805)

	Egypt **Israel**	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320)	36 (5180) 44 (5220) 52 (5260) 60 (5300)	40 (5200) 48 (5240) 56 (5280) 64 (5320)
	Hong Kong	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 153 (5765) 161 (5805)
	India	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 153 (5765) 161 (5805)
	Korea	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 116 (5580) 124 (5620) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 120 (5600) 128 (5640) 153 (5765) 161 (5805)

		120 (5600) 124 (5620) 128 (5640) 149 (5745) 153 (5765) 157 (5785) 161 (5805)		
	Mexico	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 153 (5765) 161 (5805)
	New Zealand **Australia**	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680) 153 (5765) 161 (5805)
	Russia	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 132 (5660) 149 (5745)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 136 (5680) 153 (5765)

		60 (5300) 64 (5320) 132 (5660) 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805)	157 (5785)	161 (1805)
	Serbia Montenegro	100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700)	100 (5500) 108 (5540) 132 (5660	104 (5520) 112 (5560) 136 (5680)
	Singapore	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500)* 104 (5520)* 108 (5540)* 112 (5560)* 116 (5580)* 120 (5600)* 124 (5620)* 128 (5640)* 132 (5660)* 136 (5680)* 140 (5700)* 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500)* 108 (5540)* 116 (5580)* 124 (5620)* 132 (5660)* 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520)* 112 (5560)* 120 (5600)* 128 (5640)* 136 (5680)* 153 (5765) 161 (5805)
	** AP-8000 does not support the channels 100 (5500) to 140 (5700).*			

	South Africa	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680) 153 (5765) 161 (5805)
	Taiwan	56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	60 (5300) 100 (5500) 108 (5540) 132 (5660) 149 (5745) 157 (5785)	64 (5320) 104 (5520) 112 (5560) 136 (5680) 153 (5765) 161 (5805)
	Austria **Belgium** **Bulgaria** **Cyprus** **Czech Rep** **Denmark** **Estonia** **Finland** **France** **Germany** **Greece**	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680)

	Hungary **Iceland** **Ireland** **Italy** **Latvia** **Liechtenstein** **Lithuania** **Luxembourg** **Malta** **Netherlands** **Norway** **Poland** **Portugal** **Romania** **Slovakia** **Slovenia** **Spain** **Sweden** **Switzerland** **UK**	112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700)		
	United States	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700) 149 (5745) 153 (5765) 157 (5785) 161 (5805) 165 (5825)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660) 149 (5745) 157 (5785)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680) 153 (5765) 161 (5805)
JAPAN	**Japan**	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520)

		56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 120 (5600) 124 (5620) 128 (5640) 132 (5660) 136 (5680) 140 (5700)	108 (5540) 116 (5580) 124 (5620) 132 (5660)	112 (5560) 120 (5600) 128 (5640) 136 (5680)
EUROPE	**Austria** **Belgium** **Bulgaria** **Cyprus** **Czech Republic** **Denmark** **Estonia** **Finland** **France** **Germany** **Greece** **Hungary** **Iceland** **Ireland** **Italy** **Latvia** **Liechtenstein** **Lithuania** **Luxembourg** **Malta** **Netherlands** **Norway** **Poland** **Portugal** **Romania** **Slovakia** **Slovenia** **Spain** **Sweden** **Switzerland** **United Kingdom**	36 (5180) 40 (5200) 44 (5220) 48 (5240) 52 (5260) 56 (5280) 60 (5300) 64 (5320) 100 (5500) 104 (5520) 108 (5540) 112 (5560) 116 (5580) 132 (5660) 136 (5680) 140 (5700)	36 (5180) 44 (5220) 52 (5260) 60 (5300) 100 (5500) 108 (5540) 132 (5660)	40 (5200) 48 (5240) 56 (5280) 64 (5320) 104 (5520) 112 (5560) 136 (5680)

Bootloader CLI and Scan Tool

B

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

: For AP-8100, you can download the software image using ScanTool, as the Bootloader CLI mode (only accessible through the serial interface) is not applicable to AP-8100.

This interface is only accessible through the serial interface, and used when:

- The device does not contain a software image
- An existing image is corrupted
- An automatic (default) download of image over TFTP has failed

The Bootloader CLI supports the following commands.

- **factory_reset**: Restores the factory settings
- **help**: Prints online help
- **reboot**: Reboots the device
- **set**: Sets the parameters
- **show**: Shows the parameters

The Bootloader CLI supports the following parameters (for viewing and modifying).

- **ipaddr:** IP Address
- **systemname:** System Name
- **gatewayip:** Gateway IP Address
- **serverip:** Server IP Address
- **ipaddrtype:** IP Address Type
- **netmask:** Net Mask
- **filename:** Image file name (including the file extension)

If the Bootloader fails to load the firmware from flash, it tries to get the firmware from the network. While trying to get firmware from the network, the device should be powered on by using ethernet interface. The default configuration of the Bootloader parameters are as follows:

Parameter	Value
ipaddr	169.254.128.132
netmask	255.255.255.0
gatewayip	169.254.128.133
systemname	systemname
serverip	169.254.128.133
filename	imagename
ipaddrtype	dynamic

To load the firmware from the Network

- Use the **show** command to view parameters and their value, and use the set command to set the parameters value.

To get the IP parameters dynamically for loading the firmware

1. Set the ipaddrtype to dynamic
2. Run the BOOTP and TFTP Servers and reboot the device

When the device reboots, the device gets the IP Address and Boot filename from the BOOTP server. You need not change any of the above default bootloader parameters. After BOOTP succeeds, the device initiates a TFTP request with the filename it gets from BOOTP.

To load the firmware by using Static IP parameters

1. Use the **set** command to set the IP parameters like 'ipaddr', 'serverip', 'filename' and also set the parameter 'ipaddrtype' to static.
2. Run the TFTP Server and also reboot the unit.

When the device reboots, the TFTP request is initiated with the value taken from the parameter "filename". This request is sent to the IP address which is set as "serverip". Please note that the TFTP Server should be reachable to the device.

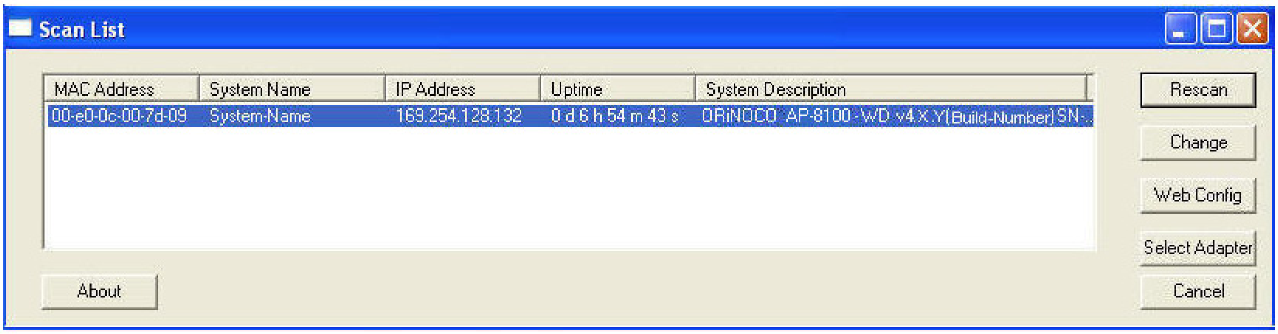
ScanTool

To access the device with ScanTool, the host running the ScanTool should also be in the same network as the device. The ScanTool broadcast requests will be discarded by the routers if the device and the host running the ScanTool are in the different network.

A device in Bootloader can be recognized by looking at the system description. If the system description does not contain any build number in braces, conclude that the device is in Bootloader mode.

For example:

ORiNOCO® AP-8XXX	: name of the board (Example: Name of the board for AP-8100 shall be ORiNOCO® AP-8100)
WD	: Regulatory Domain
v4.X.Y	: Firmware Version
SN-08UT41110039	: Serial number of the device
BL-V1.0.2	: Bootloader Version



Scan List

MAC Address	System Name	IP Address	Uptime	System Description
00-e0-0c-00-7d-09	System-Name	169.254.128.132	0 d 6 h 54 m 43 s	ORiNOCO AP-8100 - WD v4.X.Y(Build-Number) SN-..

Figure B-1 Scan Tool

00-e0-0c-00-7d-09	: Device's MAC Address.
169.254.128.132	: Device's IP Address
0d 6h 54m 43s	: System Uptime.

System-Name : Device’s System-Name.

ASCII Character Chart

C

You can configure WEP Encryption Keys in either Hexadecimal or ASCII format. Each ASCII character corresponds to two hexadecimal digits.

The WEP Encryption Keys include ASCII characters consisting of 0-9, A-F, a-f (case sensitive), and punctuation marks. Tabulated below are the ASCII characters along with their Hexadecimal equivalent.

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

Frequently Asked Questions (FAQs)

D

This chapter covers the Frequently Asked Questions (FAQs) on the following topics:

- Link Integrity
- Rogue Scan
- Wireless Distribution Systems (WDS)
- RADIUS VLAN
- Packet Forwarding

❗: All the interface (radio) 2 parameters discussed in this chapter are applicable only to a dual-radio device.

Link Integrity

Q. What will happen to a WDS link if the wireless interface (radio) goes down due to link integrity?

WDS link will remain unaffected, if the wireless interface goes down due to link integrity. Let's say, you have 6 VAPs and 2 WDS links within the same wireless interface. If the connectivity to the server nodes (listed in the link integrity server configuration table) is lost, then all the 6 VAPs will go down but the WDS link is not affected.

Q. What are the messages generated in Event Logs and Syslog, while the radio is down/up due to the link integrity?

"Wireless Interface is down due to link non availability" is the message generated, once the interface is down and "Wireless Interface is up due to Link availability" is the message generated when the interface is up and server nodes are reachable. Check Event Log and SysLog for the messages generated.

Rogue Scan

Q. Does the Rogue Scan feature on AP device detect non Wi-Fi interferences?

No, Rogue Scan feature on the AP device, detects only the sources of Wi-Fi interference.

Q. What is the maximum number of entries supported in the Rogue Scan results page?

For **Current channel scan** : 32 entries for all device types detected (10 entries for each device type)
For **All channel scan** : 512 entries for all device types detected (100 entries for each device type)

Q. Can I perform the background Rogue Scan on both the radios (where, radio 1 = 5 GHz and radio 2 = 2.4 GHz) at the same time?

Yes. You can perform the Rogue Scan on both the wireless interfaces (radios) at the same time.

Q. Does Rogue Scan apply on a WDS enabled radio?

Yes. Rogue Scan can be applied on a WDS enabled radio.

Q. Does Rogue Scan apply on the adjacent channels, if it is set to Current Channel Scan?

No. Rogue Scan is not applied on the adjacent channels, if it is set to Current Channel Scan.

Q. Where I can find the Rogue Scan results?

In the Web (HTTP) Interface, navigate to **Monitor** -> **Rogue Scan** -> **Interface**.

Q. How does the Rogue Scan feature on AP device, detect the Wi-Fi interferences?

i) For AP Devices: AP Devices are detected based on beacons, which has IBSS field set to 0
ii) For STA Devices: STAs (Stations) are detected based on data packets which has TO DS bit=1.

: All probe request packets are considered as STAs.

iii) For WDS Devices: WDS Devices are detected based on data packets which has 4 address format (with 2 MAC address in the header).
iv) For ADHOC Devices: ADHOC Devices are detected based on beacons, which has IBSS field set to 1.

Q. If the radio is configured in 5GHz and Rogue Scan is set to All Channel Scan, then does the Rogue Scan feature on the AP device scan a 2.4GHz channel?

- **For AP-800/AP-8000:** Yes. Rogue Scan is applicable on both 2.4 GHz and 5GHz channels in All Channel scan mode, irrespective of the frequency band configured on the radio.
- **For AP-8100:** No. Rogue Scan feature will only scan 5GHz channels on radio 1 and 2.4 GHz channels on radio 2.

Q. How to enable Rogue Scan on the AP device?

Navigate to **Configuration** -> **Wireless Interface** -> **Properties** -> **Rogue Scan Status**. Select “**Current Channel Scan**” or “**All Channel Scan**”

Wireless Distribution Systems (WDS)

Q. By using AP-8000 / AP-8100, can I form the WDS link on both the radios at the same time?
Yes. You can form a WDS link on both the radios at the same time by configuring a VAP type in WDS mode (WDS-END-A/END-B), on both the radios. But we recommend keeping both the radios in different operational modes.

Q. How many WDS links does the AP device support?
The AP device supports a maximum of 6 WDS downlinks (with directly connected nodes) and minimum of 2 hops in a tree type topology.

Q. How to make sure that the WDS link is formed successfully and check the statistics?
To make sure that the WDS link is formed successfully, navigate to **Monitor** -> **Station Statistics**. Check the detailed statistics of entries with the VAP type set to “WDS”.

Q. Does WDS depend on the management VLAN ID?
No. WDS is independent of the management VLAN ID. You can form a WDS link between two AP Devices with same or different Management VLAN ID.

Q. How different is WDS-11n mode from WDS-legacy mode, apart from data rate and throughput?	
• In **WDS-Legacy** mode, management frames are not exchanged during the link establishment. Data is directly forwarded to the peer MAC address. • This mode does not support QoS or frame aggregation.	• In **WDS-11n** mode, management frames are exchanged during the link establishment. • This mode supports QoS, frame aggregation and 11n-MIMO technology.

Q. Can I configure the VAP enabled in WDS mode and VAP enabled in AP mode, on the same radio?
Yes. You can configure both the VAP types on same radio. Below is the set up that illustrates configuring both, VAP in WDS and VAP in AP modes on same radio. You need to create two VAPs on AP2, one for WDS and one for AP mode. (WDS-ENDA) **AP1** ---------- (WDS-ENDB) **AP2** (AP VAP) 1st VAP 1st VAP 2nd VAP A WDS link is established between AP1 VAP and AP2 VAPs.

Q. What should I do if the WDS link is not getting established?

- Make sure the operational mode and frequency configured is same for both the devices
- Check whether the peer MAC address added is correct.
- Configure valid and same security settings and keys on both the devices.
- Both the devices should be within the vicinity.
- Check the VAP type configuration on both devices. (One should be WDS-END-A and the other should be WDS-END-B or both should be set to WDS-Legacy in case of a legacy WDS link)

Q. At what rate, is the multicast traffic transmitted from a VAP enabled in WDS mode?

Multicast traffic is transmitted at a unicast rate upto 300Mbps, over the WDS-11n link.

Q. How to establish a WDS link, by using both the radios simultaneously? (Applicable only for a dual-radio device)

Below setup illustrates how to establish a WDS link, by using both the radios.

```
          Radio1  <-  AP1 ->   Radio2
     (WDS-ENDA)     /     \     (WDS-ENDA)
        1st VAP       /         \      1st VAP
                     /            \
      5GHz link  /                \  2.4GHz link
                 /                    \
(WDS-ENDB) AP2                  AP3 (WDS-ENDB)
   1st VAP                                  1st VAP
```

Here, based on the channel bandwidth supported, a 5GHz and a 2.4GHz WDS links are established on both Radio 1 and Radio 2 of AP1, simultaneously.

Q. Do I need to configure only the corresponding VAPs at both the radios, to establish a WDS link?

No, it is not necessary that you use only the corresponding VAPs to form a WDS link. For example, you can use VAP 1 at AP1 and VAP 8 at AP2, to establish a WDS link. Add the peer MAC address of VAP 8 in AP1 and add the peer MAC address of VAP 1 in AP2.

Q. Can I form a WDS link between an AP-400/7000 device and an AP-800/8000/8100 device?

Yes. You need to configure a 11a or 11g operational mode (WDS-Legacy mode) on the AP-800/8000/8100 device to establish a WDS link with AP-400/7000 device.

Q. How to create 2 hop WDS link?

```
 AP1 (WDS-ENDA) -------- (WDS-ENDB) AP2 (WDS-ENDA) -------- (WDS-ENDB) AP3
        1st VAP                  1st VAP             2nd VAP                  1st VAP
```

You need to create two VAPs on AP2 and set both the VAPs in WDS mode.

Q. How to establish multiple WDS downlinks?

Below setup illustrates how to establish two WDS downlinks. Here, the first link is established between VAP 1 of AP1 and VAP 1 of AP2, second link is established between VAP 2 of AP1 and VAP 1 of AP3.

```
     (WDS-ENDA)  AP1  (WDS-ENDA)
       1st VAP     /      \     2nd VAP
                  /         \
                /             \
(WDS-ENDB) AP2          AP3 (WDS-ENDB)
   1st VAP                         1st VAP
```

Q. What are the expected throughput values for WDS?

Tabulated below are the throughput values, considering that the WDS link is established with maximum data rate.

No. of Hops	20 MHz	40MHz
1st Hop	60 Mbps	130 Mbps
2nd Hop	30 Mbps	60 Mbps
3rd Hop	10 Mbps	25 Mbps

Q. What is the effect on WDS, if the link integrity is enabled and the *Link Status* is down?

If the link integrity is enabled and the *Link Status* is down, then AP device disables all the VAPs enabled in AP mode only but does not interrupt the traffic on ethernet and WDS link.

Q. Does WDS support Auto Channel Selection (ACS)?

No. WDS does not support Auto Channel Selection (ACS). You cannot enable the Auto Channel Selection (ACS), when a VAP is configured in WDS mode.

Q. Can I configure WDS on a DFS channel?

You can configure WDS on a DFS channel, but it is recommended not to use a DFS channel to establish a WDS link.

Q. How is WDS related with STP?

STP is enabled automatically when you enable a VAP in WDS mode. STP feature helps in avoiding loops in a ring topology formed by a WDS link.

RADIUS VLAN

Q. Why VLAN assignment via RADIUS is needed?

VLAN assignment via RADIUS reduces the effort of AP device, in manually configuring VLAN to a specific user. By using this feature, you can dynamically assign VLANs to wireless clients when the clients are authenticated with RADIUS server. Hence, each client can maintain its own VLAN network.

Q. What if “Tunnel-Private-Group-ID” is empty?

If the “Tunnel-Private-Group-ID” is empty, the native VLAN ID configured (if any) on the VAP is applied to the client.

Q. What is the behavior of RADIUS VLAN assignment, while sending Broadcast/Multicast traffic?

- The Broadcast/Multicast traffic being sent from an ethernet backhaul PC (associated to any VLAN or NO VLAN), reaches the wireless clients irrespective of the VLANs applied to them.
- The Broadcast/Multicast traffic being sent from the wireless client (say with VLAN ID = VLAN 100) reaches the other wireless client(s) (irrespective of the VLANs applied) and ethernet backhaul PC associated to same VLAN (that is 100) or NO VLAN (but not to the PC associated to other VLANs).

Q. How is management VLAN ID related to RADIUS VLAN assignment?

If the management VLAN ID is configured, the RADIUS server should also be in the same VLAN to receive the request packet re-directed by the AP device.

Q. How to make sure that the clients are assigned with a correct VLAN ID via RADIUS server?

Go to **Monitor** -> **Station Statistics** -> corresponding client and click the “show” tab, which details all the parameters including the VLAN ID assigned.

Q. How many number of clients can be assigned with a VLAN Id via a RADIUS server?

There is no limitation on the number of clients assigned with the VLAN ID via a RADIUS server. As a standard, AP device supports upto 128 clients per radio.

Packet Forwarding

Q. In what scenarios Packet Forwarding can be used?
Packet forwarding feature is useful for public wireless networks where the clients cannot communicate with each other but should be able to access internet. This feature can also be used to sniff all the packets by sending the wireless packets to the configured gateway, for security reasons.

Q. Can I access an Access Point directly from my wireless client, if Packet Forwarding is enabled?
Yes. You can access an Access Point from your wireless client. The traffic destined to the MAC address of an Access point will not be forwarded to the gateway.

Q. What will happen to the downlink traffic?
All the traffic from AP Device to wireless clients (downlink) will follow the regular Path, it will not go through the configured gateway.

Q. What will happen if I configure uplink port in WDS mode and disable a WDS link?
If Uplink port is configured as WDS, and later if the WDS link is disabled, then the uplink port should be re-set to AUTO.

Q. What is default mode of Packet forwarding feature and is it a re-bootable parameter?
By default, Packet forwarding feature is disabled Configured settings take effect immediately after committing the changes. Reboot is not required.

Glossary

E

A	
Access point	A wireless network transceiver or "base station" hub, often used to connect a local area network to one or more wireless devices. An access point (also called AP) can provide a communication link to a wired local area network also.
ADHOC	A ‘client’ setting for a wireless local area network that allows devices connected to the network to communicate with one another directly, independent of an access point or router.
Advanced Encryption Standard (AES)	It is a symmetric-key encryption standard, containing three block ciphers AES-128, AES-192, AES-256. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
ARP	The Address Resolution Protocol (ARP) is intended to find the MAC address belonging to an IP address.
Authentication	The process the unit uses to decide whether a wireless client is allowed to register to an access point network or not. IEEE 802.11 specifies two forms of authentication: open system and shared key; WORP only supports shared key because of security constraints.
Authentication Server “Shared Secret”	This is a kind of password shared between the unit and the RADIUS authentication server. This password is used to encrypt important data exchanged between the unit and the RADIUS server.

B	
Basic Service Set (BSS)	A wireless network with atleast one Access Point (either connected to a wired network infrastructure or a wireless backhaul) and a set of wireless devices forms a **Basic Service Set (BSS)**.
Boolean Operators	Boolean operators define the relationships between words or groups of words. – **AND**: Narrow search and retrieve records containing all of the words it separates. – **OR**: Broaden search and retrieve records containing any of the words it separates. The | can be used instead of 'or' (e.g., 'mouse | mice | rat' is equivalent to 'mouse or mice or rat'). *: Depending on how the Boolean Operator AND is used with the Keyword Field (KW), results may be slightly different.*
BPDU Packets	A spanning tree protocol (STP) message unit that describes the attributes of a switch port such as its MAC address, priority and cost to reach. BPDUs enable switches that participate in a spanning tree protocol to gather information about each other.

B	
Bridge	An interface connecting a local area network to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.
Broadcast	Broadcast traffic is a large series of broadcast packets (most often caused by wrong network configuration) that severely impact the network performance.
Broadband	In data communications, a "broadband connection" is a connection with a high speed of data transfer, fast enough to support a video streaming.
Broadcast SSID (BSSID)	BSSID refers to the MAC address of the wireless client within an Access Point (AP) coverage area.

C	
Client IP Address Pool	This a pool of IP addresses from which the unit can assign IP addresses to clients, which perform a DHCP Request.
Carrier Sense Multiple Access with Collision Avoidance (CSMA / CA)	It is a wireless network multiple access method in which: • A carrier sensing scheme is used. • A node wishing to transmit data has to first listen to the channel to determine whether or not another node is transmitting on the channel within the wireless range. If the channel is sensed "idle," then the node is permitted to begin the transmission process. If the channel is sensed as "busy," the node defers its transmission for a random period of time. Once the transmission process begins, it is still possible for the actual transmission of application data to not occur.
Contention Window (CW)	Contention Window is a set of time slots, that helps in configuring the random backoff timer value, that should be within the Contention Window range (i.e) from CWmin to CWmax, where CWmin varies between each of the queues. See Access Category Every wireless client waits for this random backoff timer value set, to access the wireless medium. This avoids collision over the medium, giving an equal chance to every wireless station on the network to access the medium.
Cyclic Redundancy Check (CRC)	A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents; on retrieval the calculation is repeated, and corrective action can be taken against presumed data corruption if the check values do not match.

D	
Digital Subscriber Line (DSL)	Digital subscriber line is a technology that provides internet access by transmitting digital data over the wires of a local telephone network.
Domain Name Server (DNS)	A domain name server is an Internet service that translates domain names into IP addresses. For example, www.ietf.org is translated into 4.17.168.6.
Downstream / Downlink	Downstream means a data stream from the central part of the network to the end user. Also, refer Upstream / Uplink.
Dual-Band	Dual-band refers to a device's ability to function on two different frequency bands.
Dynamic Frequency Selection (DFS)	DFS helps you select the operating frequency that does not interfere with the RADAR signals, by continuously detecting the range of operating frequencies with a RADAR interference.
Dynamic Host Configuration Protocol (DHCP)	Dynamic Host Configuration Protocol (DHCP) is a method to dynamically assign IP addresses. If DHCP is enabled, the device or computer broadcasts a request that is answered by a DHCP Server.
Dynamic IP address	An IP address assigned to a client, each time the client connects to the network. The dynamic IP address is configured by the DHCP server and can be different each time the client connects to the network.

E	
Extensible Authentication Protocol (EAP)	EAP is an authentication framework providing the transport and usage of keying material and parameters generated by EAP methods. EAP is not a wire protocol, instead it only defines the message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.
Encryption	Encryption is a means of coding data with a key before sending it across a network. The same key must be used to decode the information at the receiver. This way, it prevents unauthorized access to the data that is sent across the network.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted, so it can be securely shared among members of the same network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

G	
Group	A group is a logical collection of network parameters. For example, the System Group is composed of several parameters and tables giving system information of the unit. All items for a group are grouped under one tab of the Web Interface and start with the same prefix for the command line interface.

H	
Hexadecimal	A numeral system with a radix or base, of 16. It uses sixteen distinct symbols, 0–9 to represent values zero to nine and A, B, C, D, E, F to represent values ten to fifteen. Each hexadecimal digit represents four binary digits (bits).
HTTP	Hypertext Transfer Protocol (HTTP) is the protocol to transport Web pages. When you access the Internet with your browser, the HTTP protocol is used for data transport (http://www.Tsunamiwireless.com). When you access the unit by using the Web Interface, HTTP is used to transport the information. HTTPS is the Secure Hypertext Transfer Protocol.

I	
ICMP	Internet Control Message Protocol (ICMP) is used by computers and devices to report errors encountered during processing packets, and to perform other IP-layer functions, such as diagnostics (‘ping’).

L	
LAN	A Local Area Network (LAN) is a network of limited size to which computers and devices can connect so that they can communicate with each other.
License File	A license file is used to enable certain features of the unit. The unit already has a license file when it is shipped. When more features become available, you can purchase a license file and download it to the unit to enable these additional features.

M	
MAC Address	A MAC (Media Access Control) address is a globally unique network device address, which is hardware bound. It is used to identify a network device in a LAN. A MAC address is represented by six two-digit hexadecimal numbers (0 - 9 and A - F) separated by colons: for example 00:02:2D:47:1F:71 and 00:D0:AB:00:01:AC.
Management Information Base (MIB)	A Management Information Base (MIB) is a formal description of a set of network objects that can be managed with the Simple Network Management Protocol (SNMP). A MIB can be loaded by a management application so that it knows the unit specific objects.
MPDU Packets	MPDU stands for MAC Protocol Data Unit. MPDUs are the fragmented units of MSDUs.
MSDU	MSDU stands for MAC Service Data Unit. The MSDU is that unit of data that is received from the LLC sub-layer, which lies above the MAC sub-layer in a protocol stack.
Multicast	A one-to-many communication or a delivery of a message or information to a group of destination computers simultaneously in a single transmission.

N	
NETBIOS	It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
Network Address Translation	Network Address Translation is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to end hosts.
Network Mask	See Subnet Mask

O	
Orthogonal Frequency Division Multiplexing (OFDM)	OFDM is a frequency-division multiplexing (FDM) scheme, a method of encoding digital data on multiple carrier frequencies. A large number of closely spaced orthogonal sub-carrier signals are used to carry data. The data is divided into several parallel data streams or channels, one for each sub-carrier, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

P	
Pass Phrase	A text string used for WPA security on a wireless network. A passphrase may contain up to 8 to 64 alphanumeric characters, including spaces and other special characters.
Ping	Ping is a basic Internet program that lets you verify if a particular computer or device with a certain IP address is reachable. If the computer or device receives the ping packet, it responds to it, which gives the ping program the opportunity to display the round-trip time.
Port Number	TCP and UDP provide an address mechanism, the **port number**, for identifying different applications communicating from the same IP address. Thus an active Web browser and an independently active mail program operating from the same IP location would typically use different port numbers so that packets are correctly delivered to specific applications.
Probe Request	A wireless client sends a probe request frame when it needs to obtain information from another wireless client or an access point. For example, a radio NIC would send a probe request to determine which access points are within range.
Probe Response	A wireless client or an access point will respond to the probe request with a probe response frame, containing capability information, supported data rates, etc.

Q	
QoS	The Quality of Service (QoS) feature is based on the 802.16 standard and defines the classes, service flows, and packet identification rules for specific types of traffic. The main priority of QoS is to guarantee a reliable and adequate transmission quality for all types of traffic under conditions of high congestion and bandwidth over-subscription.

R	
RADIUS Server	Remote Authentication Dial In User Service (RADIUS) is a client/server networking protocol that runs in the application layer, by using UDP as transport and provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. The RADIUS server is a background process that serves the following three functions: • To authenticate users or devices before granting them access to a network • To authorize those users or devices for certain network services • To account the users for usage of the provided services.
Rogue Devices	Rogue devices include Rogue 802.11n AP devices and Rogue wireless devices (AP/STA/WDS/ADHOC), that are not authorized and secure.
RTS Frame	A node wishing to send data initiates the process by sending a Request-to-Send (RTS) frame.
RIP	Routing Information Protocol (RIP) is used between routers to update routing information so that a router automatically ‘knows’ which port to use for a certain destination IP address.
Router	Routers forward packets from one network to another based on routing information. A router uses a dynamic routing protocol like RIP or static routes to base its forwarding decision on.

S	
ScanTool	A computer program that can be used to retrieve or set the IP address of a locally connected unit.
Simple Network Management Protocol (SNMP)	A protocol used for the communication between a network management application and the devices it is managing. The network management application is called the SNMP manager and the devices it manages will have SNMP agents. Not only the unit but also almost every network device contains a SNMP agent. The manageable objects of a device are arranged in a Management Information Base, also called MIB. The Simple Network Management Protocol (SNMP) allows managers and agents to communicate for accessing these objects.
Single-Band	Single-band refers to a device's ability to function only on one frequency band.

S	
Spanning Tree Protocol (STP)	The Spanning Tree Protocol (STP) can be used to create redundant networks (“hot standby”) and to prevent loops. If enabled, spanning tree prevents loops by disabling redundant links. If a link fails, it can automatically enable a backup link.
SSH	A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.
SSL	Secure Socket Layer is a commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions.
SSID	A Service Set Identifier (also referred to as a network name) is a common name that identifies a wireless network. The identifier is attached to the wireless local area network (WLAN) and acts as an identifier when a device tries to connect to the system. A device will not be permitted to join the network unless it can provide the unique SSID. An SSID can be broadcast by the network router, allowing devices to detect it as an available network. An SSID does not supply security to the network
STP Frames	The data frames exchanged in an STP network topology are called as the STP Frames, BPDU frames being one of them.
Subnet Mask	A subnet mask is a bit mask that defines which part of an IP address is used for the network part and which part for a host (computer) number. A subnet mask is like an IP address represented by four numbers in the range 0 - 255 separated by dots. When the IP address 172.17.23.14 has a subnet mask of 255.255.255.0, the network part is 172.17.23 and the host number is 14. See also IP address.
Syslog Server	Syslog Server receives, logs, displays, and forwards syslog messages from network devices like routers.

T	
Tagged Frames	When a frame enters the VLAN-aware area of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination. These are called Tagged Frames.
TCP / IP	The TCP/IP internet-suite protocol describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination.
Telnet	Telnet is a network protocol used on the Internet or local area networks to access the command-line interface, on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration.
Topology	Topology is the physical layout of network components (cable, wireless clients, gateways, hubs, and so on).

T	
Trap	A trap is used within SNMP to report an unexpected or unallowable condition.
Trivial File Transfer Protocol (TFTP)	Trivial File Transfer Protocol (TFTP) is a lightweight protocol for transferring files that is like a simple form of File Transfer Protocol (FTP). A TFTP client is implemented on the unit. By using the upload and download commands, the unit can copy a file to or from a TFTP server. TFTP server software is provided on the product CD-ROM.

U	
Unicast	Unicast transmission is the sending of messages to a single network destination identified by a unique address.
Untagged Frames	Untagged frame is a frame which not added with a tag or has no VLAN Id associated to it.
Upload	Uploading a file means copying a file from a network device to a remote server. In case of the unit, uploading means transferring a file from the unit to a TFTP server. See also download.
Upstream / Uplink	Upstream means a data stream from the end users to the central part of the network. See also Downstream / Downlink.

V	
VLAN	The Virtual Local Area Network (VLAN) feature helps in logical grouping of network host on different physical LAN segments, which can communicate with each other as if they are all on the same physical LAN segment.

W	
WEP	The Wired Equivalent Privacy (WEP) algorithm is the standard encryption method used to protect wireless communication from eavesdropping.
Wireless Client / Station (STA)	A computer or program, connected to an access point network, that can access the wireless network, download files for manipulation, run applications, or request application-based services from a file server is called a wireless client or a wireless station (STA).
WLAN	A flexible data communication system implemented as an extension to or as an alternative for a wired LAN within a building or campus. By using electromagnetic waves, WLANs transmit and receive data over the air, minimizing the need for wired connections.

W	
WPA	Wi-Fi Protected Access is a security standard based on IEEE 802.11i specification, that provides a high level of wireless network security. It uses data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys and ensures that the keys haven't been tampered with. User authentication is performed through the Extensible Authentication Protocol (EAP), to ensure that only authorized network users can access the network.

Abbreviations

F

A	
AP	Access Point
ACL	Access Control List
ACS	Automatic Channel Selection
ACM	Admission Control Mandatory
AES	Advanced Encryption Standard
AMPDU	Aggregated MAC Protocol Data Unit
ARP	Address Resolution Protocol
ATPC	Adaptive Transmit Power Control
AIFS	Arbitration Inter-Frame Spacing
ASCII	American Standard Code for Information Interchange
B	
BBS	Bulletin Board Systems
BPDU	Bridge Protocol Data Units
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
C	
CLI	Command Line Interface
CW	Contention Window
CRC	Cyclic Redundancy Check
D	
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Disk Operating System
DSL	Digital Subscriber Line
DSCP	Differentiated Services Code Point
DTIM	Delivery Traffic Indication Map

DUT	Device Under Test
E	
EAP	Extensible Authentication Protocol
EDCA	Enhanced Distributed Channel Access
G	
Gbps	Gigabit Per Second
GPL	General Public License
GPS	Global Positioning System
H	
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I	
IANA	Internet Assigned Numbers Authority (IANA)
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ISP	Internet Service Provider
L	
LAN	Local Area Network
LGPL	Lesser General Public License
LSP	Layered Service Providers
M	
MAN	Metropolitan Area Networks
Mbps	Megabits Per Second
MD5	Message-Digest Algorithm
MIB	Management Information Base
MIMO	Multiple-input and multiple-output
MIR	Maximum Information Rate
MPDU	MAC (Media Access Control) Protocol Data Units
MSDU	MAC (Media Access Control) Service Data Units

MTU	Maximum Transmission Unit
N	
NAS	Network Attached Storage
NAT	Network Address Translation
NBD	Next Business Date
NETBIOS	Network Basic Input / Output System
NMS	Network Management System
NIC	Network Interface Card
NoACK	No Acknowledgement
O	
OFDM	Orthogonal Frequency Division Multiplexing
P	
PoE	Power Over Ethernet
POST	Power On Self Test
PSDU	Protocol Service Data Unit
PSK	Pre-Shared-Key
PVES	ProximVision ES
R	
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Services
RF	Radio Frequency
RIP	Routing Information Protocol
RMA	Return Material Authorization
RSSI	Received Signal Strength Indicator
RTS	Request-To-Send
S	
SAP	Service Advertising Protocol
SHA	Secure Hash Algorithm
SKU	Stock Keeping Unit
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell

SSL	Secure Socket Layer
STA	Wireless client / Wireless Station
STP	Spanning Tree Protocol
SSLv3	Secure Socket Layer - Version 3
SSID	Service Set Identifier
T	
TBC	Text Based Configuration
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TPID	Tag Protocol Identifier
TSLF	Time Since Last Frame
TxOP	Transmission Opportunity
U	
UDP	User Datagram Protocol
V	
VAP	Virtual Access Point
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
W	
WAN	Wide Area Networks
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Networks
WME	Wireless Multimedia Extensions
WPA	Wi-Fi Protected Access
X	
XML	Extensible Markup Language

Statement of Warranty

G

Warranty Coverage

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

Repair or Replacement

When Proxim determines that a returned product does not meet the warranted criteria during the warranty period, Proxim at its option, will either: (a) repair the defective product; (b) replace the defective product with a new or refurbished product that is at least equivalent to the original; or (c) refund the price paid for the defective product. Generally, products are repaired or replaced within thirty (30) business days of receipt of the product at a Proxim Logistical/Repair Center. The warranty period for repaired or replacement products is ninety (90) days or the remainder of the original warranty period, whichever is longer. These three alternatives constitute the customer's sole and exclusive remedy and Proxim's sole and exclusive liability under warranty provisions.

Limitations of Warranty

Proxim's warranties do not apply to any product (hardware or software) which has (a) been subjected to abuse, misuse, neglect, accident, or mishandling, (b) been opened, repaired, modified, or altered by anyone other than Proxim, (c) been used for or subjected to applications, environments, or physical or electrical stress or conditions other than as intended and recommended by Proxim, (d) been improperly stored, transported, installed, or used, or (e) had its serial number or other identification markings altered or removed.

Buyers can contact Proxim Wireless Customer Service Center either by telephone or via web. Support and repair of products that are out of warranty will be subject to a fee. Contact information is shown below. Additional support information can be found at Proxim Wireless's web site at http://support.proxim.com.

Contact technical support via telephone as follows:

USA and Canada Customers

- **Phone**: +1-408-383-7700; +1-866-674-6626
- **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

International Customers

- **Phone**: +1-408-383-7700; 0800-916475 (France); 8-800-100-9485 (Russia)
- **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

General Procedures

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

In the event the Customer Service Center determines that the problem can be corrected with a software update, Buyer might be instructed to download the update from Proxim Wireless's web site or, if that's not possible, the update will be sent to Buyer. In the event the Customer Service Center instructs Buyer to return the product to Proxim Wireless for repair or replacement, the Customer Service Center will provide Buyer a Return Material Authorization ("RMA") number and shipping instructions. Buyer must return the defective product to Proxim Wireless, properly packaged to prevent damage, shipping prepaid, with the RMA number prominently displayed on the outside of the container.

Calls to the Customer Service Center for reasons other than product failure will not be accepted unless Buyer has purchased a Proxim Wireless Service Contract or the call is made within the warranty period. After the warranty period, Technical Support is fee based (detailed in Technical Services and Support).

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

Other Information

Search Knowledgebase

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

Ask a Question or Open an Issue

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

Technical Services and Support

H

Obtaining Technical Service and Support

If you are having trouble using the Proxim product, please read this manual and the additional documentation provided with your product. If you require additional support to resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services team:

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

: Technical Support is free for the warranty period from the date of purchase.

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at http://support.proxim.com. On the Proxim eService Web Site, you can access the following services:

- **Product Download Page**: Provides quick links to product firmware, software, and documentation downloads.
- **Proxim TV Links**: A link to helpful video tutorials.
- **Knowledgebase**: A solution database of all the resolved problems. You can search by product, category, keywords, or phrases.
- **Live Chat**: Chat with a support technician on-line or request to call back at a later time.\
- **Open Ticket / Ask Question**: Submit a question to our technical support staff who will reply to you by email.
- **My Account / Tickets**: Login to check the status of your questions, modify your answer update notifications, update your personal profile, or access restricted information and features.
- **Provide Feedback**: Submit a suggestion, complaint, or other feedback about the support site.

Telephone Support

Contact technical support via telephone as follows:

USA and Canada Customers

- **Phone**: +1-408-383-7700; +1-866-674-6626
- **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

International Customers

- **Phone**: +1-408-383-7700; 0800-916475 (France); 8-800-100-9485 (Russia)
- **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

ServPak Support

To provide even greater investment protection, Proxim Wireless offers a cost-effective support program called ServPak. ServPak is a program of enhanced service support options that can be purchased as a bundle or individually, tailored to meet your specific needs. Whether your requirement is round the clock technical support or advance replacement service, we are confident that the level of support provided in every service in our portfolio will exceed your expectations.

- **Advanced Replacement of Hardware**: Can you afford to be down in the event of a hardware failure? Our guaranteed turnaround time for return to factory repair is 30 days or less. Those customers who purchase this service are entitled to advance replacement of refurbished or new hardware guaranteed to be shipped out by the Next Business Day. Hardware is shipped Monday – Friday, 8:00 AM – 2:00 PM (PST).
- **Extended Warranty**: Extend the life of your networking investment by adding 1, 2, or 3 years to your products standard warranty. This service coverage provides unlimited repair of your Proxim hardware for the life of the service contract. The cost of an extended warranty is far less than the cost of a repair providing a sensible return on your investment.
- **7x24x365 Technical Support**: This service provides unlimited, direct access to Proxim’s world-class Tier 3 technical support engineers 24 hours a day, 7 days a week, 365 days a year including Holidays. Customers who purchase this service can rest assured that their call for technical assistance will be answered and a case opened immediately to document the problem, troubleshoot, identify the solution and resolve the incident in a timely manner or refer to an escalation manager for closure.
- **8x5 Technical Support**: This service provides unlimited, direct access to Proxim's world-class technical support 8 hours a day, 5 days a week from 8:00AM - 5:00PM (PDT). Typically, technical support is provided for free for the entire time the product is covered by a Proxim warranty. Beyond this period, technical support is available at cost on a per incident basis. With the 8x5 Technical Support service, technical support will be available for the duration of the ServPak contract at no additional costs.
- **Software Maintenance**: It's important to maintain and enhance security and performance of wireless equipment and Proxim makes this easy by providing a Software Maintenance program that enables customers to access new features and functionality, rich software upgrades and updates. Customers will also have full access to Proxim's vast knowledgebase of technical bulletins, white papers and troubleshooting documents.
- **Priority Queuing Phone Support**: This service provides customers with a one hour response time for technical phone support. There is no waiting in line for those urgent calls for technical support.

Packaged Services

- 24 x 7 Enhanced ServPak
  - 24 x7 Technical Support
  - Software Maintenance
  - Advanced Hardware Replacement
  - Extends Warranty*
  - Knowledge Base Access

  - Priority Queuing

* if units are out of standard warranty

- 8 x 5 Enhanced ServPak
  - 8 x 5 Technical Support
  - Software Maintenance
  - Advanced Hardware Replacement
  - Extends Warranty*
  - Knowledge Base Access
  - Priority Queuing

* if units are out of standard warranty

ServPak Standalone Services

- Extended Warranty ServPak
- Advance Hardware Replacement ServPak

Proxim Warranty vs. ServPak Service

Service Features	ServPak	Warranty
Expert Technical Support	Technical Support, Configurations, Troubleshooting	Duration of Product Warranty. 8X5 Normal Business Hrs
Priority Queuing	Available	-
Knowledge Base Access	Available	Available
Software Upgrades	Available	-
Advance Replacement Service	8x5xNBD	-

- *Not a feature service option*

To purchase ServPak support services, please contact your authorized Proxim distributor. To receive more information or for questions on any available ServPak support options, please visit our web site http://www.proxim.com/support/servpak, call Proxim Support (For telephone numbers, see Telephone Support) or send an email to servpak@proxim.com.

Technical Support Policy

Technical Support for Current Products during Warranty Period

All Customers are entitled to free technical support for the Proxim products they purchase from Proxim's authorized resellers or distributors. Technical Support is defined as communication via the Proxim Support web site (http://support.proxim.com) and/or via telephone. This technical support will be provided for free for the entire time the product is covered by a Proxim warranty. The term of Proxim's warranty is determined according to the agreement under which the product was sold and generally varies from 3 months to 2 years depending on the product. If a Customer disagrees with Proxim's determination of warranty duration, a request for review supported by a copy of all product purchase documentation may be submitted.

Technical Support for Current Products after Warranty Period

After the warranty period, technical support on products then being sold by Proxim will be based upon one of the following three options Customers can choose:

- Customers can choose to purchase one of Proxim’s ServPak extended warranty and enhanced support packages for the product
- Customers can choose to purchase one-time per-incident technical support for the product for a fee
- Customers can choose to call the reseller or distributor who sold them the product for technical support

Tech Support on Discontinued Products

Technical Support on some products that Proxim has declared as EOL (End of Life) or otherwise is no longer selling is available based upon one of the following three options Customers can choose:

- For some discontinued products, Customers can choose to purchase one of Proxim’s EOL ServPak support packages for the product
  - No EOL ServPak support package will be available for any product discontinued more than 5 years ago
  - No EOL ServPak support package is available for certain discontinued products
- Customers can choose to purchase one-time per-incident technical support for the product on a per hour basis at a rate of $125 an hour (4 hours minimum payable in advance by major credit card). This fee is payable in addition to any RMA fee that may be charged to subsequently repair the product.
- Customers can choose to call the reseller or distributor who sold them the product for technical support

All Proxim technical support for discontinued products, whether through an EOL ServPak package or otherwise, is provided on a “best effort” basis and is subject to the continued availability of necessary components, equipment, and other technical resources.

Note that Proxim is unable to support or warrant any equipment that has been modified, whether this modification is physical, or if third-party software codes have been loaded onto the product.