

# EnGenius Mesh AP M9000



## User Manual

Version: 1.0

## Table of Content

<b>1</b>	<b>Document History</b>	<b>4</b>
<b>2</b>	<b>Overview</b>	<b>5</b>
<b>3</b>	<b>EnGenius Mesh Web-based Interface</b>	<b>6</b>
<b>4</b>	<b>System</b>	<b>11</b>
4.1	System > System	11
4.2	System > Syslog	13
4.3	System > Advance	14
4.4	System > Profile	17
<b>5</b>	<b>Network</b>	<b>18</b>
5.1	Network > Network	18
5.2	Network > WAN	19
5.3	Network > VLAN	23
5.4	Network > Mesh	25
5.5	Network > Wireless	30
5.6	Network > Route	33
5.7	Network > IPSEC	35
5.8	Network > L2TPC	36
5.9	Network > OLSR	37
<b>6</b>	<b>Service</b>	<b>39</b>
6.1	Service > DHCPD	39
6.2	Service > Firewall	42
6.3	Service > MAC Access	45
6.4	Service > NAT	47
6.5	Service > NTP	49
6.6	Service > Traffic Shaping	51
6.7	Service > PPTP Server	53
6.8	Service > AutoIP	55
6.9	Service > Captive Portal	56
6.10	Service > RADIUS	58
6.11	Service > Dynamic DNS	60
6.12	Service > Zero Config	61
6.13	Service > Mobile IP	62
6.14	Service > Route Watchdog	63
6.15	Service > Linux Kernel Watchdog	64
6.16	Service > SSHD	65
6.17	Service > WME	66
6.18	Service > DHCP Relay	69
<b>7</b>	<b>Management</b>	<b>71</b>
7.1	Management > HTTPD	71
7.2	Management > Configuration	73

7.3	Management > SNMP	76
7.4	Management > Firmware	79
7.5	Management > Trap	80
7.6	Management > User group	83
7.7	Management > Database	85
7.8	Management > Webspaces	87
7.9	Management > Customize Login	88
7.10	Management > NMS Addresses	90
7.11	Management > Reboot	92
<b>8</b>	<b>Tools</b>	<b>93</b>
8.1	Tools > Ping	93
8.2	Tools > Ifconfig	94
8.3	Tools > Route	95
8.4	Tools > TFTP	96
<b>9</b>	<b>Status</b>	<b>97</b>
9.1	Status > Status	97
9.2	Status > Interfaces	97
9.3	Status > Services	99
9.4	Status > Users	101
9.5	Status > System Log	103
9.6	Status > Topology	104
9.7	Status > Mobile IP	105
9.8	Status > Neighbor	106
<b>10</b>	<b>Help</b>	<b>107</b>

## 1 Document History

Revision	Date	Remark	Authors
1.0	23 Sep, 2007	Initial Version	Ivy
1.1	13 Aug, 2009	Second Draft Version: Webpage Interface Update	Mingl

## 2 Overview

The purpose of this document is to describe the detail features of EnGenius Mesh Access Point (M9000), and also the procedure and methodology of configuring and the use of EnGenius M9000.

DORADO CONFIDENTIAL

### 3 EnGenius Mesh Web-based Interface

Web-based configuration interface is accessible with computer with TCP/IP capability and web browser (e.g. Safari, Firefox, Mozilla or IE). To access web-based configuration interface, enter

https://<Device IP>/.

In the browser URL/Location field.

You will see an authentication page display as shown in Figure 3.1.1.

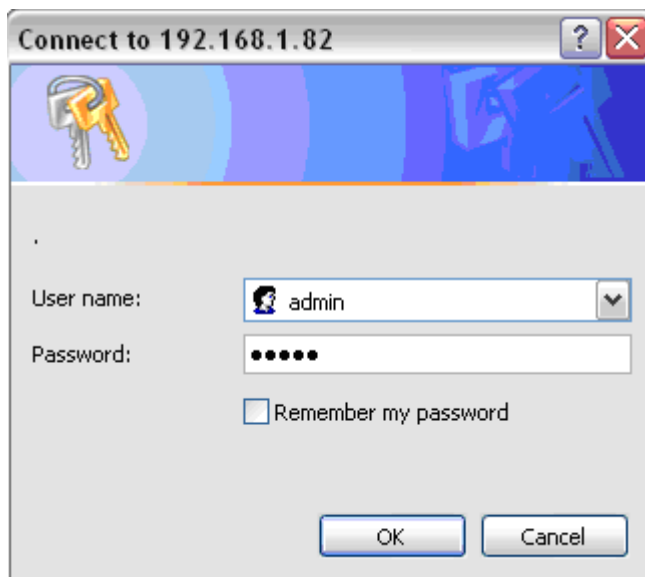


Figure 3.1.1: Windows authentication page

Type “admin” in User Name and Password field, then click **OK** button.

\*Obtain default IP address for EnGenius Mesh AP for different Interfaces:

Interface	Default IP	Notes
WAN	DHCP	Administrator needs to check their DHCP server lease to obtain device IP address
VLAN/LAN/AP	Auto IP	Connect a DHCP client computer/laptop to EnGenius Mesh AP's LAN (with cross cable) or wireless interface. Device IP address is the 'Gateway' address given to DHCP client (computer/laptop)

EnGenius Mesh page has six main menus: System, Network, Services, Management, Tools and Status. Each main menu also will have its submenu.

<i>Welcome</i>	
<i>System</i>	
<i>System</i>	<i>System settings</i>
<i>Syslog</i>	<i>Syslog settings</i>
<i>Advance</i>	<i>Advance tuning</i>
<i>Network</i>	
<i>Network</i>	<i>Network settings</i>
<i>WAN</i>	<i>WAN settings</i>
<i>VLAN</i>	<i>VLAN settings</i>
<i>Mesh</i>	<i>Mesh settings</i>
<i>Wireless</i>	<i>Wireless settings</i>
<i>Route</i>	<i>Route settings</i>
<i>IPSEC</i>	<i>IPSEC settings</i>
<i>L2TPC</i>	<i>L2TPC settings</i>
<i>OLSR</i>	<i>OLSR settings</i>
<i>Services</i>	
<i>DHCPD</i>	<i>DHCP server settings</i>
<i>DHCRelay</i>	<i>DHCP relay settings</i>
<i>Firewall</i>	<i>Firewall settings</i>
<i>MAC Access</i>	<i>Filter MAC address</i>

<i>NAT</i>	<i>Network Address Translation</i>
<i>NTP</i>	<i>Network Time Protocol</i>
<i>Traffic Shaping</i>	<i>Bandwidth management</i>
<i>PPTP Server</i>	<i>PPTP server settings</i>
<i>AutoIP</i>	<i>AutoIP settings</i>
<i>Captive Portal</i>	<i>Captive Portal settings</i>
<i>RADIUS</i>	<i>RADIUS client settings</i>
<i>Dynamic DNS</i>	<i>DDNS settings</i>
<i>Zero Config</i>	<i>Zero Config settings</i>
<i>Mobile IP</i>	<i>Mobile IP settings</i>
<i>Route Watchdog</i>	<i>Route watchdog settings</i>
<i>Linux Kernel Watchdog</i>	<i>Linux Kernel Watchdog settings</i>
<i>SSHD</i>	<i>SSHD Configuration</i>
<i>WME</i>	<i>WME Settings</i>
<i>Management</i>	
<i>HTTPD</i>	<i>Internal webserver settings</i>
<i>Configuration</i>	<i>Configuration management</i>
<i>SNMP</i>	<i>SNMP settings</i>
<i>Firmware</i>	<i>Firmware maintenance</i>
<i>Trap</i>	<i>Trap settings</i>
<i>User Group</i>	<i>User group maintenance</i>
<i>Database</i>	<i>Database settings</i>

<i>Webspace</i>	<i>Webspace maintenance</i>
<i>Customize Login</i>	<i>Customize Login Page</i>
<i>NMS Addresses</i>	<i>Network Management System notifying settings.</i>
<i>Reboot</i>	<i>Reboot device</i>
<i>Tools</i>	
<i>Ping</i>	<i>Ping</i>
<i>Ifconfig</i>	<i>Ifconfig</i>
<i>Route</i>	<i>Route</i>
<i>TFTP</i>	<i>TFTP</i>
<i>Status</i>	
<i>Status</i>	<i>System status</i>
<i>Interfaces</i>	<i>Interfaces statistics</i>
<i>Services</i>	<i>Services status</i>
<i>Users</i>	<i>Users details</i>
<i>System Log</i>	<i>System logging</i>
<i>Topology</i>	<i>Simple topology view</i>
<i>Mobile IP</i>	<i>Simple mobile IP status</i>
<i>Neighbor</i>	<i>Mesh node status</i>
<i>Help</i>	

## 4 System

### 4.1 System > System

M9000 supports different type of operation mode in one firmware. Supported operations are Layer 3 and Layer 2 oriented mesh network. Gateway, Relay , and Client Relay are those operate in layer 3. Layer 2 Gateway and Layer 2 Relay are those fall in layer 2 operation. Figure 4.1.1 illustrates the System Information Configuration page.

Name	<input type="text" value="Dorado"/>
Location	<input type="text" value="Unknown"/>
Contact Name	<input type="text" value="Unknown"/>
Contact Email	<input type="text" value="Unknown"/>
Contact Phone	<input type="text" value="Unknown"/>
Description	<input type="text" value="Dorado Mesh AP"/>
Object ID	1.3.6.1.4.1.25541.1
Operation Mode	<input type="text" value="Gateway"/> ▼
<input type="button" value="Apply"/>	

**Figure 4.1.1: System Information Configuration page**

System Information Configuration page contains the following parameters:

- **Name** – Name of the device.
- **Location** – Location name that device located.
- **Contact Name** – Name of the contact person for consulting about the device.
- **Contact Email** – Email address of the contact person.
- **Contact Phone** – Phone number of the contact person.
- **Description** – Description of the device.

- **Object ID** – Display SNMP MIB object identification (OID) of the device.
- **Operation Mode** – Type of operation mode such as “Gateway”, “Relay”, “Client Relay”, “Layer 2 Gateway”, or “Layer 2 Relay”.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

DORADO CONFIDENTIAL

## 4.2 System > Syslog

Certain system message is useful to understand the problem behind any undesired result. M9000 is enabled with Syslog server that can log message locally and remotely.

Figure 4.2.1 illustrates the Syslog configuration page.

The screenshot shows the Syslog configuration page with the following settings:

Active	Enable
Klog	Disable
Level	Notice
Remote Syslog	Disable
Remote Server Address	<input type="text"/>

Below the settings is an **Apply** button.

**Figure 4.2.1: Syslog configuration page**

Syslog contains the following parameters:

- **Active** – Enable or disable system logging feature.
- **Klog** – Enable or disable kernel logging feature.
- **Level** – 8 levels of logging : emergency, alert, critical, error, warning, notice, info and debug.
- **Remote Syslog** – Enable or disable remote syslog server.
- **Remote Server Address** – Address of remote syslog server when remote syslog is enabled.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

### 4.3 System > Advance

In this advance feature, networking and some wireless fine tune done. Figure 4.3.1 illustrates the advance configuration page.

#### Networking-CONTRACK

Maximum session	<input type="text" value="10000"/>	(4096~200000)
Generic Timeout	<input type="text" value="600"/>	(50~1200s)
ICMP Timeout	<input type="text" value="30"/>	(10~60s)
TCP Close Timeout	<input type="text" value="10"/>	(5~30s)
TCP Close Wait Timeout	<input type="text" value="60"/>	(10~120s)
TCP Established Timeout	<input type="text" value="3600"/>	(600~864000s)
TCP Finished Wait Timeout	<input type="text" value="120"/>	(10~3600s)
TCP Last ACK Timeout	<input type="text" value="30"/>	(10~60s)
TCP SYN Receive Timeout	<input type="text" value="60"/>	(10~120s)
TCP SYN Sent Timeout	<input type="text" value="120"/>	(10~240s)
TCP Time Wait Timeout	<input type="text" value="120"/>	(10~240s)
UDP Timeout	<input type="text" value="30"/>	(10~60s)
UDP Stream Timeout	<input type="text" value="180"/>	(10~360s)

#### Wireless

Radio 1 distance	<input type="text" value="1000"/>	(100~30000m)
Radio 1 ack timeout	<input type="text" value="29"/>	
Radio 2 distance	<input type="text" value="1000"/>	(100~30000m)
Radio 2 ack timeout	<input type="text" value="29"/>	
Country	<input type="text" value="United States"/>	<input type="button" value="v"/>
Outdoor Mode	<input type="text" value="Enable"/>	<input type="button" value="v"/>
External Channel Mode	<input type="text" value="Disable"/>	<input type="button" value="v"/>
Preamble Type	<input type="text" value="Short"/>	<input type="button" value="v"/>
Extended Range Mode	<input type="text" value="Enable"/>	<input type="button" value="v"/> (Hardware not supported)

Fast Frame Mode	Enable ▼
Compression Mode	Enable ▼
Bandwidth Mode	Normal (20Mhz) ▼
Mesh Minimum Signal Strength:	<input type="text" value="15"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

**Figure 4.3.1: Advance configuration page**

Advance configuration have the following parameters:

- **Maximum Session** – Maximum connection tracking session, a higher value is desired to support large number of local users.
- **Generic Timeout** – Generic timeout for a connection tracking instance
- **ICMP Timeout** – ICMP timeout
- **TCP Close Timeout** – TCP close timeout
- **TCP Close Wait Timeout** – TCP close wait timeout
- **TCP Established Timeout** – TCP established timeout
- **TCP Finished Wait Timeout** – TCP finished wait timeout
- **TCP Last Ack Timeout** – Last acknowledgement timeout
- **TCP SYN Receive Timeout** – TCP SYN receive timeout
- **TCP SYN Sent Timeout** – TCP SYN sent timeout
- **TCP Time Wait Timeout** – TCP Time wait timeout
- **UDP Timeout** – UDP timeout
- **UDP Stream Timeout** – UDP stream timeout
- **Radio 1 distance** – Desired operating distance for radio 1 ( usually refer to mesh radio )
- **Radio 1 ack timeout** – ACK timeout for radio 1
- **Radio 2 distance** – Desired operating distance for radio 2 ( usually refer to client access radio )
- **Radio 2 ack timeout** – ACK timeout for radio 2
- **Country** – List of supported country available from the wireless interface.
- **Outdoor Mode** – Enable or disable use of outdoor mode on the wireless

interface.

- **External Channel Mode** – Enable or disable use of external channel mode of the wireless interface
- **Preamble Type** – Type of preamble
- **Extended Range Mode** – Enable or disable of extended range mode (depend on hardware supported)
- **Fast Frame Mode** – Enable or disable of fast frame mode (depend on hardware supported)
- **Compression Mode** – Enable or disable of compression mode (depend on hardware supported)
- **Bandwidth Mode** – Select different type of bandwidth (depend on hardware supported)
- **“Apply”** button to save any changes made. New settings are active after reboot.
- **“Reset”** button to restore the settings on advance page back to factory default settings.

## 4.4 System > Profile

Different settings on System > Advance, Network > Wireless and Network > Mesh (Wireless) will be profiled as a unique settings. User can switch to different profile as ease. Figure 4.4.1 illustrates the profile configuration page.

**Profile**

Please configure the  
\*System -> Advance  
\*Network -> Wireless  
\*Network -> Mesh ( Wireless )  
before saving a profile.

Note that activating a profile will need a system reboot to enable new settings.

Profile name

Action

**Figure 4.1.1 Profile settings.**

Profile page has the following parameters:

- **Profile name** – Select different profile name
- **Action** – Select different action such as **“Activate”**, **“Save”**, and **“Delete”**
- **“Apply”** button to save any changes made. New settings are active after reboot.

## 5 Network

### 5.1 Network > Network

Figure 5.1.1 illustrates the network configuration page.

**Note that static DNS will overwrite DHCP settings.**

Primary DNS	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Secondary DNS	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Domain	<input type="text" value="dorado"/>			
Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

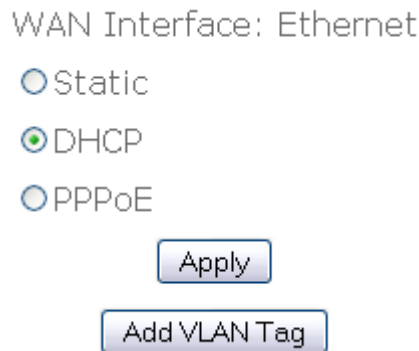
**Figure 5.1.1: Network configuration page**

Network contains the following parameters:

- **Primary DNS** – Primary Domain Name Server used to translates domain names to IP addresses. Edit this field to match your ISP DNS address or leave it unchanged to use received DNS address from your ISP.
- **Secondary DNS** – Secondary Domain Name Server used to translates domain names to IP addresses. A backup DNS address to primary DNS. Specify the Secondary DNS address.
- **Domain** – Specify the Domain name of network.
- **Gateway** – IP address of router or nodes that serves as an entrance to another network, and vice-versa. Edit this field to match your ISP settings or leave it unchanged to use defaults from your ISP.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 5.2 Network > WAN

WAN (Wide Area Network) are used to connect local area networks (LANs) to other networks through your ISP (Internet Service Provider). Figure 5.2.1 illustrates the WAN configuration page.



WAN Interface: Ethernet

Static

DHCP

PPPoE

Apply

Add VLAN Tag

Figure 5.2.1: WAN configuration page

To configure WAN:

- Choose option either for **Static**, **DHCP** or **PPPoE**.
- Click on **“Apply”** button.
- If choose for **Static** option, Static IP configuration page is shown in Figure 5.2.2.



IP

Netmask

Apply

Figure 5.2.2: Static IP configuration page

Static IP configuration page contains the following parameters:

- **IP** – IP address is a unique address used to identify and communicate with different device on a computer network utilizing the Internet

- Protocol standard. Specify the Static IP address.
- **Netmask** – Specify subnet mask for this IP.
  - **“Save changes”** button – Click on **“Save changes”** button if you have made any changes. New settings are active after the device reboot.
  - If ISP or network assigns the IP address dynamically using a DHCP server. Select this radio button and press **“Apply”**. Using this option, all the network related configuration will be provided by ISP or network. You might need to remove any changes done in the *Network Configuration*..

Configuration saved. Please reboot to enable new settings.

Warning: An early DNS servers configuration found. Please remove those settings in network menu if dns server assigned by DHCP server is needed.

Warning: An early default gateway configuration found. Please remove the settings in network menu if gateway assigned by DHCP server is needed.

### Figure 5.2.3: DHCP Client configuration page

- PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating PPP frames in Ethernet compression. Widely adapted by ADSL service provider. Basic authentication based on username and password is required for this type of connection. Select this radio button and press **“Apply”** to configure the following fields as shown in Figure 5.2.4.

Active	<input type="button" value="Disable"/>
Authentication type	<input type="button" value="PAP"/>
Username	<input type="text"/>
Password	<input type="text"/>
Reconfirm Password	<input type="text"/>
	<input type="button" value="Apply"/>

Figure 5.2.4: PPPoE configuration page

PPPoE configuration page contain the following parameters:

- **“Active”** - Click on **“Active”** drop down menu to select enable or disable PPPoE service.
- **Username** – Specify PPPoE service username.

- **Password** – Specify PPPoE service password.
- **Reconfirm password** – Re-enter PPPoE service password to confirm it.
- **“Apply”** button - Click on **“Save changes”** button if you have made any changes. New settings are active after the device reboot.

To Add VLAN Tag to WAN:

- Click on **“Add VLAN Tag”** button.
- Click on **“Action”** drop down menu to select **“Add”**, **“Edit”** or **“Delete”** VLAN Tag.
- Click on **“Apply”** to add, edit, or delete VLAN Tag.
- If select to add new VLAN Tag, VLAN Tag – add page will display as shown in Figure 5.2.5.

The screenshot shows a configuration form for adding a VLAN tag. It contains the following elements:

- ID**: A text input field with a range indicator "( 1 ~ 4095 )".
- Type**: A dropdown menu currently set to "Static".
- IP**: Four text input fields for entering the IP address.
- Netmask**: Four text input fields for entering the network mask.
- Comments**: A single-line text input field.
- Active**: A dropdown menu currently set to "Enable".
- Apply**: A button located below the form fields.

Figure 5.2.5: VLAN Tag - add configuration page

Add VLAN Tag – add page contain the following parameter:

- **ID** – Enter the VLAN ID.
- **Type** – Click on **“Type”** drop down menu to select **“Static”** or **“DHCP”**.
- **IP** - Specify the VLAN IP address.
- **Netmask** – Specify the network mask for IP.
- **Comments** – Specify VLAN comments.
- **Active** – Click on **“Active”** drop down menu to select enable or

disable VLAN.

- **“Apply”** button - Click on **“Save changes”** button if you have made any changes. New settings are active after the device reboot.
- If select to edit existing VLAN Tag, a page similar to Figure 5.2.5 with configured settings will be displayed
- If select to delete existing VLAN Tag, a page similar to Figure 5.2.5 with configured settings will be displayed.

### 5.3 Network > VLAN

Virtual LAN is a method of creating independent networks within a physical network. Several VLANs can co-exist within such a network. This VLAN implementation is based on the IEEE 802.1Q tagging protocol. Figure 5.3.1 illustrates the VLAN configuration page.

Active VLAN					
ID	Name	IP	Netmask	Comments	Configure
0	vlan0	172.23.203.1	255.255.255.0	Default VLAN	<input type="button" value="Edit"/>

Inactive VLAN

Figure 5.3.1: VLAN configuration page

To configure VLAN:

- Active VLAN list all activated VLAN. By default, only VLAN0 is active. Click on “Edit” button to edit active VLAN.
- VLAN0 – edit page will display as shown in Figure 5.3.2.

ID  ( 0 ~ 4095 )

Type

IP

Netmask

Routed

Comments

Active

Figure 5.3.2: VLAN0 – edit page

VLAN0 - edit page contain the following parameter:

- **ID** – Enter the VLAN ID.
  - **Type** – Click on “**Type**” drop down menu to select “Static” or “DHCP”.
  - **IP** – Specify the VLAN IP address.
  - **Netmask** – Specify the network mask for this IP.
  - **Routed** – Click on “**Routed**” drop down menu to select “Routeable address” or “NAT address”. A routeable network is visible to other Mesh Node.
  - **Comments** – Specify VLAN comments.
  - **Active** – Click on “**Active**” drop down menu to select enable or disable VLAN.
  - “**Apply**” button to save any changes made. New settings are active after the device reboot.
- To edit inactive VLAN, click on “**Inactive VLAN**” drop down menu, select on VLAN you want to edit. For example, select VLAN1. Click on bottom “**Edit**” button to edit inactive VLAN1.
  - VLAN1 – edit page will display as shown in Figure 5.3.2

## 5.4 Network > Mesh

This device will form a wireless mesh network with other device provided the correct configuration. Each of the mesh will have its own IP address. If two device with the same IP, one is not visible to each other in the mesh routing table. Hence, an initial network planning is needed to plan the whole mesh network.

AutoIP service could be used for simplicity and easy deployment of the mesh network. The following fields will change accordingly if AutoIP is used. However, if you plan to use the configured IP and Netmask, please disable AutoIP service. Figure 5.4.1 illustrates the mesh configuration page.

**Please disable autoIP to configure static mesh IP**

IP	<input type="text" value="10"/>	<input type="text" value="23"/>	<input type="text" value="203"/>	<input type="text" value="1"/>
Netmask	<input type="text" value="255"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Comments	<input type="text" value="Mesh"/>			
Active	<input type="text" value="Enable"/> ▼			
<input type="button" value="Apply"/>				
<input type="button" value="Wireless settings"/>				

**Figure 5.4.1: Mesh configuration page**

Mesh configuration page contains the following parameters:

- **IP** – Specify the Mesh IP address.
- **Network** – Specify the Network mask for this IP.
- **Comments** – Optional comments.
- **Active** – Enable or disable Mesh interface.
- **“Apply”** button to save any changes made. New settings are active after the

device reboot.

- Click on “**Wireless settings**” button to edit Mesh – wireless. Mesh – wireless configuration page will display as shown in Figure 5.4.2.

MAC address	00:0b:6b:2b:ee:58
Mode	ADHOC
Band	802.11a ▼
ESSID	DoradoMesh
Frequency	160: 5.800 GHz ▼
Beacon Interval	100 ( 20 ~ 1000 ms )
RTS Threshold	2346 ( 256 ~ 2346 )
Fragmentation Threshold	2346 ( 1500 ~ 2346 )
DTIM interval	1 ( 1 ~ 256 )
Datarate	auto ▼
Tx antenna	Card Default ▼
Rx antenna	Card Default ▼
Current Maximum Tx Power ( dBm )	20
*Maximum Tx Power ( dBm )	20 ▼
Security	Open ▼

\* Power value begin with "x" indicate that the power value is not supported by the hardware.

Apply

**Figure 5.4.2: Mesh - wireless configuration page**

Mesh – wireless page contain the following parameter:

- **MAC address** – Display the MAC address of Mesh – wireless interface.
- **Mode** – Click on “**Mode**” drop down menu to select “AP”, “STA”, “ADHOC” or “WDS” operating mode. **AP mode** will bring the wireless device to Access Point mode. Under this mode, it can connect multiple

wireless communication devices together to form a wireless network and can relay data between wireless and wired devices.

**STA** mode will bring the wireless device to Station mode. Under this mode, it needs to connect to an AP to join the wireless network.

**ADHOC** mode will bring the wireless device to adhoc mode where no AP is required. The connection is established for the duration of one session by discovering others device within range.

**WDS** mode will bring the wireless device to form a wireless distribution system that connects to other AP to form a larger network. Data can be relayed between 2 stations.

Only **ADHOC** mode is allowed in mesh network. Mode other than ADHOC is disabled and not supported.

- **Band** – Click on “**Band**” drop down menu to select “802.11a”, “802.11b” or “802.11g” operating band. Choose 802.11a if you want to operates mesh network under the 5GHz spectrum and up to 54Mbps. However, make sure your hardware is supported for this kind of operation. Choose 802.11b for operation under 2.4 GHz spectrums for rates up to 11Mbps. Choose 802.11g for operation under 2.4GHz that are backward compatible with 802.11b band. It can support rates up to 54Mbps.
- **ESSID** – Extended Service Set Identifier is a code attached to all packets on a wireless network to identify each packet as part of that network. This entry is case sensitive text string which consists of a maximum of 32 alphanumeric characters. Enter your ESSID into this field that consistent with other mesh so that it can join or form the mesh network.
- **Frequency** – Click on “**Frequency**” drop down menu to select operating frequency of wireless network in GHz.
- **Beacon Interval** – Beacon are management packets sent by an Access Point to manage and synchronize a wireless network. Value in the range of 20 to 1000 milliseconds is permitted. The default value is set to 100 milliseconds.

- **RTS Threshold** – Request to Send management packet. With smaller RTS length value, the wireless network can recover from interference and collisions quicker at a cost of reducing the maximum throughput. Network with heaving loading or interference is advised to use smaller value of RTS.
- **Fragmentation Threshold** – Fragmentation of packet into desired length. Network with high packet error should use smaller value. Use of small value will results in lower throughput due to more overheads is introduced.
- **DTIM Interval** – Delivery Traffic Indication Message is a countdown mechanism for informing associated stations of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages, it sends the next DTIM with a DTIM interval value. Clients hear the beacons and awaken to receive the broadcast and multicast messages. A range of value 1 to 255 is permitted. The default value is 1.
- **Datarate** – Click on “**Datarate**” drop down menu to select wireless network datarate. For example, 1 Mbps, 2 Mps, 5.5 Mbps.....
- **Tx antenna** – Click on “**Tx antenna**” drop down button to select “Diversity”, “Card Default”, “Port 1”, or “Port 2”.
- **Rx antenna** - Click on “**Rx antenna**” drop down button to select “Diversity”, “Card Default”, “Port 1”, or “Port 2”.
- **Current Maximum Tx Power (dBm)** – Display current maximum Tx power.
- **Maximum Tx Power (dBm)** - Click on “**Maximum Tx Power**” drop down button to select maximum Tx power.
- **Security** – Add security features to the wireless network. Click on “**Security**” drop down button to select “Open”, “WEP” or “AES”. Only when select “WEP” or “AES” will display “Encryption Key” field as shown in Figure 5.4.3.

Security

Encryption key

0

1

2

3

\* Power value begin with "x" indicate that the power value is not supported by the hardware.

Apply

**Figure 5.4.3: Mesh - wireless configuration page (with encryption key)**

- Open-no encryption or security is applied.
  - WEP-Wired Equivalent Privacy. An encryption using either 64-bit or 128-bit to encrypt the network packets.
  - AES-Advanced Encryption Standard. An encryption scheme that uses 128-bit to encrypt the network packets.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 5.5 Network > Wireless

Figure 5.5.1 illustrates the AP configuration page.

MAC address	00:0b:6b:2b:ee:f5
Mode	AP
Band	802.11g ▼
Frequency	auto ▼
Tx antenna	Card Default ▼
Rx antenna	Card Default ▼
Current Maximum Tx Power ( dBm )	20
*Maximum Tx Power ( dBm )	20 ▼

\* Power value begin with "x" indicate that the power value is not supported by the hardware.

---

**Active Virtual AP**

ESSID	Security	Comments	Active	Configure
DoradoAP	open	VAP1	Enabled	<input type="button" value="Edit"/>

**Figure 5.5.1: AP configuration page**

Wireless AP contains the following parameters:

- **MAC address** – Displays the MAC address of the wireless interface.
- **Mode** – Only AP mode is available in M9000 4000.
- **Band** – “802.11a”, “802.11b” or “802.11g” operating band.
- **Frequency** – Operating frequency of the wireless network in Ghz.
- **Tx antenna** – Select “Diversity”, “Port 1”, “Port 2” or “Card Default”.
- **Rx antenna** – Select “Diversity”, “Port 1”, “Port 2” or “Card Default”.
- **Current Maximum Tx Power** – Displays current transmit power of the wireless card due to regulatory limitation.
- **Maximum Tx Power (dBm)** – Select transmit power of the AP wireless card.

- **“Apply”** button to save any changes made. New settings are active after the device reboot.
- **“Edit”** button to edit Active Virtual AP. AP configuration – edit page is shown in Figure 5.5.2.

ESSID	<input type="text" value="DoradoAP"/>
Broadcast SSID	<input type="button" value="Enable"/> ▾
Beacon Interval	<input type="text" value="100"/> ( 20 ~ 1000 ms )
RTS Threshold	<input type="text" value="2346"/> ( 256 ~ 2346 )
Fragmentation Threshold	<input type="text" value="2346"/> ( 1500 ~ 2346 )
DTIM interval	<input type="text" value="1"/> ( 1 ~ 255 )
Datarate	<input type="button" value="auto"/> ▾
Security	<input type="button" value="Open"/> ▾
Wireless Separation	<input type="button" value="Disable"/> ▾
Comment	<input type="text" value="VAP1"/>
Active	<input type="button" value="Enable"/> ▾

**Figure 5.5.2: AP configuration – edit page**

AP configuration – edit page contain the following parameter:

- **ESSID** – Enter the ESSID of wireless network.
- **Broadcast SSID** – Click on **“Broadcast SSID”** to enable or disable Broadcast SSID.
- **Beacon Interval** – Enter the Beacon Interval value.
- **RTS Threshold** – Enter the RTS Threshold value.
- **Fragmentation Threshold** – Enter the Fragmentation Threshold value.
- **DTIM interval** - Enter the DTIM interval value.
- **Datarate** – Click on **“Datarate”** drop down menu to select datarate. For example, 1 Mbps, 2 Mbps, 5.5 Mbps.....

- **Security** - Click on **“Security”** drop down menu to select **“Open”**, **“WEP”**, **“WPA”**,. Select **“WEP”** will display **“802.1x”** drop down menu and **“Encryption key”** field as shown in Figure 5.4.3. While select **“WPA (1 & 2)”** will display **“WPA Type”** drop down menu, **“802.1x”** drop down menu and **“Encryption key”** field as shown in Figure 5.5.4.

Security: WEP

802.1x: False

Encryption key:

- 0
- 1
- 2
- 3

**Figure 5.5.3 AP0 configuration with wep key security selected.**

Security: WPA (1 & 2)

WPA Type: TKIP

802.1x: False

Encryption key:

**Figure 5.5.4: AP0 configuration – edit page (WPA (1 & 2))**

- Open-no encryption or security is applied.
  - WEP-Wired Equivalent Privacy. A encryption using either 64-bit or 128-bit to encrypt the network packets.
  - WPA-Wi-fi Protected Access is a class of systems to secure wireless networks.
  - 802.1 x-Enable or disable 802.1x.
  - WPA Type-Select **“TKIP”** type or **“AES”** type.
- **Wireless Seperation** – Click on **“Wireless Seperation”** drop down menu to enable or disable wireless separation.
  - **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 5.6 Network > Route

Routing refers to selecting paths in a network along which to send data. Figure 5.6.1 illustrates the route configuration page.

Routes List					
IP	Netmask	Using	Comments	Active	Configure
192.168.2.0	255.255.255.0	VLAN0	New Route	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 5.6.1: Route configuration page

Route contains the following parameters:

- **Routes List** – Display list of routes.
- **“Modify”** button to edit the current selection
- **“Remove”** button to delete the current selection
- **“New Entry”** button to add new entry.

Figure 5.6.2 illustrates the add or edit page for route entry.

Subnet

Netmask

Direct

Device

Comments

Active

Figure 5.6.2: Routes – add or edit page

Routes – add page contain the following parameter:

- **Subnet** – Enter the IP address of destination subnet.

- **Netmask** – Enter the IP address of destination subnet network mask.
- **Gateway** – Enter the gateway address.
- **Direct** – Click on “**Direct**” drop down menu to select “Direct” or “Indirect” route.
- **Device** – Click on “**Device**” drop down menu to select device. For example, WAN, VLAN0, VLAN1.....
- **Comments** – Enter the interface comments.
- **Active** – Enable to disable this interface.
- “**Apply**” button to save any changes made. Please reboot to enable new settings.

## 5.7 Network > IPSEC

IP security (IPSEC) is a suite of protocols for securing Internet Protocol communications by encrypting and/or authenticating each IP packet in a data stream. It provides an extra level of securing the data in the network. Figure 5.7.1 illustrates the IPSEC configuration page.

The screenshot shows the IPSEC configuration page with the following fields and values:

Active	Disable
Type	x509
Local ID	
Remote ID	
Remote IP	0 0 0 0
Remote Subnet	0 0 0 0
Remote Netmask	0 0 0 0
Local Certificate Password	

Below the fields is an **Apply** button.

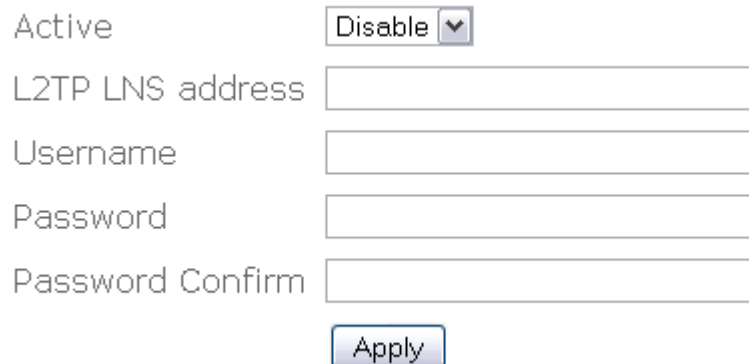
**Figure 5.7.1: IPSEC configuration page**

IPSEC configuration page contains the following parameters:

- **Active** – Enable or disable IPSEC service.
- **Type** - Select “x509”, “RSA”, or “PSK” type of IPSEC service.
- **Local ID** – Enter the local identity (only for RSA).
- **Remote ID** – Enter the remote identity (only for RSA).
- **Remote IP** – Enter the IP address of IPSEC server.
- **Remote Subnet** – Enter the subnet of IPSEC server.
- **Remote Netmask** – Enter the network mask of the remote subnet.
- **Local Certificate Password** – Enter local certificate password (for X509), local & remote RSA key (for RSA) or PSK key (for PSK).
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 5.8 Network > L2TPC

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPN). L2TPC serves as a L2TP client that creates a tunnel through existing network to the designated peer computer or network. Figure 5.8.1 illustrates the L2TPC configuration page.



Active

L2TP LNS address

Username

Password

Password Confirm

**Figure 5.8.1: L2TPC configuration page**

L2TPC configuration page contains the following parameters:

- **Active** – Enable or disable L2TPC service.
- **L2TP LNS address** – Enter the L2TP LNS address.
- **Username** – Enter L2TP username.
- **Password** – Enter L2TP password.
- **Password Confirm** – Re-enter L2TP password to confirm.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 5.9 Network > OLSR

Optimized Link State Routing protocol is a protocol to connect mobile ad-hoc networks. It is a link-state routing protocol that collects data about available network and then calculates an optimized routing table. Figure 5.9.1 illustrates the OLSR configuration page.

Active	Enable
TOS value	Minimize delay
Willingness	Disable
Willingness level	4 ( 0 ~ 7 )
Hysteresis	Disable
Hysteresis Scaling	0.50 ( 0 ~ 1.00 )
Hysteresis THR High	0.80 ( 0 ~ 1.00 )
Hysteresis THR Low	0.30 ( 0 ~ 1.00 )
Link Quality Type	Disable link quality
Link Quality Size	10 ( 3 ~ 128 )
Poll Rate	0.05 ( 0.02 ~ 10.0 )
TC Type	Only send MPR selectors
MPR	1 ( 1 ~ 20 )
Shared Key	••••••
Reconfirm Shared Key	••••••
	Apply Reset

Figure 5.9.1: OLSR configuration page

OLSR configuration page contains the following parameters:

- **Active** – Enable or disable OLSR service.
- **TOS value** – Enter the value of TOS. Type Of Service ( TOS ). Value for the IP header of control traffic.

- 0 : normal service.
- 2 : minimize monetary cost.
- 4 : maximize reliability.
- 8 : maximize throughput.
- 16 : minimize delay. (Default)

- **Willingness** – Enable or disable Willingness. Willingness will be calculated dynamically if disabled.
- **Willingness level** – Enter the Willingness level.
- **Hysteresis** – Hysteresis adds more robustness to the link sensing but delays neighbor registration. Enable or disable hysteresis.
- **Hysteresis Scaling** – Enter the Hysteresis Scaling.
- **Hysteresis THR High** – Enter the Hysteresis THR High value.
- **Hysteresis THR Low** – Enter the Hysteresis THR Low value.
- **Link Quality Type** – Select type of link quality.
- **Link Quality Size** – Enter the Link Quality Size.
- **Poll rate** – Enter the Poll rate.
- **TC type** – Specify how much neighbor information should be sent in TC message.
  - 0 : only send MPR selectors. (Default)
  - 1 : send MPR selectors and MPRs.
  - 2 : send all neighbors.
- **MPR** – Specify how many MPRs a node should try select to reach every 2 hop neighbor. Default is 1.
- **Shared Key** – Specify a pre-shared key for the control traffic. Control traffic with different shared key will be discarded.
- **Reconfirm shared key** – Re-enter the Shared Key to confirm it.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 6 Service

### 6.1 Service > DHCPD

DHCP is a protocol used by networked computers (clients) to obtain unique IP addresses, and other parameters such as default router, subnet mask, and IP addresses for DNS server from a DHCP server. Figure 6.1.1 illustrates the DHCPD configuration page.

Active  ▾

---

DHCPD List

Interface	Subnet	Netmask	Comment	Active	Configure
vlan0	172.23.203.0	255.255.255.0	Default DHCP server	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 6.1.1: DHCPD configuration page**

DHCPD configuration page contains the following parameters:

- **Active** – Enable or disable DHCPD service.
- **“Apply”** button to save any changes made.
- **“Modify”** button to edit current selection.
- **“Remove”** button to delete current selection.
- **“New Entry”** button to add new entry to the service.

Figure 6.1.2 illustrates the configuration page when new entry is added or edited.

Interface	<input type="text" value="VLAN1"/>			
Subnet	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
IP Start	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
IP End	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Netmask	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Max Lease	<input type="text"/>	( 600 ~ 864000 s )		
Lease	<input type="text"/>	( 600 ~ 864000 s )		
Domain	<input type="text"/>			
DNS	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Router	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Comments	<input type="text"/>			
Active	<input type="text" value="Enable"/>			

**Figure 6.1.2: DHCPD – edit or new entry page**

DHCPD – add or edit page contain the following parameters:

- **Interface** – Click on “**Interface**” drop down menu to select interface.
- **Subnet** – Enter the interface network address.
- **IP Start** – Enter the IP address of IP start.
- **IP End** – Enter the IP address of IP end.
- **Netmask** – Enter the network mask for this network address.
- **Max Lease** – Enter the value of Max Lease.
- **Lease** – Enter the value of Lease.
- **Domain** – Enter the name of Domain.
- **DNS** – Enter the network address of DNS.
- **Router** – Enter the network address of Router.
- **Comments** – Enter the DHCPD comments.
- **Active** – Click on “**Active**” drop down menu to select enable or disable this

interface.

- **“Apply”** button to save any changes made. New settings are active after the device reboot.

DORADO CONFIDENTIAL

## 6.2 Service > Firewall

Firewall is used to allow or deny data either in or out. Figure 6.2.1 illustrates the firewall configuration page.

Active  Enable

Firewall List											
Target	Source IP	Source mask	Destination IP	Destination Mask	Protocol	Start port	End port	User Group	Comments	Active	Configure
Deny	172.23.203.0	255.255.255.0	192.168.1.81	255.255.255.255	tcp and udp	21	21	n/a	Block FTP	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 6.2.1: Firewall configuration page**

Firewall configuration contains the following parameters:

- **Active** – Enable or disable firewall service
- **“Apply”** button to save any changes made.
- **“Modify”** button to edit the current selection.
- **“Remove”** button to delete the current selection.
- **“New entry”** button to add new entry to the firewall.

Figure 6.2.2 illustrates the configuration page to edit or add new entry to the firewall.

Target	Allow ▼
Source Interface	any ▼
Destination Interface	any ▼
Source IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Source Netmask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Destination IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Destination Netmask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Protocol	Both tcp and udp ▼
Start Port	<input type="text"/> ( -1 ~ 65535 )
End Port	<input type="text"/> ( -1 ~ 65535 )
User Group:	Default ▼
Comments	<input type="text"/>
Active	Enable ▼

**Figure 6.2.2: Firewall – add page**

Firewall - add page contains the following parameters:

- **Target** – Click on “**Target**” drop down menu to allow, deny, or free target.
- **Source Interface** – Click on “**Source Interface**” drop down menu to select source interface. For example, WAN, MESH, VLAN0.....
- **Destination Interface** – Click on “**Destination Interface**” drop down menu to select destination interface. For example, WAN, MESH, VLAN0.....
- **Source IP** – Enter the source IP address.
- **Source Netmask** – Enter the network mask of source IP address.
- **Destination IP** – Enter the destination IP address.
- **Destination Netmask** – Enter the network mask of destination IP.
- **Protocol** – Click on “**Protocol**” drop down menu to select Firewall protocol.
- **Start port** – Enter the port number of start port.
- **End port** – Enter the port number of end port.

- **Comments** – Enter the Firewall comments.
- **Active** – Click on **“Active”** drop down menu to enable or disable this Firewall service.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

DORADO CONFIDENTIAL

### 6.3 Service > MAC Access

MAC Access provides another level of security by filtering the packets coming into the device. Figure 6.3.1 illustrates the MAC Access configuration page.

Active  ▾

Type  ▾

---

**MAC Access List**

MAC	Type	Comments	Active	Configuration
0a:11:5d:c9:87:ee	deny	Block User	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

---

**Figure 6.3.1: MAC Access configuration page**

MAC access configuration page contains the following parameters :

- **Active** – Enable or disable this feature.
- **Type** – Allow or deny the for this access control.
- **"Apply"** button to save any changes made.
- **"Modify"** button to edit current selection.
- **"Remove"** button to delete current selection.
- **"New Entry"** button to add new entry.
- **"Browse Active Users"** button to browse for active users that are currently associated to the access point.

Figure 6.3.2 illustrates the configuration page for edit or add new entry to the MAC access control.

MAC

Type

Comments

Active

Figure 6.3.2: MAC Access – edit page

MAC Access - edit page contain the following parameter:

- **MAC** – Enter the MAC address.
- **Type** – Click on “**Type**” drop down menu to allow or deny access MAC address.
- **Comments** – Enter MAC Access comments.
- **Active** – Click on “**Active**” drop down menu to enable or disable MAC Access.
- “**Apply**” button to save any changes made. New settings are active after the device reboot.

Figure 6.3.3 illustrates the browse active user.

MAC address	IP address	Action
00:13:02:B0:4A:8F	172.23.203.254	<input type="text" value="Allow"/> <input type="button" value="Updates"/>

Figure 6.3.3 Browse active user page

Browse active user page contains the following parameters:

- “**Refresh**” button to refresh the active user table.
- **Action** – Select allow or deny to the selected user.
- “**Updates**” button to update the entry to the mac access control

## 6.4 Service > NAT

Network address translation (NAT) involves re-writing the source and/or destination address of IP packets as they pass through this device. Figure 6.4.1 illustrates the NAT configuration page.

Active  ▾

---

**Virtual Server List**

Protocol	Port	IP	Comments	Active	Configure
tcp and udp	21	172.23.203.254	NAT To FTP Server	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 6.4.1: NAT configuration page**

NAT configuration page contains the following parameters:

- **Active** – Enable or disable NAT feature.
- **“Apply”** button to save any changes made.
- **“Modify”** button to edit current selection.
- **“Remove”** button to delete current selection.
- **“New Entry”** button to add new entry to the NAT table.

Figure 6.4.2 illustrates the add or edit page for NAT table.

Protocol  ▾

Port  (1~65535)

IP

Comments

Active  ▾

**Figure 6.4.2: NAT – add page**

NAT – add or edit page contain the following parameter:

- **Protocol** – Click on “**Protocol**” drop down menu to select NAT protocol.
- **Port** – Enter the NAT Port number.
- **IP** – Enter the NAT IP address.
- **Comments** – Enter NAT comments.
- **Active** – Click on “**Active**” drop down menu to enable or disable this NAT.
- “**Apply**” button to save any changes made. New settings are active after the device reboot.

## 6.5 Service > NTP

Network Time Protocol (NTP) is a protocol for synchronizing the system clocks over data networks. Figure 6.5.1 illustrates the NTP configuration page.

Active  ▾

Time Zone  ▾

Daylight Saving  ▾

---

**NTP Servers**

Server	Comment	Active	Configuration	
0.asia.pool.ntp.org	Default Server 1	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
1.asia.pool.ntp.org	Default Server 2	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

**Figure 6.5.1: NTP configuration page**

NTP configuration page contains the following parameters:

- **Active** – Enable or disable NTP feature
- **Time Zone** – Select the correct time zone.
- **Daylight Saving** – Enable or disable daylight saving.
- **“Apply”** button to save any changes made.
- **“Modify”** button to edit current selection.
- **“Remove”** button to delete current selection.
- **“New Entry”** button to add new entry to the NTP.

Figure 6.5.2 illustrates the configuration page for add or edit NTP server settings.



Server

Comments

Active  ▾

**Figure 6.5.2: NTP – add or edit page**

NTP add or edit page contains the following parameters:

- **Server** – Enter the NTP server name.
- **Comments** - Enter NTP server comments.
- **Active** – Click on **“Active”** drop down menu to enable or disable this NTP server.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 6.6 Service > Traffic Shaping

Traffic Shaping will limit bandwidth allocated to each user. Figure 6.6.1 illustrates the traffic shaping configuration page.

Active  Enable

WAN Uplink Speed  (Mbps)

WAN Downlink Speed  (Mbps)

User Uplink Speed  (kbps)

User Downlink Speed  (kbps)

---

Shaping List							
Protocol	Port	Min Size	Max Size	Priority	Comments	Active	Configure
1	21	1000	2000	1	Traffic Shaper	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 6.6.1: Traffic Shaping configuration page**

Traffic shaping configuration page contains the following parameters:

- **Active** – Enable or disable traffic shaping
- **WAN Uplink Speed** – Uplink speed of the device
- **WAN Downlink Speed** – Downlink speed of the device
- **User Uplink Speed** – Default user uplink speed.
- **User Downlink Speed** – Default user downlink speed.
- **“Apply”** button to save any changes made.
- **“Modify”** button to edit current selection.
- **“Remove”** button to delete current selection.
- **“New Entry”** button to add traffic shaping list.

Figure 6.6.2 illustrates the add or edit page for traffic shaping.

Protocol	<input type="text" value="tcp"/>
Port	<input type="text"/> ( 1 ~ 65535 )
Min Size	<input type="text"/> ( 1 ~ 65535 )
Max Size	<input type="text"/> ( 1 ~ 65535 )
Priority	<input type="text" value="Background"/>
Comments	<input type="text"/>
Active	<input type="text" value="Enable"/>
<input type="button" value="Apply"/>	

**Figure 6.6.2: Traffic Shaping – add or edit page**

Traffic Shaping - add or edit page contain the following parameter:

- **Protocol** – Click on “**Protocol**” drop down menu to select “tcp”, “udp”, or “both” protocol of Traffic Shaping.
- **Port** – Enter the Traffic Shaping port number.
- **Min Size** – Enter the minimum packet size of Traffic Shaping.
- **Max Size** – Enter the maximum packet size of Traffic Shaping.
- **Priority** – Click on “**Priority**” drop down menu to select priority “Background”, “Video”, “Voice” or “Best effort”.
- **Comments** – Enter Traffic Shaping comments.
- **Active** – Click on “**Active**” drop down menu to enable or disable this entry.
- “**Apply**” button to save any changes made. New settings are active after the device reboot.

## 6.7 Service > PPTP Server

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPN). Figure 6.7.1 illustrates the PPTP Server configuration page.

Active Enable ▾

Server IP 10 23 203 1

Client IP Start 10 23 203 2

Client IP End 10 23 203 11

---

**PPTP User List**

Username	IP	Comments	Active	Configuration
pptp1	0.0.0.0	Management VPN	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 6.7.1: PPTP Server configuration page**

PPTP Server configuration page contains the following parameters:

- **Active** – Enable or disable PPTP Server service.
- **Server IP** – Enter the PPTP Server IP address.
- **Client IP Start** – Enter the start of IP address for client.
- **Client IP End** – Enter the end of IP address for client.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.
- **“Modify”** button to edit current selection.
- **“Remove”** button to delete current selection.
- **“New Entry”** button to add new entry

Figure 6.7.2 illustrates the add or edit page for PPTP server

Username	<input type="text"/>
Password	<input type="password"/>
Reconfirm Password	<input type="password"/>
IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Comments	<input type="text"/>
Active	Enable <input type="button" value="v"/>
	<input type="button" value="Apply"/>

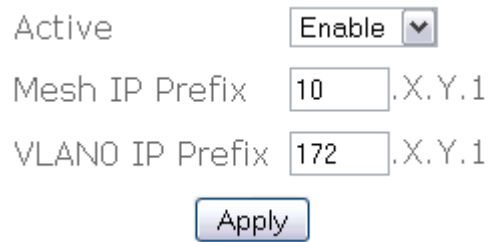
**Figure 6.7.2: PPTP User – add or edit page**

PPTP User - add page contain the following parameter:

- **Username** – Enter the PPTP username.
- **Password** – Enter the PPTP password.
- **Reconfirm Password** - Re-enter PPTP password to confirm it.
- **IP** – Enter the PPTP IP address.
- **Comments** – Enter the PPTP comments.
- **Active** – Click on “**Active**” drop down menu to enable or disable this PPTP.
- “**Apply**” button to save any changes made. New settings are active after the device reboot.

## 6.8 Service > AutoIP

AutoIP will try to assign unique IP addresses to the systems. Upon successful of autoIP, mesh IP will be assigned. IP of VLAN0 also will be modified. It'll modify the DHCPD settings to match with the VLAN0. Figure 6.8.1 illustrates the configuration page.



Active

Mesh IP Prefix  .X.Y.1

VLAN0 IP Prefix  .X.Y.1

**Figure 6.8.1: AutoIP configuration page**

AutoIP configuration page contains the following parameters:

- **Active** – Enable or disable AutoIP.
- **Mesh IP Prefix** – Assign a Mesh IP Prefix to it. Default is 10.
- **VLAN0 IP Prefix** – Assign a VLAN0 IP Prefix to it. Default is 172.
- **“Apply”** button to save any changes made. New settings will be active after reboot.

## 6.9 Service > Captive Portal

Captive portal forces an HTTP client on a network to see a special authentication web page before surfing the Internet normally. Figure 6.9.1 illustrates the captive portal configuration page.

Webbased Authentication	<input type="text" value="Disable"/>
Redirect to URL	<input type="text"/>
POP3 Email Push	<input type="text" value="Enable"/>
External Login Server	<input type="text" value="Disable"/>
External Server URL	<input type="text"/>
Default Idle Timeout	<input type="text" value="300"/> ( 0 ~ 3000000s )
Default Session Timeout	<input type="text" value="65000"/> ( 0 ~ 3000000s )
Login using HTTP	<input type="text" value="Enable"/>
HTTP Port	<input type="text" value="3000"/> ( 1000 ~ 65535 )
Login Using HTTPS	<input type="text" value="Enable"/>
HTTPS Port	<input type="text" value="3001"/> ( 1000 ~ 65535 )
Internal Web Space	<input type="text" value="Enable"/>
Web Space Port	<input type="text" value="3002"/> ( 1000 ~ 65535 )
Default Language	<input type="text" value="English"/>
Multiple Login	<input type="text" value="Disable"/>
1X LOGIN	<input type="text" value="Enable"/>
<input type="button" value="Apply"/>	

Figure 6.9.1: Captive Portal configuration page

Captive portal configuration page contains the following parameters:

- **Webbased Authentication** – Enable or disable Webbased Authentication.
- **Redirect to URL** – Enter the URL to redirect users to this URL upon success login.
- **POP3 Email Push** – Enable or disable email push to non authenticated users.

- **External Login Server** – Enable or disable external login server. A external server is required for sending the login page.
- **External Server URL** – Enter the URL of the external server.
- **Default Idle Timeout** – Enter the default idle timeout for authenticated users.
- **Default Session Timeout** – Enter the default session timeout for authenticated users.
- **Login using HTTP** – Enable or disable user login with http, unsecured method.
- **HTTP Port** – Enter the HTTP port number to be used together with http login.
- **Login using HTTPS** – Enable or disable login with https, secured method.
- **HTTPS Port** – Enter the HTTPS port number to be used together with https login.
- **Internal Web Space** – Enable or disable internal web space. Internal web space can be customize using Management > Webspaces
- **Web Space Port** – Enter the port number of Web Space service.
- **Default Language** – Select the default login language.
- **Multiple Login** – Enable enable or disable multi user login.
- **1X LOGIN** – Enable or disable 1X LOGIN.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 6.10 Service > RADIUS

Remote Authentication Dial In User Service (RADIUS) is an AAA (Authentication, Authorization and Accounting) protocol for applications such as network access or IP mobility. RADIUS client will verify authentication push by RADIUS server. Figure 6.10.1 illustrates the RADIUS client configuration page.

Active

NAS ID

Called Station ID

NAS Port  ( 1 ~ 65535 )

NAS Port Type  ( 1 ~ 65535 )

Interim Update Interval  ( 1 ~ 65535 )

---

**RADIUS Server List**

Name	Type	Port	Comments	Active	Configure	
192.168.1.81	1	1812	Authentication	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
192.168.1.81	2	1813	Accounting	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

**Figure 6.10.1: RADIUS client configuration page**

RADIUS client configuration page contains the following parameters :

- **Active** – Enable or disable RADIUS client.
- **NAS ID** – Enter the NAS ID.
- **Called Station ID** – Enter the Called Station ID.
- **NAS Port** – Enter the NAS Port number.
- **NAS Port Type** – Enter the NAS Port Type.
- **Interim Update Interval** – Enter the value of Interim Update Interval.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

- “**Modify**” button to edit RADIUS server entry.
- “**Remove**” button to delete RADIUS entry.
- “**New Entry**” button to add new entry.

Figure 6.10.2 illustrates the add or edit page for RADIUS entry.

Server Name

Server Type

Server Port  ( 1 ~ 65535 )

Server Secret

Reconfirm Server Secret

Comments

Active

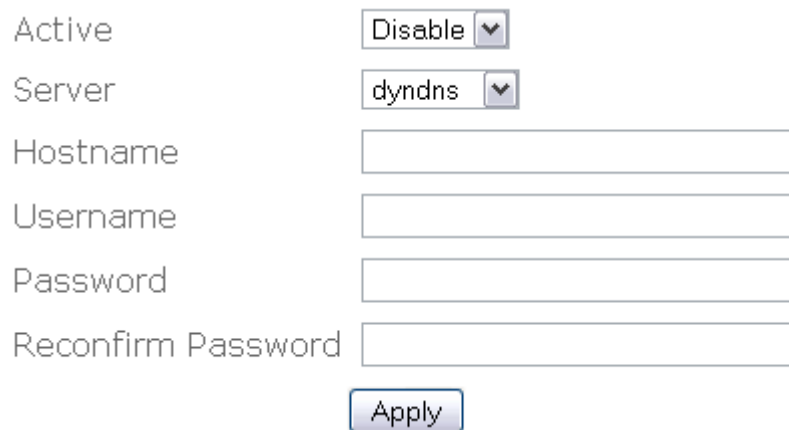
**Figure 6.10.2: RADIUS server – add or edit page**

RADIUS server - add or edit page contain the following parameter:

- **Server Name** – Enter the RADIUS server name.
- **Server Type** – Click on “**Server Type**” drop down menu to select “Authenticate” or “Accounting” server type.
- **Server Port** – Enter the number of Server Port.
- **Server Secret** – Enter the Server Secret.
- **Reconfirm Server Secret** – Re-enter the Server Secret to confirm it.
- **Comments** – Enter RADIUS server comments.
- **Active** – Enable or disable this entry.
- “**Apply**” button to save any changes made. New settings are active after the device reboot.

## 6.11 Service > Dynamic DNS

Dynamic DNS allows an Internet domain name to be assigned with a dynamic IP address. Figure 6.11.1 illustrates the Dynamic DNS configuration page.



Active	Disable ▼
Server	dyndns ▼
Hostname	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Reconfirm Password	<input type="text"/>

**Figure 6.11.1: Dynamic DNS configuration page**

Dynamic DNS configuration page contains the following parameters:

- **Active** – Enable or disable Dynamic DNS.
- **Server** – Select “dyndns”, “easydns”, “zoneedit”, or “tzo” dynamic DNS provider.
- **Hostname** – Enter the Hostname that associated with the service provide.
- **Username** – Enter the Dynamic DNS username.
- **Password** – Enter the Dynamic DNS password.
- **Reconfirm Password** – Re-enter Dynamic DNS password to confirm.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 6.12 Service > Zero Config

Figure 6.12.1 illustrates the Zero Config configuration page.

The screenshot shows the Zero Config configuration page with the following settings:

Active	Disable
Handle Client Proxy	Disable
Proxy Login Port	8080 ( 1000 ~ 65535 )
Handle Static IP Client	Disable

Below the settings is an "Apply" button.

**Figure 6.12.1: Zero Config configuration page**

Zero Config configuration page contains the following parameters:

- **Active** – Enable or disable Zero Config service.
- **Handle Client Proxy** – Enable or disable handling of proxy clients.
- **Proxy Login Port** – Enter the port number used in Proxy Login.
- **Handle Static IP Client** – Enable or disable handling of client with static IP.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 6.13 Service > Mobile IP

Mobile IP provide client with IP roaming capability. Client will have same IP no matter which node it reside. Figure 6.13.1 illustrates the mobile IP configuration page.



Active  ▾

Netname

Network  ▾

MLRD IP

**Figure 6.13.1: Mobile IP configuration page**

Mobile IP configuration page contains the following parameters:

- **Active** – Enable or disable Mobile IP service.
- **Netname** – Enter the Mobile IP network name.
- **Network** – Select the interface mobile ip should attached to.
- **MLRD IP** – Enter the IP address of the Mobile Location Register server.
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 6.14 Service > Route Watchdog

Route watchdog will probe for default route periodically. If not default route is detected, it'll change the essid of active wireless radio to a desired value such as "ServiceDown". Figure 6.14.1 illustrates the route watchdog configuration page.

Active	<input type="button" value="Disable"/> ▾
Alert SSID	<input type="text" value="ServiceDown"/>
Interval	<input type="text" value="30"/> ( 10 ~ 60 s )
Reboot Device	<input type="button" value="Enable"/> ▾
Number Of Interval	<input type="text" value="0"/>
	<input type="button" value="Apply"/>

**Figure 6.14.1: Routedog configuration page**

Routedog configuration page contains the following parameters:

- **Active** – Enable or disable routedog service.
- **Alert SSID** – Specify the desired Alert SSID.
- **Interval** – Specify the interval for the routedog to check for the default route.
- **Reboot Device** – Enable or disable reboot device once routedog is triggered.
- **"Apply"** button to save any changes made. Please reboot to enable new settings.

## 6.15 Service > Linux Kernel Watchdog

Linux kernel watchdog will constantly monitor the integrity of the system. During system locked up, kernel watchdog will trigger a system reboot to recover the system from failure. Figure 6.15.1 illustrates the linux kernel watchdog configuration page.



Active

Interval  ( 10 ~ 60 s )

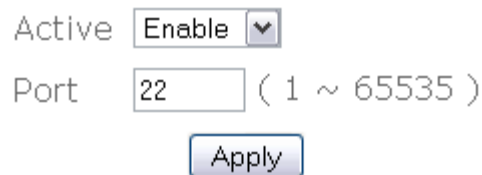
Figure 6.15.1: Lindog configuration page

Linux kernel watchdog configuration page contains the following parameters:

- **Active** – Enable or disable this service.
- **Interval** – Specify the interval watchdog will pool for system status.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.

## 6.16 Service > SSHD

SSHD provides remote management using command line interface (CLI). Figure 6.16.1 illustrates the SSHD configuration page.



Active

Port  ( 1 ~ 65535 )

**Figure 6.16.1: SSHD configuration page**

SSHD configuration page contains the following parameters:

- **Active** – Enable or disable this service.
- **Port** – Specify the TCP/IP port that the SSHD will listen for incoming connection.
- **“Apply”** button to save any changes. Please reboot to enable new settings.

## 6.17 Service > WME

Based on 802.11e draft standard. It provides basic quality of service (QoS) features to 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort, and background.

However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones. Figure 6.17.1 illustrates the WME configuration page.

**Active Wireless Interface List**

Interface	Comments	Configure
MESH0	Default Mesh	<input type="button" value="Modify"/>
AP1	VAP1	<input type="button" value="Modify"/>

**Figure 6.17.1: WME configuration page**

WME configuration page contains the following parameters:

- **“Modify”** button to edit the current selection of the active wireless interface list.

Figure 6.17.2 illustrates the edit page for WME parameters.

Interface MESH0  
 Comments default adhoc

Access Class	CWMIN (0 ~ 255 ms)	CWMAX (0 ~ 255 ms)	AIFS (0 ~ 255 ms)	TX OP LIMIT (0~65535 ms)	ACM	NO ACK POLICY
Best Effort	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="2"/>	<input type="text" value="2048"/>	<input type="button" value="Enable"/>	<input type="button" value="Enable"/>
Best Effort (BSS)	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>		
Background	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="2"/>	<input type="text" value="2048"/>	<input type="button" value="Enable"/>	<input type="button" value="Enable"/>
Background (BSS)	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>		
Video	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="button" value="Enable"/>	<input type="button" value="Enable"/>
Video (BSS)	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>		
Voice	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="button" value="Enable"/>	<input type="button" value="Enable"/>
Voice (BSS)	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>		

**Figure 6.17.2: WME - edit page**

WME – edit page contains the following parameters:

- **Interface** – Specify the interface for WMM.
- **Comments** – Optional comments for this entry.
- **Active** – Enable or disable WME.
- **CWMIN** – Minimum contention window. This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- **CWMAX** – Maximum contention window. Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value.
- **AIFS** – The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames.
- **TX OP LIMIT** – Transmission Opportunity is an interval of time when a WME AP/station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP); that is, the interval of time when the WMM AP/station as the right to initiate transmissions on the wireless network.
- **ACM** – Enable or disable Admission Control
- **NO ACK POLICY** – Enable or disable No-acknowledgement
- **Best Effort** – AP side, low priority, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue.
- **Video** – AP side, high priority, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Voice** – AP side, high priority. Time-sensitive data like VoIP and streaming media are automatically sent to this queue.
- **Best Effort (BSS)** – Station side, low priority, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue.

- **Background (BSS)** – Station side, medium priority, medium throughput and delay. Most traditional IP data is sent to this queue.
- **Video (BSS)** – Station side, high priority, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Voice (BSS)** – Station side, high priority. Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

DORADO CONFIDENTIAL

## 6.18 Service > DHCP Relay

For a dynamic network, M9000 4000 is able to forward the DHCP request to a backend DHCP server when operating in layer 2 mode. Figure 6.18.1 illustrates the configuration page for DHCP Relay.

Active	<input type="text" value="Enable"/>	
Port	<input type="text" value="67"/>	( 1 ~ 65535 )
Hop count	<input type="text" value="10"/>	( 1 ~ 255 )
Max packet size	<input type="text" value="1400"/>	( 600 ~ 1400 )
<input type="button" value="Apply"/>		

---

<b>DHCRELAY List</b>					
<b>Server/Interface</b>	<b>Extra</b>	<b>Comment</b>	<b>Active</b>	<b>Configure</b>	
Interface	vlan0	DHCP Relay	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

**Figure 6.18.1 DHCP Relay Settings**

DHCP Relay contains the following parameters:

- **Active:** Enable or disable DHCP Relay feature.
- **Port:** Port to listen for DHCP packet. Default value is 67.
- **Hop count:** Number of hop the DHCP discover packet can travel before it is dropped by this device. Default value is 10.
- **Max packet size:** Maximum packet size of the DHCP discover packet. Normally specify a large number of packet size is recommended. Default value is 1400.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.
- **“Modify”** button to edit current selection.
- **“Remove”** button to delete current selection.
- **“New Entry”** button to add server IP or Interface.

Figure 6.18.2 illustrates the add or edit configuration page.

Type	Interface ▼
Interface Name	MESH ▼
Comments	<input type="text"/>
Active	Enable ▼
<input type="button" value="Apply"/>	

**Figure 6.18.2 Server or Interface configuration page.**

The add or edit configuration page contains the following parameters.

- **Type** – Server IP or interface list
- **Interface Name** – Once the “type” drop down menu is changed to interface, interface name selection drop down menu will appear for the users to make selection on the interface where the DHCP server can be reach. The interface also must include the interface where the client can be reach.
- **IP** – Specify the IP address of the backend DHCP server.
- **Comments** – Additional comments on this entry.
- **Active** – Enable or disable this entry.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.

## 7 Management

### 7.1 Management > HTTPD

Webbased configuration management is done through the secure HTTP. Figure 7.1.1 illustrates the HTTPD server configuration page.

Active

Port  ( 1 ~ 65535 )

Username

Password

Reconfirm Password

Certificate Password

Reconfirm Certificate Password

Access Control

---

**Access Control List**

Device	Subnet	Netmask	Comments	Active	Configure	
MESH	-	-	Mesh	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
WAN	-	-	WAN	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
VLAN0	-	-	VLAN	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

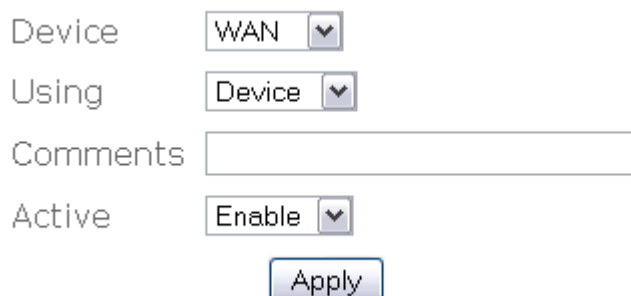
**Figure 7.1.1: HTTPD server configuration page**

HTTPD server configuration page contains the following parameters:

- **Active** – Enable or disable HTTPD server.
- **Port** – Enter the HTTPD port number.
- **Username** – Enter the HTTPD username.
- **Password** – Enter the HTTPD password.
- **Reconfirm Password** – Re-enter password to confirm it.
- **Certificate Password** – Enter the certificate password.

- **Reconfirm Certificate Password** – Re-enter certificate password to confirm it.
- **Access Control** – Enable or disable access control.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.
- **“Modify”** button to edit current selection.
- **“Remove”** button to edit current selection.
- **“New Entry”** button to add entry to the access control table.

Figure 7.1.2 illustrates the access control configuration page.



Device

Using

Comments

Active

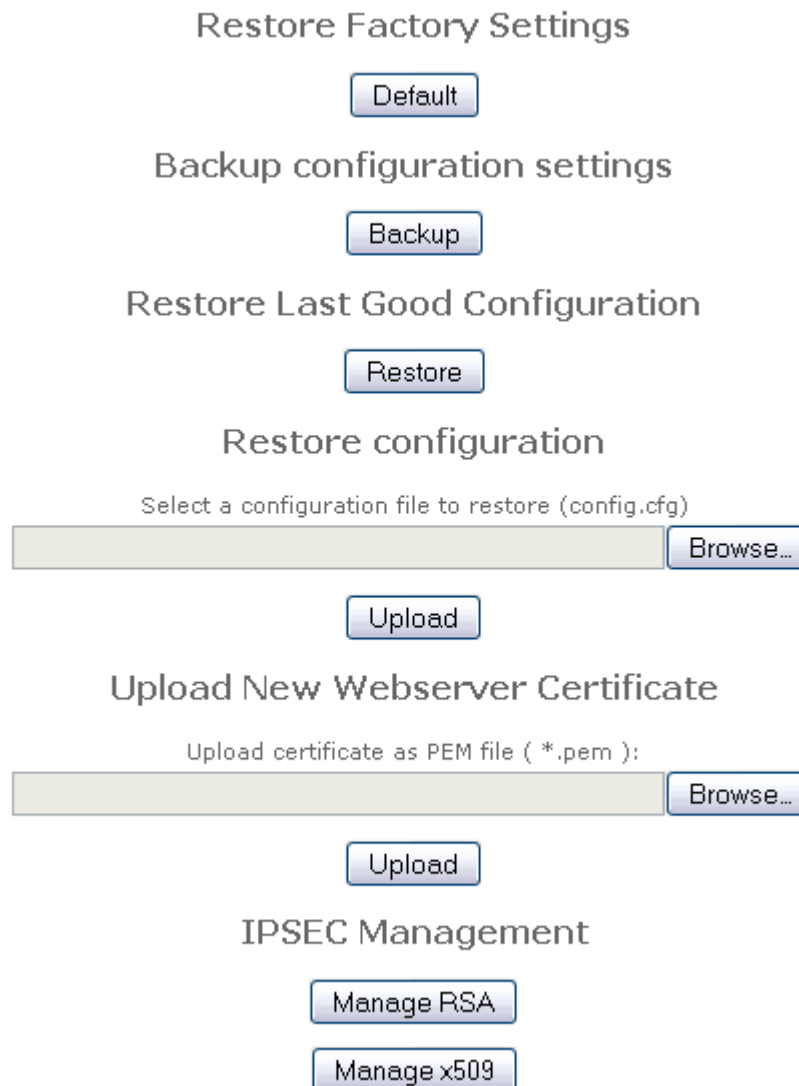
**Figure 7.1.2: HTTPD Access Control – add or edit page**

HTTPD Access Control page contains the following parameters:

- **Device** – Click on **“Device”** drop down menu to select device. For example WAN, MESH, VLAN0.....
- **Using** – Click on **“Using”** drop down menu to select using **“Device”** or **“Network”**.
- **Subnet** – Specify subnet to access or deny access HTTPD server configuration page.
- **Netmask** – Specify netmask for this subnet
- **Comments** – Enter comments for this entry.
- **Active** – Enable or disable this entry.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.

## 7.2 Management > Configuration

Under this configuration menu, you can perform the following action. Figure 7.2.1 illustrates the configuration page.



The screenshot displays the Configuration page with the following sections and buttons:

- Restore Factory Settings**
  - Default
- Backup configuration settings**
  - Backup
- Restore Last Good Configuration**
  - Restore
- Restore configuration**
  - Select a configuration file to restore (config.cfg)
  - Browse...
  - Upload
- Upload New Webserver Certificate**
  - Upload certificate as PEM file ( \*.pem ):
  - Browse...
  - Upload
- IPSEC Management**
  - Manage RSA
  - Manage x509

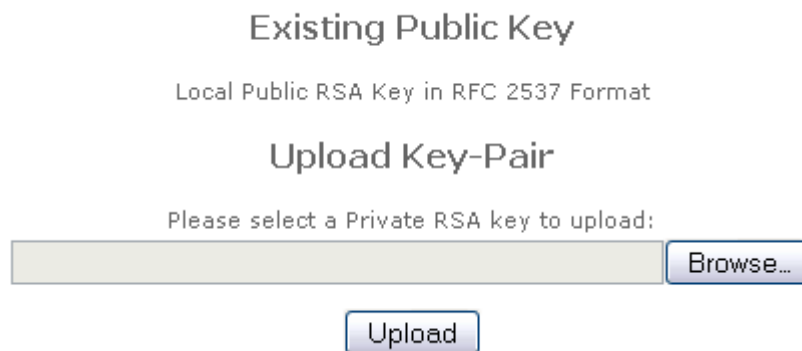
Figure 7.2.1: Configuration page

Configuration page contains the following parameters:

- **“Default”** button to restore factory default settings.
- **“Backup”** button to save configuration settings file (config.cfg).
- **“Restore”** button to restore configuration to last good configuration.

- **“Browse”** & **“Upload”** button to perform file searching and uploading.
- **“Manage RSA”** button to manage RSA certificates.
- **“Manage x509”** button to manage x509 related certificates.

Figure 7.2.2 illustrates the IPSEC management configuration page.



Existing Public Key

Local Public RSA Key in RFC 2537 Format

Upload Key-Pair

Please select a Private RSA key to upload:

Browse...

Upload

**Figure 7.2.2: IPSEC Management – RSA page**

IPSEC Management – RSA page contain the following parameter:

- **Existing Public Key** – Display the local public RSA key format.
- **Upload Key-Pair** – Click on **“Browse...”** button to browse and select private RSA key. Then, click on **“Upload”** button to upload selected private RSA key.

Figure 7.2.3 illustrates the IPSEC Management x509 configuration page.

### Local Certificate

Existing local certificate:  
None

Existing root certificate authority:  
None

Upload certificate as PKCS 12 file (Extension \*.p12):

### Remote Certificate

This certificate is required as it will be used to authenticate the server.

Existing Certificate:  
None

Upload remote certificate as PEM file (Extension \*.pem):

**Figure 7.2.3: IPSEC Management – x509 page**

IPSEC Management – x509 page contain the following parameter:

- **Local Certificate** – Display existing local certificate and existing root certificate authority. Click on “**Browse...**” button to browse and select certificate as PKCS 12 file. Then, click on “**Upload**” button to upload selected certificate.
- **Remote Certificate** - Display existing certificate. Click on “**Browse...**” button to browse and select remote certificate as PEM file. Then, click on “**Upload**” button to upload selected certificate.

### 7.3 Management > SNMP

Simple Network Management Protocol (SNMP) used to monitor devices for conditions that warrant administrative attention. Figure 7.3.1 illustrates the SNMP configuration page.

Active	<input type="button" value="Enable"/>
Version	<input type="button" value="all"/>
Port	<input type="text" value="161"/> ( 1 ~ 65535 )
v2 Read Community	<input type="text" value="....."/>
Reconfirm v2 Read Community	<input type="text" value="....."/>
v2 Read-write Community	<input type="text" value="....."/>
Reconfirm v2 Read-write Community	<input type="text" value="....."/>
v3 Read Username	<input type="text" value="snmpv3rouser"/>
v3 Read-write Username	<input type="text" value="snmpv3rwuser"/>
v3 Password	<input type="text" value="....."/>
Reconfirm v3 Password	<input type="text" value="....."/>
v3 Passphrase	<input type="text" value="....."/>
Reconfirm v3 Passphrase	<input type="text" value="....."/>
Access Control	<input type="button" value="Enable"/>

---

**Access Control List**

Device	Subnet	Netmask	Comments	Active	Configure	
MESH	-	-	Mesh	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
WAN	-	-	WAN	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
VLAN0	-	-	VLAN	Enabled	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

**Figure 7.3.1: SNMP configuration page**

SNMP configuration page contains the following parameters:

- **Active** – Enable or disable SNMP management.
- **Version** – Select “v1 or v2c”, “v3”, or “all” SNMP version.
- **Port** – Enter the SNMP port number.
- **v2 Read Community** – Enter the v2 Read Community.
- **Reconfirm v2 Read Community** – Re-enter v2 Read Community to verify.
- **v2 Read-write Community** – Enter the v2 Read-write Community.
- **Reconfirm v2 Read-write Community** – Re-enter v2 Read-write Community for verification.
- **v3 Read Username** – Enter the v3 Read Username.
- **v3 Read-write Username** – Enter the v3 Read-write Username.
- **v3 Password** – Enter the v3 Password.
- **Reconfirm v3 Password** – Re-enter v3 Password for verification.
- **v3 Passphrase** – Enter the v3 Passphrase.
- **Reconfirm v3 Passphrase** – Re-enter v3 Passphrase for verification.
- **Access control** – Enable or disable SNMP access control.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.
- **“Modify”** button to edit access control entry.
- **“Remove”** button to remove access control entry.
- **“New Entry”** button to add new access control rule.

Figure 7.3.2 illustrates the access control configuration page for SNMPD



The image shows a configuration form for SNMP access control. It includes the following fields and controls:

- Device**: A dropdown menu with "WAN" selected.
- Using**: A dropdown menu with "Device" selected.
- Comments**: A text input field.
- Active**: A dropdown menu with "Enable" selected.
- Apply**: A button to save the configuration.

**Figure 7.3.2: SNMP Access Control – add or edit page**

SNMP Access Control – add or edit page contains the following parameters:

- **Device** - Click on “**Device**” drop down menu to select device. For example, WAN, MESH, VLAN0.....
- **Using** - Click on “**Using**” drop down menu to select “Device” or “Network”.
- **Subnet** – Specify subnet to access or deny access SNMP server.
- **Netmask** – Specify netmask for this subnet.
- **Comments** - Enter comments for this entry.
- **Active** - Click on “**Active**” drop down menu to enable or disable this entry.
- “**Apply**” button to save any changes made. Please reboot to enable new settings.

## 7.4 Management > Firmware

Under firmware upgrade management. You can view the current firmware release version, update latest firmware. Please note that do not power off the device while upgrading the firmware. Otherwise you'll render this device unrecoverable. The firmware process will take around 6 minutes to complete. Figure 7.4.1 illustrates the Firmware Upgrade page.

**Caution! Do not switch off the device while upgrading the firmware.**

**Current Version:** mesh-2.1.12  
Select a firmware to upgrade:

**Figure 7.4.1: Firmware Upgrade page**

Firmware Upgrade process:

- Click on **“Browse...”** button to browse and select firmware to upgrade.
- Click on **“Upgrade”** button upgrade selected firmware.
- **“Current Version”** display current firmware revision number.

## 7.5 Management > Trap

Trap used to report an alert or other asynchronous event about managed system.

Figure 7.5.1 illustrates the trap configuration page.

Active	Enable	▼
Configuration	Enable	▼
Security	Enable	▼
Wireless	Enable	▼
Operational	Enable	▼
Flash	Enable	▼
Tftp	Enable	▼
Image	Enable	▼
Auth failure	Enable	▼

---

**Trap Server List**

Version	Trap to	Comments	Active	Configure
2c	192.168.1.81	Trap Server	Enabled	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 7.5.1: Trap configuration page**

Trap configuration page contains the following parameters:

- **Active** – Enable or disable trap report.
- **Configuration** – Enable or disable report on configuration issue.
- **Security** – Enable or disable security trap report.
- **Wireless** – Enable or disable wireless trap report.
- **Operational** – Enable or disable operational trap report.
- **Flash** – Enable or disable flash trap report.
- **Tftp** – Enable or disable tftp trap report.

- **Image** – Enable or disable image trap report.
- **Auth failure** – Enable or disable authentication failure trap report.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.
- **“Modify”** button to edit trap server entry.
- **“Remove”** button to delete trap server entry.
- **“New Entry”** button to add new server entry.

Figure 7.5.2 illustrates the configuration page for add or delete trap server.

The screenshot shows a configuration form for a trap server. It includes the following fields and controls:

- IP**: Four separate input boxes for entering the IP address.
- Community**: A single text input field.
- Reconfirm Community**: A single text input field.
- Version**: A dropdown menu currently set to "2c".
- Comments**: A large text area for entering notes.
- Active**: A dropdown menu currently set to "Enable".
- Apply**: A button to save the configuration.

**Figure 7.5.2: Trap server – add or edit page**

Trap server – add or edit page contain the following parameter:

- **IP** – Enter destination IP to send trap.
- **Community** – Enter community of trap.
- **Reconfirm Community** – Re-enter community to confirm it.
- **v3 Username** – Enter v3 username.
- **v3 Password** – Enter v3 user password.
- **Reconfirm v3 Password** – Re-enter password to confirm it.
- **v3 Passphrase** – Enter v3 user passphrase.
- **Reconfirm v3 Passphrase** – Re-enter passphrase to confirm it.
- **Version** – SNMP Version.
- **Comments** – Enter Trap comments.

- **Active** – Enable or disable this entry.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.

DORADO CONFIDENTIAL

## 7.6 Management > User group

Users within a predefined user group will share the common parameter of the group. This allows administrator to create various types of user groups depending on their needs. Figure 7.6.1 illustrates the user group configuration page.

Default Upload Speed Limit  (Kbps)

Default Download Speed Limit  (Kbps)

Default Idle Timeout  (0-3000000s)

Default Session Timeout  (0-3000000s)

Redirect to URL

User Groups List								
Name	Language	Upload Limit	Download Limit	Idle Timeout	Session Timeout	URL	Comment	Configure
TG	English	256	500	200	6000	www.google.com	Test Group	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 7.6.1 User Group configuration**

There are one default group which is listed on figure 7.6.1. To configure the default parameters for default group:-

- **Default Upload Speed Limit** – Upload speed limit in kbps for users in this group.
- **Default Download Speed Limit** – Download speed limit in kbps for users in this group.
- **Default Idle Timeout** – Auto logout when user idle , with no activity for the period of time defined.
- **Default Session Timeout** – Logout user when the session of the login expired for the period of time defined.
- **Redirect to URL** – Redirect user to this URL when login is successful.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.
- **“Modify”** button to edit selected user group.
- **“Remove”** button to delete selected user group.
- **“New Entry”** button to add entry to user group.

Figure 7.6.2 illustrates the configuration page for user group entry.

Name	<input type="text"/>
Language	English <input type="button" value="v"/>
Upload Speed Limit	<input type="text"/> (Kbps)
Download Speed Limit	<input type="text"/> (Kbps)
Idle Timeout	<input type="text"/> (0-3000000s)
Session Timeout	<input type="text"/> (0-3000000s)
Redirect To Url	<input type="text"/>
Comments	<input type="text"/>
<input type="button" value="Apply"/>	

**Figure 7.6.2 User group edit page**

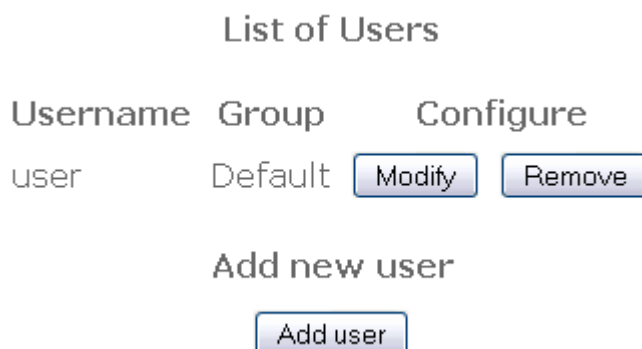
User group edit page contains the following parameters:

- **Name** – Alias for this group.
- **Language** – Language option for this group.
- **Upload Speed Limit** – Upload limit in kbps for users in this group.
- **Download Speed Limit** – Download limit in kbps for users in this group.
- **Default Idle Timeout** – Auto logout when user idle , with no activity for the period of time defined.
- **Default Session Timeout** – Logout user when the session of the login expired for the period of time defined.
- **Redirect to URL** – Redirect user to this URL when login is successful.
- **Comments** – Additional comments for this group entry.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.

## 7.7 Management > Database

Database contains list of local users that are currently configured to the database.

Database - Users page is shown in Figure 7.7.1.



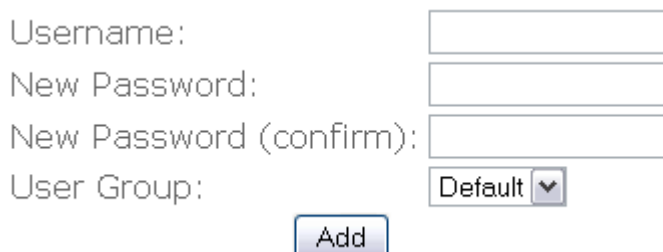
The screenshot shows a web interface titled "List of Users". It features a table with columns for "Username", "Group", and "Configure". A single user named "user" is listed with the "Default" group. To the right of the "user" entry are two buttons: "Modify" and "Remove". Below the table, there is a section titled "Add new user" with a single "Add user" button.

**Figure 7.7.1: Database - Users page**

Database configuration page contains the following parameters:

- **List of Users** – Display list of users currently in the database.
- **“Modify”** button to edit the selected user.
- **“Remove”** button to delete the selected user.
- **“Add user”** button to add new user to database.

Figure 7.7.2 illustrates the configuration page for add or edit user.



The screenshot shows a web form for adding a user. It includes four input fields: "Username:", "New Password:", "New Password (confirm):", and "User Group:". The "User Group:" field is a dropdown menu currently set to "Default". Below the fields is an "Add" button.

**Figure 7.7.2: Database – Add user page**

Add user configuration page contains the following parameters:

- **Username** – Enter new username.
- **New Password** – Enter new user password.
- **New Password (confirm)** – Re-enter new user password to confirm it.

- **“Add”** button to add new user.

DORADO CONFIDENTIAL

## 7.8 Management > Webspaces

EnGenius Mesh AP's Captive portal is capable to store local web content. Webspaces management is used to manage local web content. Figure 7.8.1 illustrates the webspaces configuration page.

The screenshot displays the 'Existing files' section with a table:

File	Actions
index.html	<input type="button" value="Delete"/>

Below this is the 'Upload File' section, which includes a 'Filename:' label, a text input field, a 'Browse...' button, and an 'Upload' button.

**Figure 7.8.1: Management –Webspaces management**

Webspaces management contains the following parameters:

- **Existing files** – display existing webspaces file.
- **“Delete”** button to delete existing webspaces file.
- **“Browse”** button to search webspaces file that want to upload.
- **“Upload”** button to upload webspaces file.

## 7.9 Management > Customize Login

Customize login page is used to modify look and feel for the captive portal login page of EnGenius Mesh. Figure 7.9.1 illustrates the customize login page.

### Existing files

Directory: /lang

File	Description	Actions
Common	Directory, containing language independent files that are displayed before login.	
English	Directory for language English.	<input type="button" value="Delete"/>
style.css	User file	<input type="button" value="Delete"/>

### Upload File

Filename:

### Add Language

New Language:

### Default Language

Login Language  
(If not supplied by the RADIUS):

**Figure 7.9.1: Customize Login configuration page.**

Customize Login configuration page contains the following parameters:

- **Existing files** – display existing login file.
- **“Delete”** button to delete existing login file.
- **“Browse”** button to search login file that want to upload.

- **“Upload”** button to upload login file.
- **New Language** – Type in new language
- **“Add”** button to add new language.
- **“Login Language”** to choose default login language.
- **“Change”** button to save any changes made.

DORADO CONFIDENTIAL

## 7.10 Management > NMS Addresses

NMS address is used for the system to report back to Network Management System located outside of the network. Figure 7.10.1 illustrates the NMS server address configuration page.

NMS Address List						
Address	Port	Interval	Comments	Active	Configuration	
192.168.1.81	8188	60	NMS Server	Enabled	Modify	Remove

New Entry

Figure 7.10.1 NMS Address List

NMS address configuration page contains the following parameters:

- **NMS Address List** – List of NMS server.
- **“Modify”** button to edit the selected entry.
- **“Remove”** button to delete the selected entry.
- **“New Entry”** button to add new entry to the NMS server.

Figure 7.10.2 illustrates the NMS address configuration page for add or edit.

Address

Port

Interval  (60-300000s)

Comments

Active

Figure 7.10.2: NMS Addresses – add or edit page

NMS Address – add page contain the following parameter:

- **Address** – Enter the IP address of the NMS server.
- **Port** – Enter the port of the NMS server which is waiting for the report.
- **Interval** – Enter the interval of report to NMS server.

- **Comments** – Enter comments for the entry.
- **Active** – Enable or disable this entry.
- **“Apply”** button to save any changes made. Please reboot to enable new settings.

DORADO CONFIDENTIAL

## 7.11 Management > Reboot

You can perform system reboot here. Figure 7.11.1 illustrates the reboot page.



**Figure 7.11.1: Reboot page**

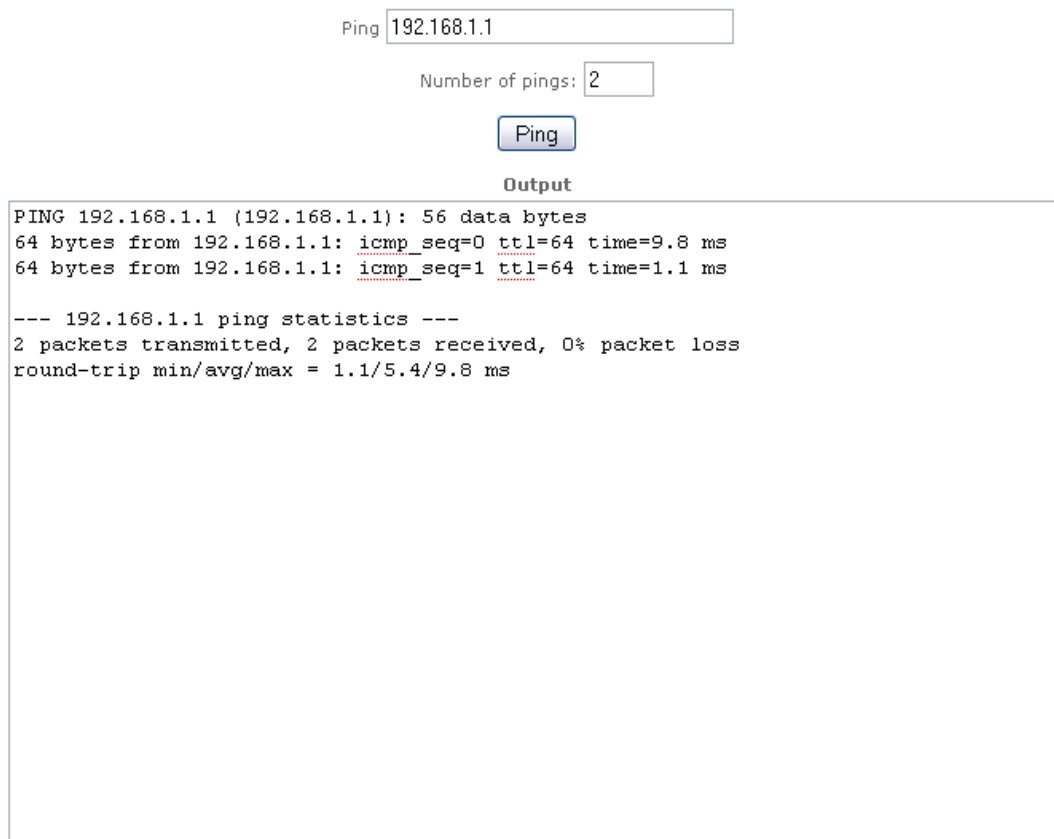
Reboot page contains the following parameters:

- **“Reboot”** button to reboot the device.

## 8 Tools

### 8.1 Tools > Ping

Figure 8.1.1 illustrates the ping page.



Ping

Number of pings:

**Output**

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=9.8 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.1 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 1.1/5.4/9.8 ms
```

**Figure 8.1.1: Ping page**

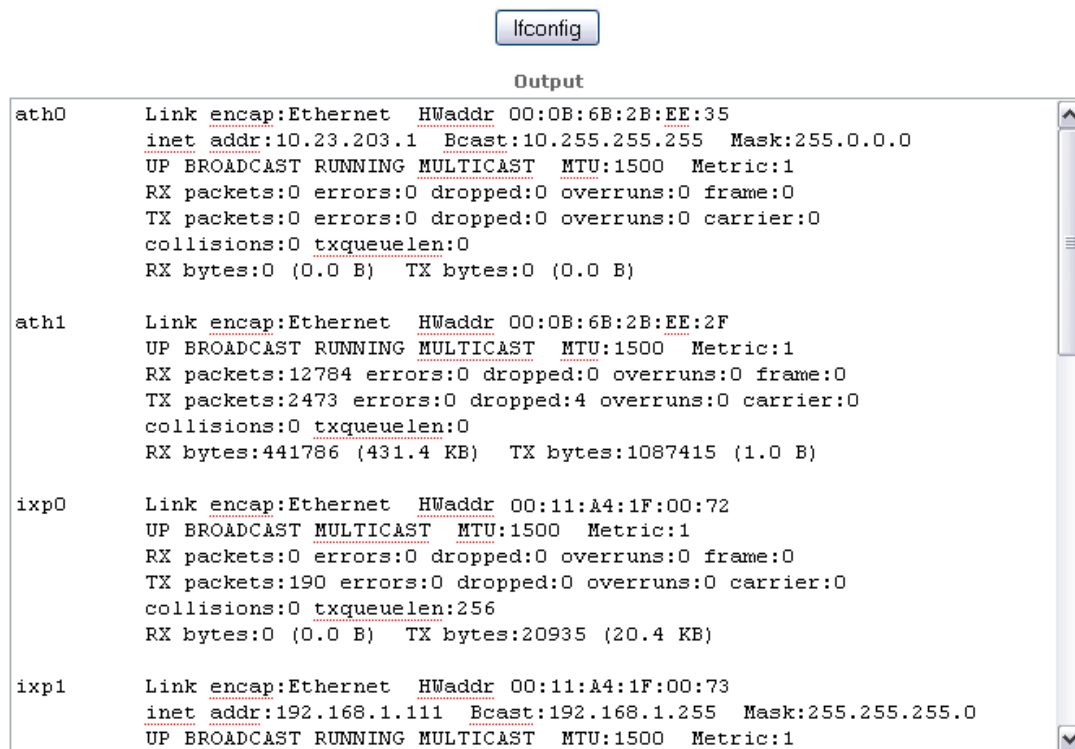
Ping page contains the following parameters:

- **Ping** – Enter the IP address to ping.
- **Number of pings** – Enter the number of pings to send.
- **“Ping”** button to ping and display output of ping command.
- **“Output”** text area display result of the ping command.

## 8.2 Tools > Ifconfig

Ifconfig page is used to collect verbose information about device network interfaces.

Figure 8.2.1 illustrates the ifconfig page.



The screenshot shows a web interface with a button labeled "Ifconfig" at the top. Below the button is a text area titled "Output" containing the following text:

```
ath0      Link encap:Ethernet  HWaddr 00:0B:6B:2B:EE:35
          inet addr:10.23.203.1  Bcast:10.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ath1      Link encap:Ethernet  HWaddr 00:0B:6B:2B:EE:2F
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2473 errors:0 dropped:4 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:441786 (431.4 KB)  TX bytes:1087415 (1.0 B)

ixp0      Link encap:Ethernet  HWaddr 00:11:A4:1F:00:72
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256
          RX bytes:0 (0.0 B)  TX bytes:20935 (20.4 KB)

ixp1      Link encap:Ethernet  HWaddr 00:11:A4:1F:00:73
          inet addr:192.168.1.111  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Figure 8.2: Ifconfig page

Ifconfig page contains the following parameters:

- “Ifconfig” button to call ifconfig command.
- “Output” text area to display the output of the command.

### 8.3 Tools > Route

Route page is used to collect information about device's routing table. Figure 8.3.1 illustrates the route page.

**Output**

```
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0      0.0.0.0        255.255.255.0  U      0      0      0    ixp1
172.23.203.0    0.0.0.0        255.255.255.0  U      0      0      0    vlan0
10.0.0.0         0.0.0.0        255.0.0.0      U      0      0      0    ath0
127.0.0.0       0.0.0.0        255.0.0.0      U      0      0      0    lo
224.0.0.0       0.0.0.0        240.0.0.0      U      0      0      0    ixp1
0.0.0.0         192.168.1.2    0.0.0.0        UG     0      0      0    ixp1
```

**Figure 8.3.1: Route page**

Route page contains the following parameters:

- **“Route”** button to display output of route command.
- **“Output”** text area display result of the route command.

## 8.4 Tools > TFTP

Figure 8.4.1 illustrates the TFTP page.

Use TFTP to get or put file to a remote TFTP server  
Getting of firmware will result in firmware upgrade follow by system reboot.  
Getting of config will result in configuration upgrade.

TFTP to

Operation  ▼

File Name

Type of File  ▼

**Figure 8.4.1: TFTP page**

TFTP contains the following parameters:

- **TFTP to** – Enter the destination IP address of remote TFTP server.
- **Operation** – Select “put”, “get” or “get and reboot” file to remote TFTP server.
- **File Name** – Enter the File Name to put or get.
- **Type of File** – Select “config”, “firmware”, “ipsec x509 local”, “ipsec x509 remote”, or “ipsec rsa” file.
- **Execute** button to perform directed action.

## 9 Status

### 9.1 Status > Status

Status page will display current system status of Mesh AP. Figure 9.1.1 illustrates the system status page.

System Uptime:	0 days, 0 hrs, 3 minutes
CPU Speed:	527.56
Average CPU usage: (Since boot)	83.00 %
Average CPU usage: (Last two seconds)	14.77 %
Free RAM:	48340992 byte
Firmware Release Version	mesh-2.1.12

Figure 9.1.1: System Status page

System Status will display system uptime in format: day, hours, minute. For example, “Uptime0 days, 2 hrs, 17 minutes”

### 9.2 Status > Interfaces

Figure 9.2.1 illustrates the interface page. Active interface will be listed under the interface page.

Interface ixp1 (WAN)	<a href="#">Get Details</a>
Interface ath0 (MESH)	<a href="#">Get Details</a>
Interface vlan0 (Client Access)	<a href="#">Get Details</a>

Figure 9.2.1: Interface page

Interface page contains the following parameters:

- “**Get Details**” button to obtain details on the selected interface.

Figure 9.2.2 illustrates the details when interface `ixp0` ( WAN ) is selected.

Hardware Address:	00:11:A4:1F:00:73
IP Type:	dhcp
IP Address:	192.168.1.111
Broadcast Address:	192.168.1.255
Netmask:	255.255.255.0
MTU:	1500
Rx bytes:	38800 (37.8 KB)
Tx bytes:	9716 (9.4 KB)
Rx packets:	504
Tx packets:	101
Rx errors:	0
Tx errors:	0
Rx dropped:	0
Tx dropped:	0

**Figure 9.2.2: Details of interface `ixp0` ( WAN ).**

Interface `ixp1` page contain the following parameter:

- **Hardware Address** – Display the hardware address of interface.
- **IP Type** – Interface get IP via which way (like DHCP).
- **IP Address** – Display the IP address of interface.
- **Broadcast Address** – Display the broadcast address of interface.
- **Netmask** – Display the network mask of this IP.
- **MTU** – Display MTU value of interface.
- **Rx bytes** – Display Rx bytes value of interface.
- **Tx bytes** – Display Tx bytes value of interface.
- **Rx packets** – Display Rx packets value of interface.
- **Rx errors** – Display Rx errors value of interface.
- **Rx dropped** – Display Rx dropped value of interface.

### 9.3 Status > Services

Figure 9.3.1 illustrates the status of each service running in the device.

**Status**

Service	Status
DHCP Server	O.k.
DNS Server	O.k.
Dynamic DNS	Disabled
IPSEC	Disabled
L2TPC	Disabled
MobileIP	Disabled
NTP Client	O.k.
OLSR	O.k.
PPPoE	Disabled
PPTP Server	O.k.
Routedog	Disabled
SSHD	O.k.
SNMP Server	O.k.
Syslog Server	O.k.
Traffic shaping	O.k.
Webservers	O.k.

**Figure 9.3.1: Services page**

Services page display status of each service. Services page contains the following parameters:

- **DHCP Server**
- **DNS Server**
- **Dynamic DNS**
- **IPSEC**
- **L2TPC**
- **Mobile IP**
- **NTP Client**
- **OLSR**

- **PPPoE**
- **PPTP Server**
- **Routedog**
- **SSHD**
- **SNMP Server**
- **Syslog Server**
- **Traffic Shaping**
- **Webservers**

DORADO CONFIDENTIAL

## 9.4 Status > Users

Figure 9.4.1 illustrates the status of logged in users.

List of Users		
Username	IP Address	Actions
user	172.23.203.254	<a href="#">Logout</a>

**Figure 9.4.1: Users status page**

Users status page contains the following parameters:

- **List of Users** – list of authenticated users
- **<user name hyperlink>** - details of the users
- **“Logout”** button to logout the selected user.

Figure 9.4.2 illustrates the details of the selected user.

172.23.203.254

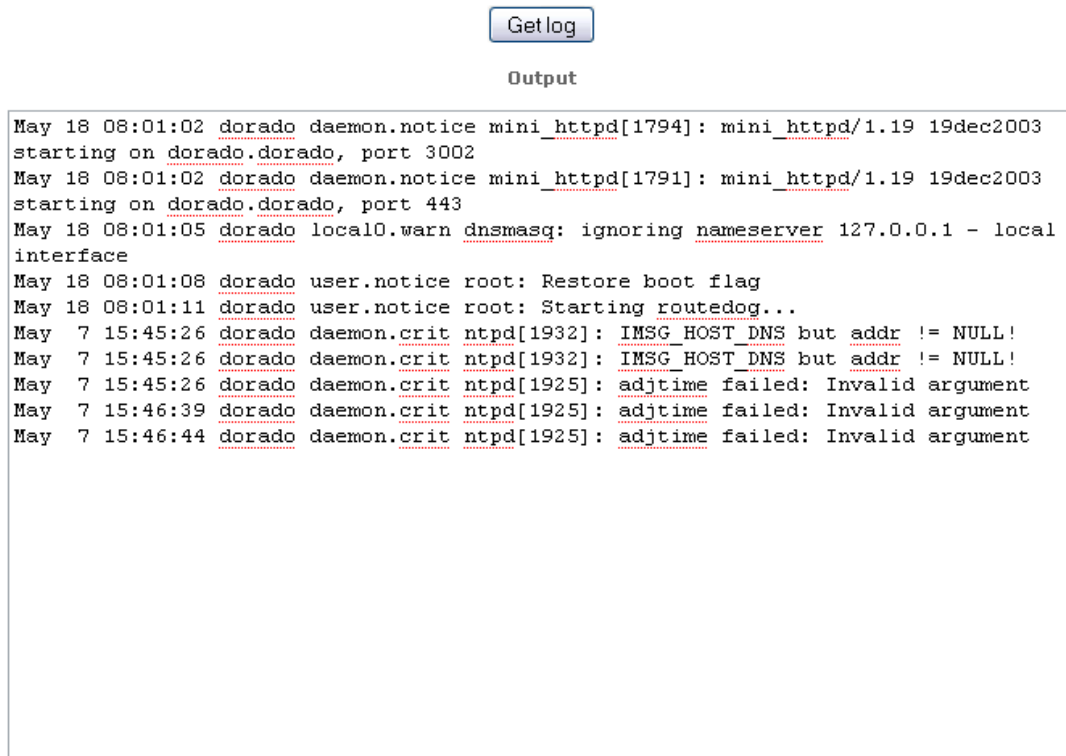
User Name:	user
MAC Address:	00:13:02:B0:4A:8F
Auth Mode:	prep
Auth Message:	
Start Page	www.google.com
Language	English
Customizable Info:	
Login During	0:03:22
Idle:	0:00:03
Session Timeout:	1083 min
Idle Timeout	5 min
Tx bytes:	4449B
Rx bytes:	0B

User details page contains the following parameters:

- **IP** – IP currently being used by the authenticated user.
- **User Name** – Name of the authenticated user.
- **MAC Address** – MAC address of the authenticated user.
- **Auth Mode** – Type of authentication used.
- **Auth Message** – Authentication message.
- **Start Page** – User start page after successfully authenticated.
- **Language** – Language of the authenticated user.
- **Customizable Info** – Customize additional info for this authenticated user.
- **Login During** – Time of login.
- **Idle** – Period of time the user is idle on this connection.
- **Session Timeout** – User will be logged out when usage time exceed the session timeout value will

## 9.5 Status > System Log

Figure 9.5.1 illustrates the system log page.



The screenshot shows a web interface for the system log. At the top, there is a button labeled "Get log". Below the button is a text area labeled "Output" which contains the following log entries:

```
May 18 08:01:02 dorado daemon.notice mini_httpd[1794]: mini_httpd/1.19 19dec2003
starting on dorado.dorado, port 3002
May 18 08:01:02 dorado daemon.notice mini_httpd[1791]: mini_httpd/1.19 19dec2003
starting on dorado.dorado, port 443
May 18 08:01:05 dorado local0.warn dnsmasq: ignoring nameserver 127.0.0.1 - local
interface
May 18 08:01:08 dorado user.notice root: Restore boot flag
May 18 08:01:11 dorado user.notice root: Starting routedog...
May 7 15:45:26 dorado daemon.crit ntpd[1932]: MSG_HOST_DNS but addr != NULL!
May 7 15:45:26 dorado daemon.crit ntpd[1932]: MSG_HOST_DNS but addr != NULL!
May 7 15:45:26 dorado daemon.crit ntpd[1925]: adjtime failed: Invalid argument
May 7 15:46:39 dorado daemon.crit ntpd[1925]: adjtime failed: Invalid argument
May 7 15:46:44 dorado daemon.crit ntpd[1925]: adjtime failed: Invalid argument
```

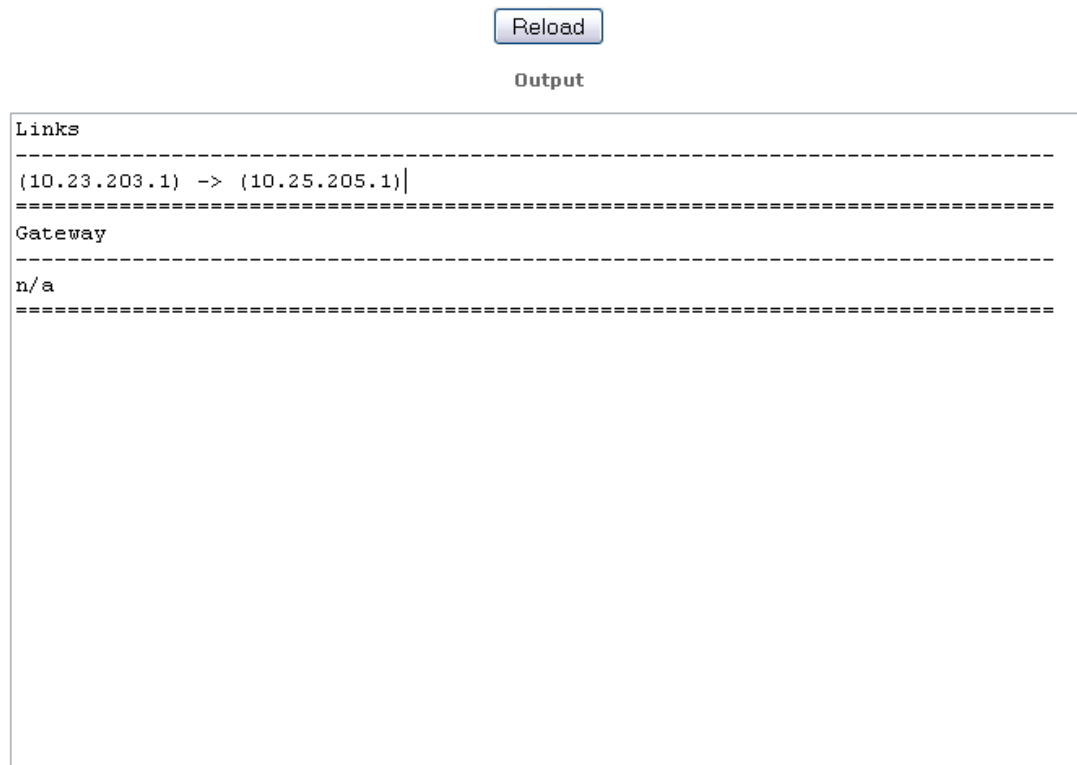
Figure 9.5.1: System Log page

System log page contains the following parameters:

- **“Get log”** button to display output of system log command.
- **“Output”** text area to display the result of the output.

## 9.6 Status > Topology

Figure 9.6.1 illustrates the simple topology view of the mesh network.



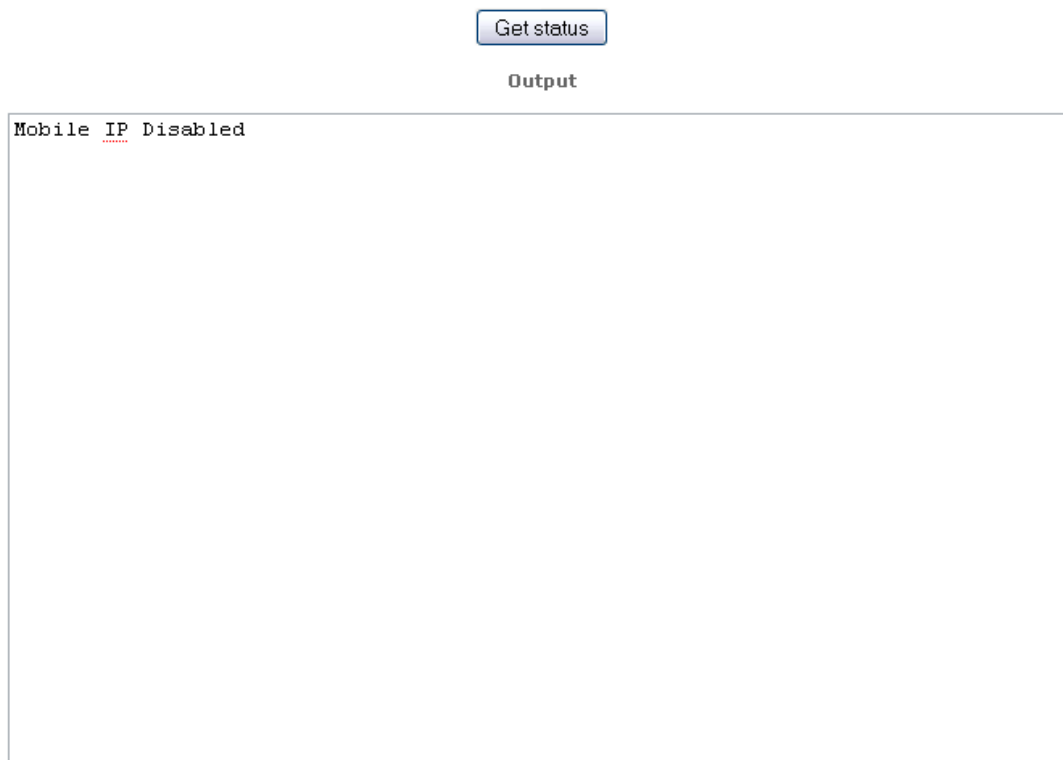
**Figure 9.6.1: Simple Topology page**

Simple topology page contains the following parameters:

- **“Reload”** button to reload output content of topology command.
- **“Output”** text area to display the result of the **“Reload”** button.

## 9.7 Status > Mobile IP

Figure 9.7.1 illustrates the status of the mobile IP client in this device.



**Figure 9.7.1 Mobile IP Status**

Mobile IP page contains the following parameters:

- **“Get Status”** button to display mobile IP status.
- **“Output”** text area to display the result of **“Get Status”** button.

## 9.8 Status > Neighbor

Neighbor status page will show the mesh node status. It show neighbor with details such as rate, rssi, timeout. Figure 9.8.1 illustrates the neighbor status page.

List of Neighbors

MAC Address	Rate (Mbps)	RSSI (dBm)	Timeout (Seconds)	Mac Table
00:0b:6b:2b:ee:35	36M	63	120	<a href="#">View</a>
00:0b:6b:2b:ee:63	36M	63	123	<a href="#">View</a>

[View All Macs](#)

**Figure 9.8.1: Neighbor Status page**

Neighbor Status page contains the following parameters:

- **List of Neighbors** – display a list of connected neighbor
- **<View hyperlink>** - display the MAC table of the selected entry.
- **View All Macs** – display all the MAC currently visible to the device.

Figure 9.8.2 illustrates the MAC registered under the selected node.

List of Macs (00:0b:6b:2b:ee:35)

Neighbor	MAC Address	Timeout (Seconds)
00:0b:6b:2b:ee:35	00:0b:6b:2b:ee:35	120
00:0b:6b:2b:ee:63	00:0b:6b:2b:ee:35	120

**Figure 9.8.2: MAC table of the specific nodes**

## 10 Help

Help page provide links to specific help related to configuration and some description according to each submenu of the configuration..

DORADO CONFIDENTIAL