

# EnGenius Mesh AP M8000



## User Manual & Configuration Guide

Version : 1.0

## Table of Content

|  |           |
|--|-----------|
| <b>Table of Content</b>                    | <b>2</b>  |
| <b>1 Document History</b>                  | <b>4</b>  |
| <b>2 Overview</b>                          | <b>5</b>  |
| <b>3 EnGenius Mesh Web-based Interface</b> | <b>6</b>  |
| <b>4 System</b>                            | <b>9</b>  |
| 4.1 System > System                        | 9         |
| 4.2 System > Syslog                        | 10        |
| 4.3 System > Advance                       | 11        |
| <b>5 Network</b>                           | <b>13</b> |
| 5.1 Network > Network                      | 13        |
| 5.2 Network > VLAN                         | 14        |
| 5.3 Network > Mesh                         | 16        |
| 5.4 Network > Wireless                     | 20        |
| 5.5 Network > Route                        | 23        |
| <b>6 Service</b>                           | <b>25</b> |
| 6.1 Service > MAC Access                   | 25        |
| 6.2 Service > NTP                          | 27        |
| 6.3 Service > RADIUS                       | 28        |
| 6.4 Service > Linux Kernel Watchdog        | 31        |
| 6.5 Service > SSHD                         | 32        |
| 6.6 Service > WME                          | 33        |
| 6.7 Service > DHCP Relay                   | 35        |
| <b>7 Management</b>                        | <b>37</b> |
| 7.1 Management > HTTPD                     | 37        |
| 7.2 Management > Configuration             | 39        |
| 7.3 Management > SNMP                      | 42        |
| 7.4 Management > Firmware                  | 45        |
| 7.5 Management > Trap                      | 46        |
| 7.6 Management > NMS Addresses             | 49        |
| 7.7 Management > Reboot                    | 51        |
| <b>8 Tools</b>                             | <b>52</b> |
| 8.1 Tools > Ping                           | 52        |
| 8.2 Tools > Ifconfig                       | 53        |
| 8.3 Tools > Route                          | 54        |
| 8.4 Tools > TFTP                           | 55        |
| <b>9 Status</b>                            | <b>56</b> |
| 9.1 Status > Status                        | 56        |
| 9.2 Status > Interfaces                    | 57        |

|           |                     |           |
|-----------|---------------------|-----------|
| 9.3       | Status > Services   | 59        |
| 9.4       | Status > System Log | 60        |
| 9.5       | Status > Neighbor   | 61        |
| <b>10</b> | <b>Help</b>         | <b>61</b> |

EnGenius CONFIDENTIAL

## 1 Document History

| Revision | Date       | Remarks       | Authors |
|----------|------------|---------------|---------|
| 1.0      | 2008-04-07 | Draft Release |         |

EnGenius CONFIDENTIAL

## 2 Overview

The purpose of this document is to describe the detail features of EnGenius Mesh Access Point (M8000), and also the procedure and methodology of configuring and the use of EnGenius MAP.

EnGenius CONFIDENTIAL

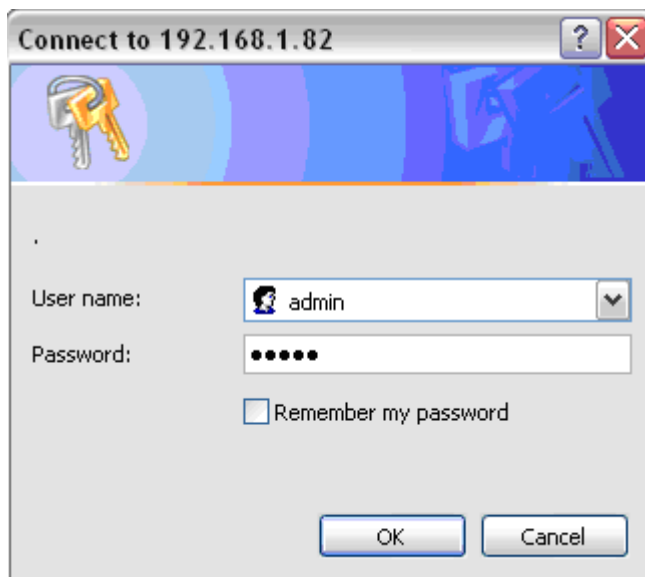
### 3 EnGenius Mesh Web-based Interface

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

`https://192.168.0.1/`.

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.

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

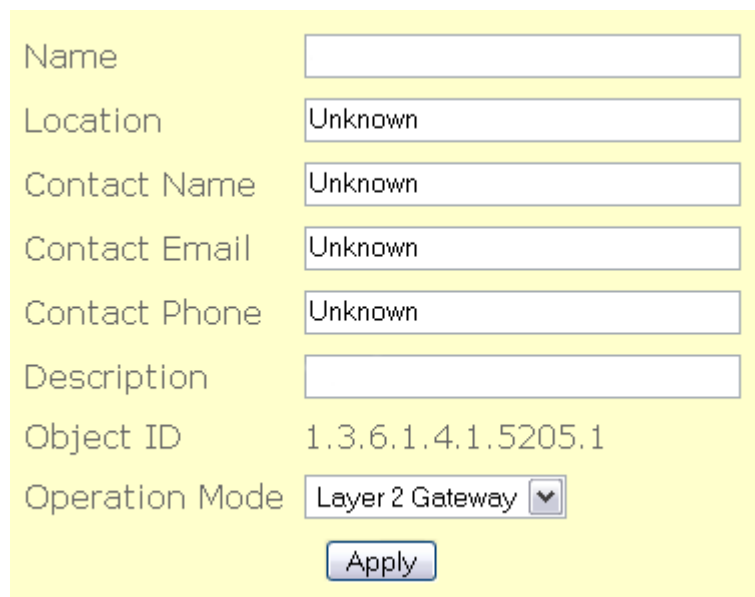
|                              |                                       |
|------------------------------|---------------------------------------|
| <i>Welcome</i>               |                                       |
| <i>System</i>                |                                       |
| <i>System</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>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>Services</i>              |                                       |
| <i>MAC Access</i>            | <i>Filter MAC address</i>             |
| <i>NTP</i>                   | <i>Network Time Protocol</i>          |
| <i>RADIUS</i>                | <i>RADIUS client 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>DHCP Relay</i>            | <i>DHCP relay 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>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>System Log</i>    | <i>System logging</i>                                |
| <i>Neighbor</i>      | <i>Mesh node status</i>                              |
| <i>Help</i>          |  |

## 4 System

### 4.1 System > System

MAP 1000 is a layer 2 mesh network that supports gateway and relay operation mode. Figure 4.1.1 illustrates the system information configuration page.



|                                      |  |
|--------------------------------------|--|
| Name                                 | <input type="text"/>                         |
| 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"/>                         |
| Object ID                            | 1.3.6.1.4.1.5205.1                           |
| Operation Mode                       | <input type="text" value="Layer 2 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 “Layer 2 Gateway” & “Layer 2 Relay”
- **“Apply”** button to save any changes made. New settings are active after the device reboot.

## 4.2 System > Syslog

Certain system message is useful to understand the problem behind any undesired result. Mesh AP 4000 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"/> |

Apply

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 contrack 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="400"/>   | (100~10000m) |
| Radio 2 distance      | <input type="text" value="400"/>   | (100~10000m) |
| Regulatory Domain     | 0 - NO_ENUMRD  |              |
| Country               | <input style="border: 1px solid #ccc;" type="text" value="United States"/> ▼ |              |
| Outdoor Mode          | <input style="border: 1px solid #ccc;" type="text" value="Enable"/> ▼        |              |
| External Channel Mode | <input style="border: 1px solid #ccc;" type="text" value="Disable"/> ▼       |              |

**Figure 4.3.1: Advance configuration page**

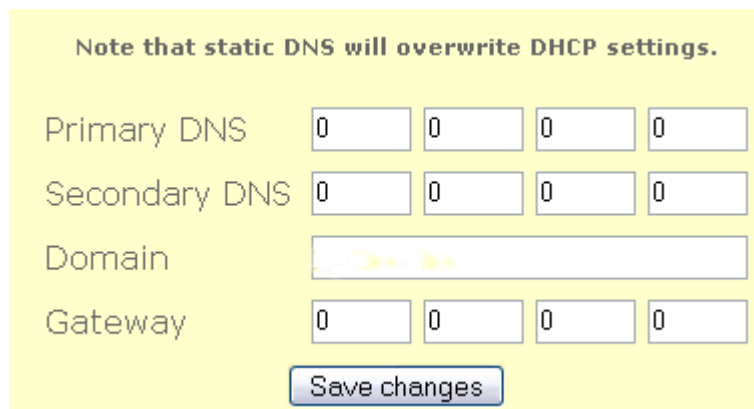
Advance configuration have the following parameters:

- **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 2 distance** – Desired operating distance for radio 2 ( usually refer to client access radio )
- **Regulatory Domain** – Display the regulatory domain of the wireless interface
- **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
- **“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.

## 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

Secondary DNS

Domain

Gateway

**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 > 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 5.2.1 illustrates the VLAN configuration page.

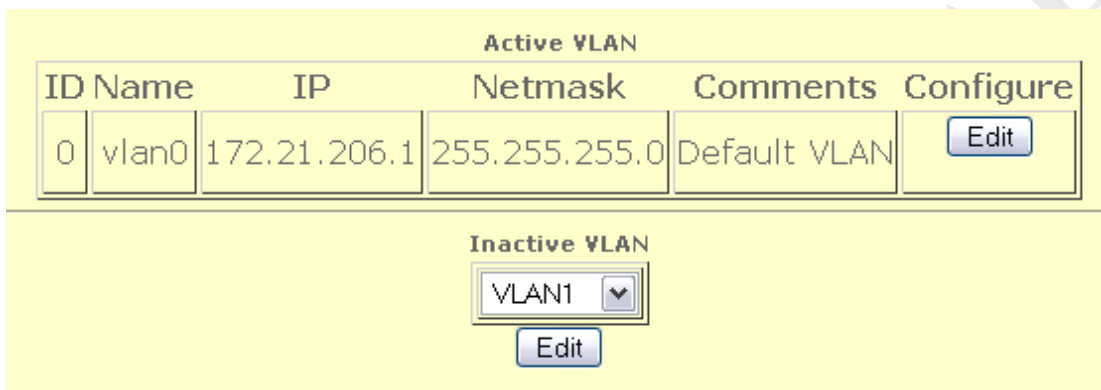


Figure 5.2.1: VLAN configuration page

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 5.2.2.

ID  ( 0 ~ 4095 )  
 Type    
 IP      
 Netmask      
 Routed    
 Comments   
 Active

**Figure 5.2.2: 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

### 5.3 Network > Mesh

This device will form a wireless mesh network with other device provided the correct configuration. Figure 5.3.1 illustrates the wireless settings of the mesh.

|                                      |                      |
|--------------------------------------|----------------------|
| MAC address                          | 00:0b:6b:4d:9c:5e    |
| Mode                                 | ADHOC                |
| Band                                 | 802.11a              |
| ESSID                                |                      |
| 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 )     | 18                   |
| Maximum Tx Power ( dBm )             | 18                   |
| Security                             | Open                 |
| <input type="button" value="Apply"/> |                      |

Figure 5.3.1: 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.

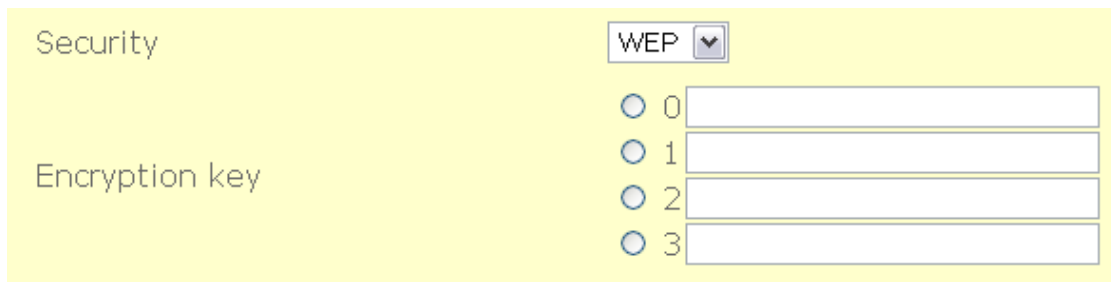
**ADHOC** mode will bring the wireless device to adhoc mode where no AP is required. The connection is established for the duration of one session by discovering others device within range.

**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 5.3.2.



The screenshot shows a configuration page with a yellow background. On the left, the text "Security" is positioned above "Encryption key". On the right, there is a dropdown menu currently set to "WEP". Below the dropdown are four radio buttons labeled "0", "1", "2", and "3", each followed by an empty text input field.

**Figure 5.3.2: 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.

## 5.4 Network > Wireless

Figure 5.4.1 illustrates the AP configuration page.

|                                  |                   |
|----------------------------------|-------------------|
| MAC address                      | 00:0b:6b:4d:9d:51 |
| Mode                             | AP                |
| Band                             | 802.11g           |
| Frequency                        | auto              |
| Tx antenna                       | Card Default      |
| Rx antenna                       | Card Default      |
| Current Maximum Tx Power ( dBm ) | 18                |
| Maximum Tx Power ( dBm )         | 18                |

Apply

| Active Virtual AP |          |          |         |           |
|-------------------|----------|----------|---------|-----------|
| ESSID             | Security | Comments | Active  | Configure |
|                   | open     | VAP1     | Enabled | Edit      |

Figure 5.4.1: 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 MAP 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 5.4.2.

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

Apply

Figure 5.4.2: 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 5.4.4.

Figure 5.4.3 APO with WEP security selected

Figure 5.4.4: APO 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.

## 5.5 Network > Route

Routing refers to selecting paths in a network along which to send data. Figure 5.5.1 illustrates the route configuration page.



Figure 5.5.1: 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 5.5.2 illustrates the add or edit page for route entry.

Subnet

Netmask

Direct  ▼

Device  ▼

Comments

Active  ▼

Figure 5.5.2: 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.

## 6 Service

### 6.1 Service > MAC Access

MAC Access provides another level of security by filtering the packets coming into the device. Figure 6.1.1 illustrates the MAC Access configuration page.

| MAC               | Type  | Comments | Active  | Configuration   |
|-------------------|-------|----------|---------|---|
| 00:00:00:22:22:00 | allow | aa       | Enabled | <input type="button" value="Modify"/> <input type="button" value="Remove"/> |

Figure 6.1.1: 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 users that are currently active

Figure 6.1.2 illustrates the configuration page for edit or add new entry to the MAC access control.

**Figure 6.1.2: 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 6.1.3 illustrates the browse active user.

| MAC address       | IP address     | Action  |
|-------------------|----------------|---------|
| 00:16:CE:51:F6:54 | 172.21.206.254 | Allow ▾ |

**Figure 6.1.3 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

## 6.2 Service > NTP

Network Time Protocol (NTP) is a protocol for synchronizing the system clocks over data networks. Figure 6.2.1 illustrates the NTP configuration page.

| Active              | Enable           |         |               |
|---------------------|------------------|---------|---------------|
| Time Zone           | TW-Asia/Taipei   |         |               |
| Daylight Saving     | Disable          |         |               |
| Apply               |                  |         |               |
| NTP Servers         |                  |         |               |
| Server              | Comment          | Active  | Configuration |
| 0.asia.pool.ntp.org | Default Server 1 | Enabled | Modify Remove |
| 1.asia.pool.ntp.org | Default Server 2 | Enabled | Modify Remove |
| New Entry           |                  |         |               |

Figure 6.2.1: 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 6.2.2 illustrates the configuration page for add or edit NTP server settings.



The screenshot shows a configuration form for NTP. It has a light yellow background. There are three input fields: 'Server' (a text box), 'Comments' (a text box), and 'Active' (a dropdown menu currently showing 'Enable'). Below these fields is a blue 'Apply' button.

**Figure 6.2.2: 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.

### 6.3 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 6.3.1 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**

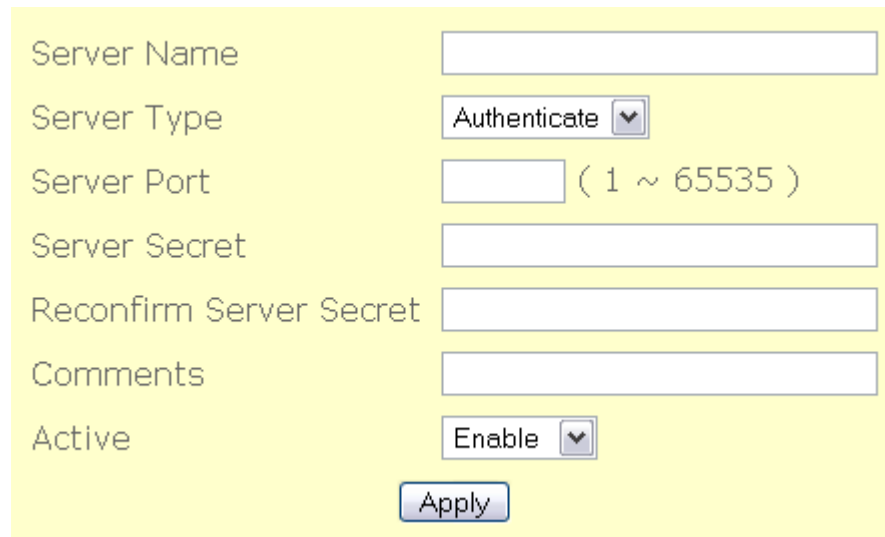
| Name           | Type | Port | Comments | Active  | Configure   |
|----------------|------|------|----------|---------|---|
| 192.168.49.251 | 1    | 1812 | aaa      | Enabled | <input type="button" value="Modify"/> <input type="button" value="Remove"/> |

**Figure 6.3.1: 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 6.3.2 illustrates the add or edit page for RADIUS entry.



|                         |                                    |
|-------------------------|------------------------------------|
| Server Name             | <input type="text"/>               |
| Server Type             | Authenticate ▾                     |
| Server Port             | <input type="text"/> ( 1 ~ 65535 ) |
| Server Secret           | <input type="text"/>               |
| Reconfirm Server Secret | <input type="text"/>               |
| Comments                | <input type="text"/>               |
| Active                  | Enable ▾                           |

Apply

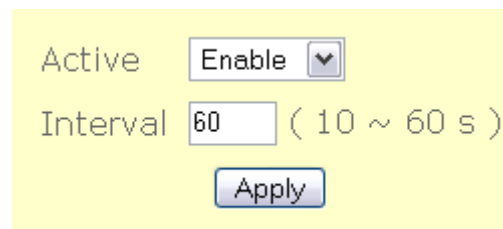
**Figure 6.3.2: RADIUS server – add or edit page**

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.

## 6.4 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 6.4.1 illustrates the linux kernel watchdog configuration page.



Active

Interval  ( 10 ~ 60 s )

Figure 6.4.1: 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.

## 6.5 Service > SSHD

SSHD provides remote management using command line interface (CLI). Figure 6.5.1 illustrates the SSHD configuration page.

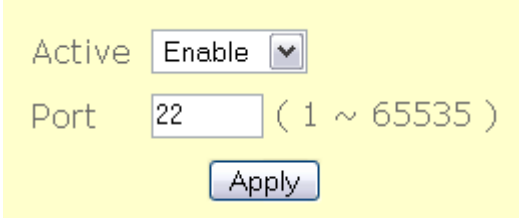
The image shows a configuration interface for SSHD. It features a yellow background. At the top, the word 'Active' is followed by a dropdown menu currently showing 'Enable'. Below this, the word 'Port' is followed by a text input field containing the number '22'. To the right of the input field is the text '( 1 ~ 65535 )'. At the bottom center of the configuration area is a button labeled 'Apply'.

Figure 6.5.1: 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.

## 6.6 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 6.6.1 illustrates the WME configuration page.

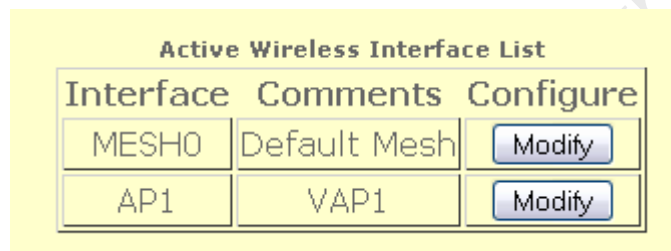


Figure 6.6.1: WME configuration page

WME configuration page contains the following parameters:

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

Figure 6.6.2 illustrates the edit page for WME parameters.

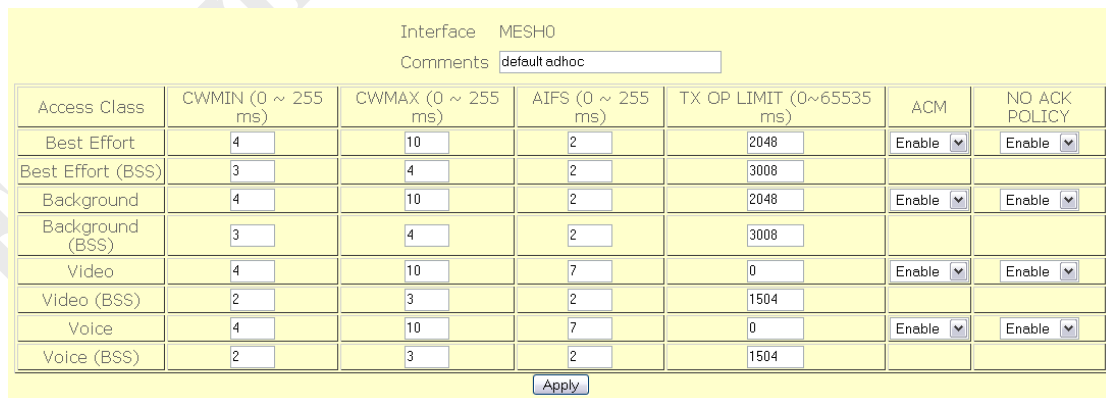


Figure 6.6.2: WME - edit page

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.

## 6.7 Service > DHCP Relay

For a dynamic network, MAP 1000 is able to forward the DHCP request to a backend DHCP server when operating in layer 2 mode. Figure 6.7.1 illustrates the configuration page for DHCP Relay.

Active

Port  ( 1 ~ 65535 )

Hop count  ( 1 ~ 255 )

Max packet size  ( 600 ~ 1400 )

| DHCRELAY List    |               |        |   |
|------------------|---------------|--------|---|
| Server/Interface | Extra Comment | Active | Configure   |
| Interface        | ixp1          | aa     | Enabled <input type="button" value="Modify"/> <input type="button" value="Remove"/> |

**Figure 6.7.1 DHCP Relay Settings**

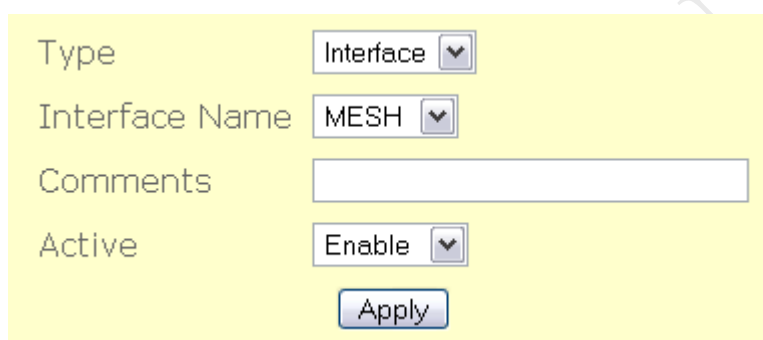
DHCP Relay contains the following parameters:

- **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 6.7.2 illustrates the add or edit configuration page.



**Figure 6.7.2 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"/> |

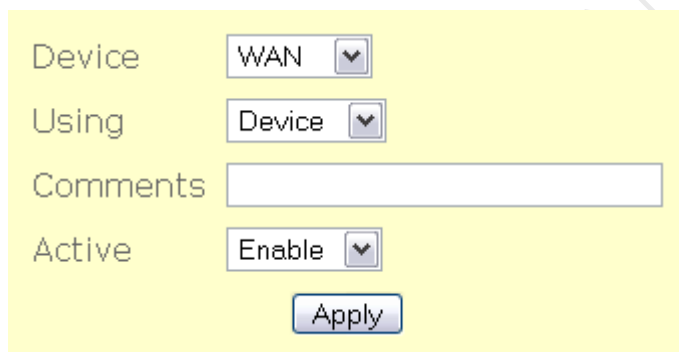
**Figure 7.1.1: HTTPD server configuration page**

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

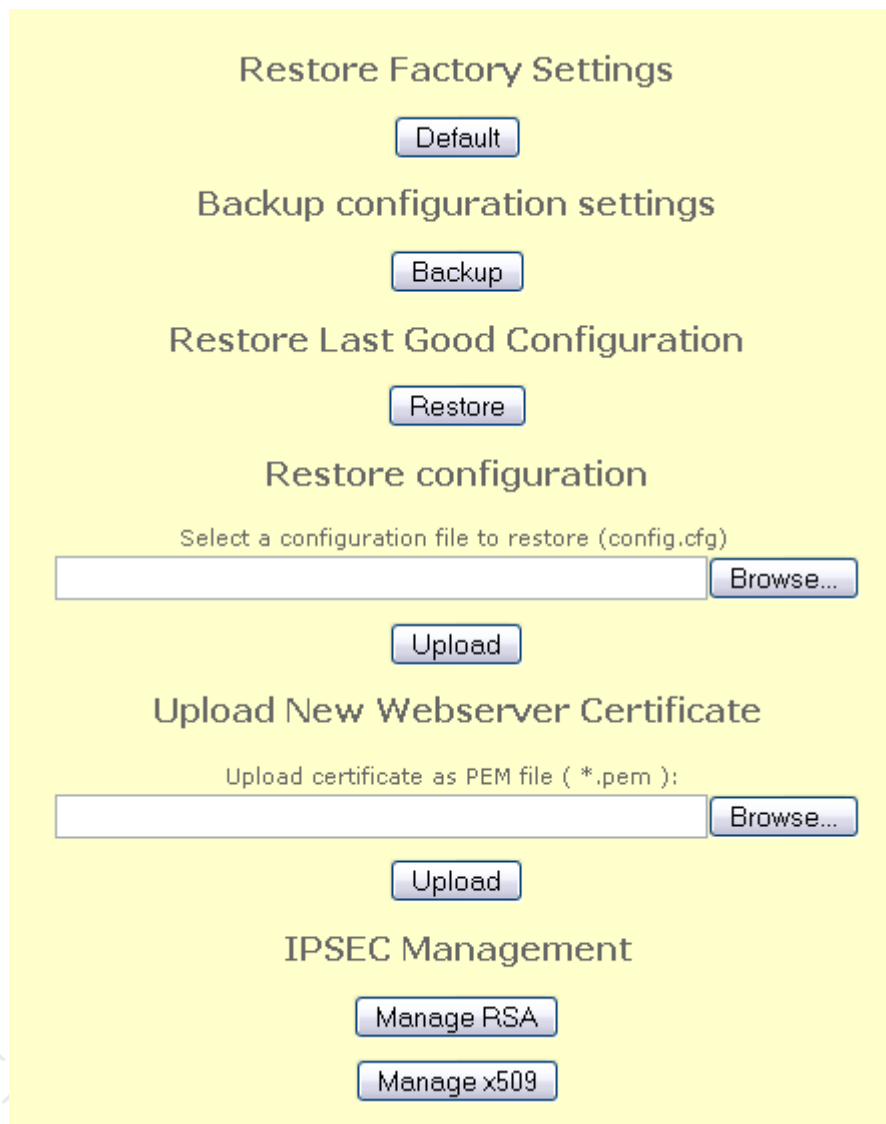
**Figure 7.1.2: HTTPD Access Control – add or edit page**

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 a configuration page with a yellow background. It features several sections with buttons and input fields:

- Restore Factory Settings**: A button labeled "Default".
- Backup configuration settings**: A button labeled "Backup".
- Restore Last Good Configuration**: A button labeled "Restore".
- Restore configuration**: A section with the text "Select a configuration file to restore (config.cfg)", an empty text input field, a "Browse..." button, and an "Upload" button.
- Upload New Webserver Certificate**: A section with the text "Upload certificate as PEM file ( \*.pem ):", an empty text input field, a "Browse..." button, and an "Upload" button.
- IPSEC Management**: Two buttons labeled "Manage RSA" and "Manage x509".

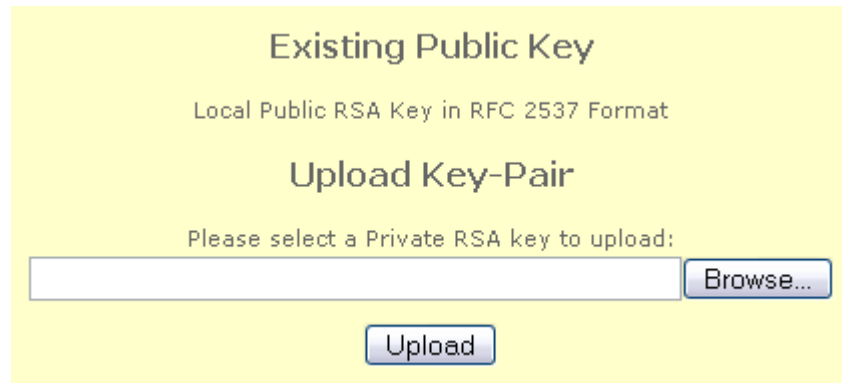
**Figure 7.2.1: Configuration page**

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:

**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.



The screenshot displays the 'Local Certificate' and 'Remote Certificate' configuration sections. The 'Local Certificate' section shows 'Existing local certificate: None' and 'Existing root certificate authority: None'. It includes a text input field for 'Upload certificate as PKCS 12 file (Extension \*.p12):' with a 'Browse...' button and an 'Upload' button. The 'Remote Certificate' section shows 'Existing Certificate: None' and includes a text input field for 'Upload remote certificate as PEM file (Extension \*.pem):' with a 'Browse...' button and an 'Upload' button.

**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.

The screenshot shows the SNMP configuration interface. It includes a form with the following fields:

- Active: Enable (dropdown)
- Version: all (dropdown)
- Port: 161 (input field) ( 1 ~ 65535 )
- v2 Read Community: [Redacted]
- Reconfirm v2 Read Community: [Redacted]
- v2 Read-write Community: [Redacted]
- Reconfirm v2 Read-write Community: [Redacted]
- v3 Read Username: snmpv3router
- v3 Read-write Username: snmpv3rwuser
- v3 Password: [Redacted]
- Reconfirm v3 Password: [Redacted]
- v3 Passphrase: [Redacted]
- Reconfirm v3 Passphrase: [Redacted]
- Access Control: Enable (dropdown)

Below the form is an "Apply" button. Underneath is the "Access Control List" table:

| Device | Subnet | Netmask | Comments | Active  | Configure     |
|--------|--------|---------|----------|---------|---------------|
| MESH   | -      | -       | Mesh     | Enabled | Modify Remove |
| WAN    | -      | -       | WAN      | Enabled | Modify Remove |
| VLAN0  | -      | -       | VLAN     | Enabled | Modify Remove |

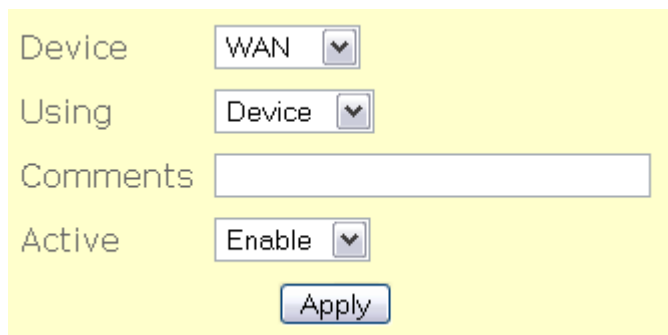
At the bottom of the table is a "New Entry" button.

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 has a light yellow background. The form contains 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 located below the "Active" dropdown.

**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.

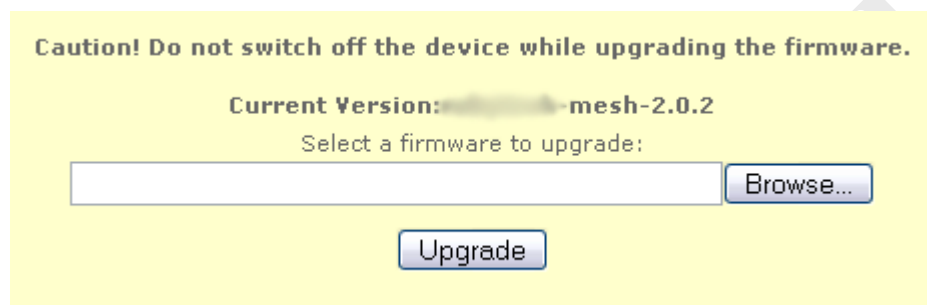


Figure 7.4.1: Firmware Upgrade page

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        | Disable ▼ |
| Configuration | Enable ▼  |
| Security      | Enable ▼  |
| Wireless      | Enable ▼  |
| Operational   | Enable ▼  |
| Flash         | Enable ▼  |
| Tftp          | Enable ▼  |
| Image         | Enable ▼  |
| Auth failure  | Enable ▼  |

Apply

| Version | Trap to     | Comments | Active  | Configure     |
|---------|-------------|----------|---------|---------------|
| 2c      | 192.168.1.1 | aaaaa    | Enabled | Modify Remove |

New Entry


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**: A field divided into four segments for entering an IP address.
- Community**: A single-line text input field.
- Reconfirm Community**: A single-line text input field.
- Version**: A dropdown menu currently set to "2c".
- Comments**: A single-line text input field.
- Active**: A dropdown menu currently set to "Enable".
- Apply**: A button located below the "Active" dropdown.

**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.

EnGenius CONFIDENTIAL

## 7.6 Management > NMS Addresses

NMS address is used for the system to report back to Network Management System located outside of the network. Figure 7.6.1 illustrates the NMS server address configuration page.

| Address      | Port | Interval | Comments | Active  | Configuration   |
|--------------|------|----------|----------|---------|---|
| 192.168.1.60 | 8182 | 60       |          | Enabled | <input type="button" value="Modify"/> <input type="button" value="Remove"/> |

Figure 7.6.1 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 7.6.2 illustrates the NMS address configuration page for add or edit.

Address

Port

Interval  (60-300000s)

Comments

Active  ▼

Figure 7.6.2: 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.

EnGenius CONFIDENTIAL

## 7.7 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=10.5 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.0 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 1.0/5.7/10.5 ms
```

**Figure 8.1.1: Ping page**

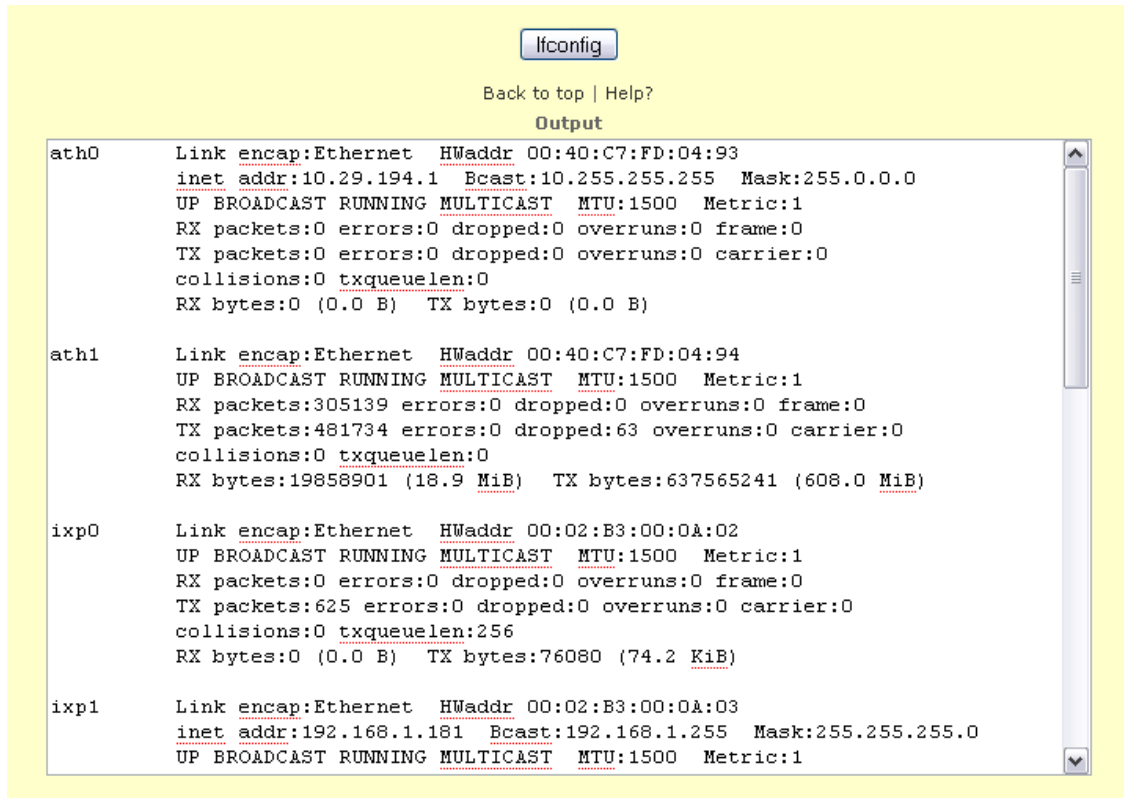
Ping page contains the following parameters:

- **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 for the ifconfig command. At the top, there is a button labeled "ifconfig" and a link "Back to top | Help?". Below this is a section titled "Output" containing a text area with the following text:

```
ath0      Link encap:Ethernet  HWaddr 00:40:C7:FD:04:93
          inet addr:10.29.194.1  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 00:40:C7:FD:04:94
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:305139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:481734 errors:0 dropped:63 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19858901 (18.9 MiB)  TX bytes:637565241 (608.0 MiB)

ixp0      Link encap:Ethernet  HWaddr 00:02:B3:00:0A:02
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:625 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256
          RX bytes:0 (0.0 B)  TX bytes:76080 (74.2 KiB)

ixp1      Link encap:Ethernet  HWaddr 00:02:B3:00:0A:03
          inet addr:192.168.1.181  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

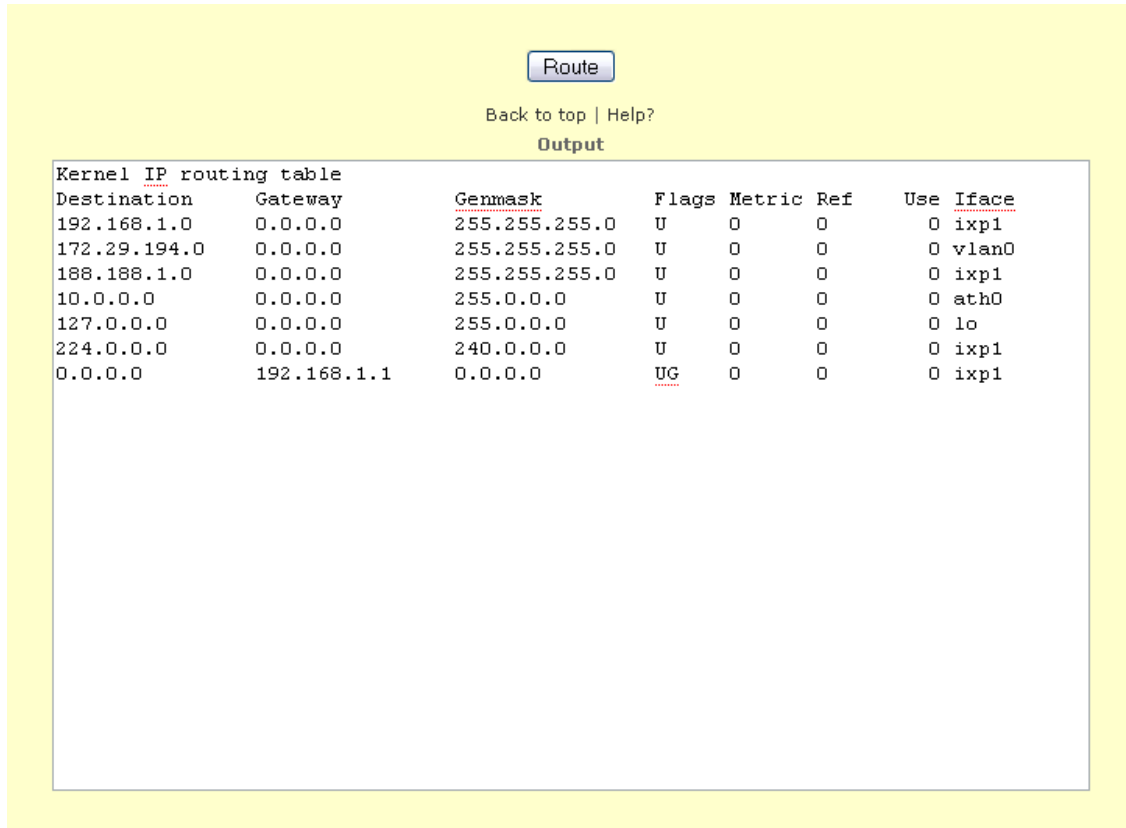
Figure 8.2: Ifconfig page

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.



**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**

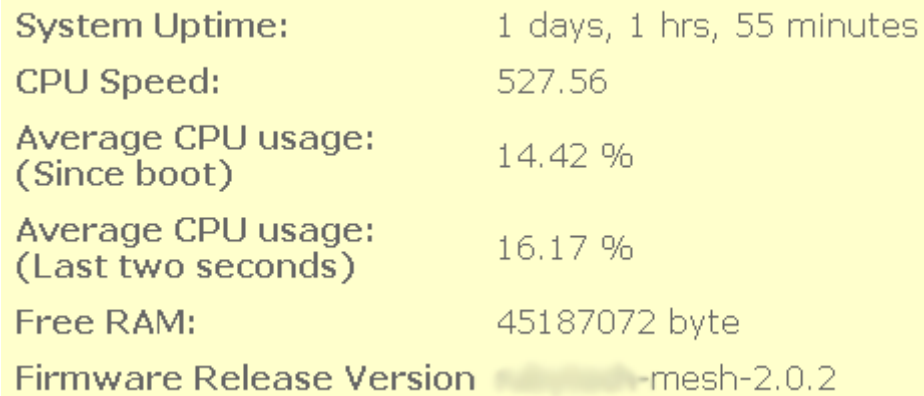
TFTP contains the following parameters:

- **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.



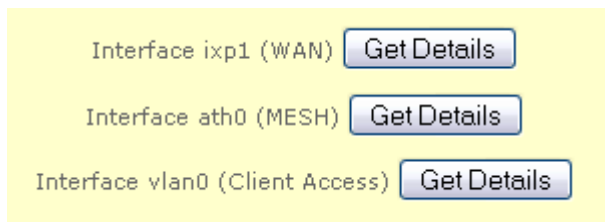
|  |                           |
|--|---------------------------|
| System Uptime:                           | 1 days, 1 hrs, 55 minutes |
| CPU Speed:                               | 527.56                    |
| Average CPU usage:<br>(Since boot)       | 14.42 %                   |
| Average CPU usage:<br>(Last two seconds) | 16.17 %                   |
| Free RAM:                                | 45187072 byte             |
| Firmware Release Version                 | mesh-2.0.2                |

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.



**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:  | 00:02:B3:00:0A:0F  |
| IP Type:           | dhcp               |
| IP Address:        | 192.168.1.122      |
| Broadcast Address: | 192.168.1.255      |
| Netmask:           | 255.255.255.0      |
| MTU:               | 1500               |
| Rx bytes:          | 80019372 (76.3 MB) |
| Tx bytes:          | 5106882 (4.8 MB)   |
| Rx packets:        | 1111210            |
| Tx packets:        | 35999              |
| Rx errors:         | 0                  |
| Tx errors:         | 0                  |
| Rx dropped:        | 0                  |
| Tx dropped:        | 0                  |

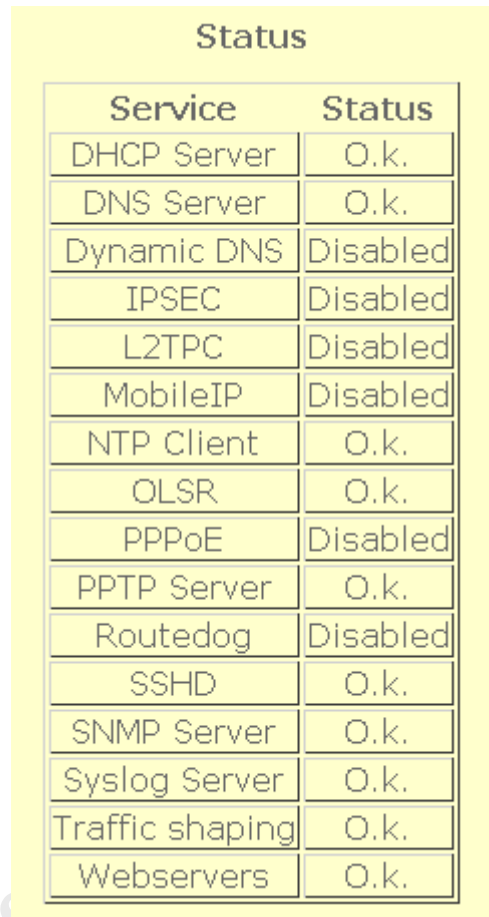
**Figure 9.2.2: Details of interface ixp0 ( WAN ).**

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.



| 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.     |

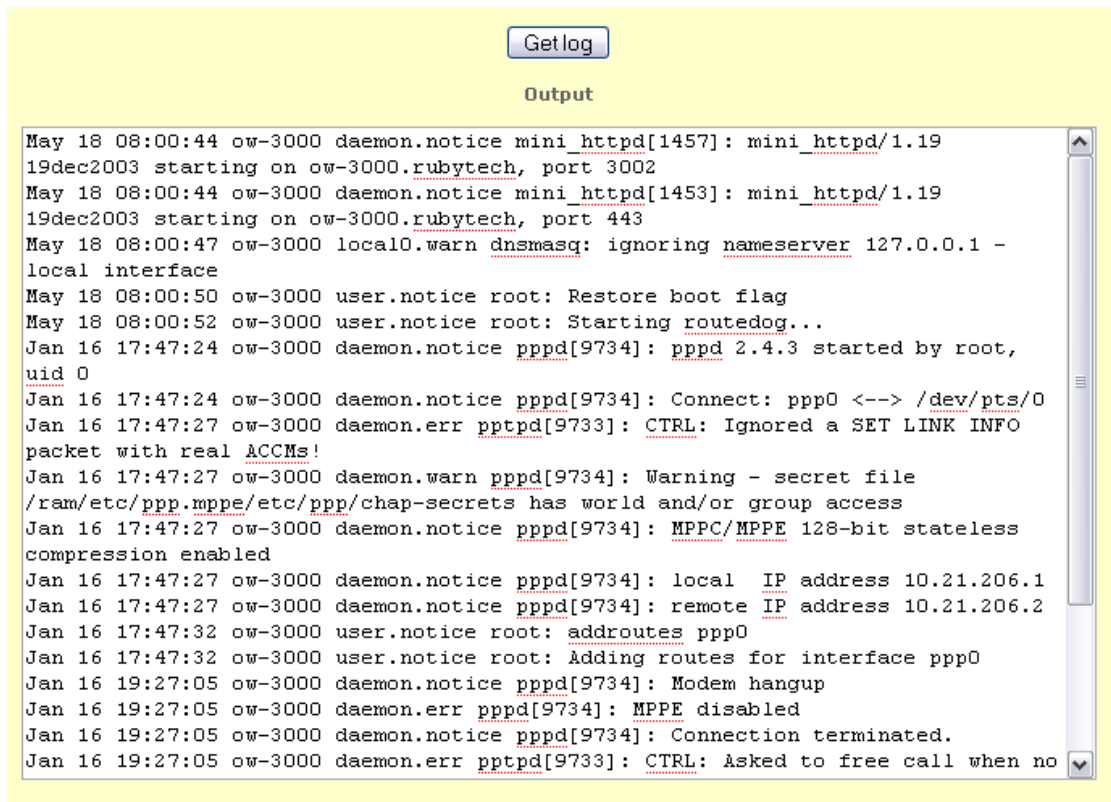
**Figure 9.3.1: Services page**

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

- **DHCP Relay**
- **NTP Client**
- **SSHD**
- **SNMP Server**
- **Syslog Server**
- **Webservers**

## 9.4 Status > System Log

Figure 9.4.1 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 it is a text area labeled "Output" containing the following log entries:

```
May 18 08:00:44 ow-3000 daemon.notice mini_httpd[1457]: mini_httpd/1.19
19dec2003 starting on ow-3000.rubyttech, port 3002
May 18 08:00:44 ow-3000 daemon.notice mini_httpd[1453]: mini_httpd/1.19
19dec2003 starting on ow-3000.rubyttech, port 443
May 18 08:00:47 ow-3000 local0.warn dnsmasq: ignoring nameserver 127.0.0.1 -
local interface
May 18 08:00:50 ow-3000 user.notice root: Restore boot flag
May 18 08:00:52 ow-3000 user.notice root: Starting routedog...
Jan 16 17:47:24 ow-3000 daemon.notice pppd[9734]: pppd 2.4.3 started by root,
uid 0
Jan 16 17:47:24 ow-3000 daemon.notice pppd[9734]: Connect: ppp0 <--> /dev/pts/0
Jan 16 17:47:27 ow-3000 daemon.err pptpd[9733]: CTRL: Ignored a SET LINK INFO
packet with real ACCMs!
Jan 16 17:47:27 ow-3000 daemon.warn pppd[9734]: Warning - secret file
/ram/etc/ppp.mppe/etc/ppp/chap-secrets has world and/or group access
Jan 16 17:47:27 ow-3000 daemon.notice pppd[9734]: MPPC/MPPE 128-bit stateless
compression enabled
Jan 16 17:47:27 ow-3000 daemon.notice pppd[9734]: local IP address 10.21.206.1
Jan 16 17:47:27 ow-3000 daemon.notice pppd[9734]: remote IP address 10.21.206.2
Jan 16 17:47:32 ow-3000 user.notice root: addroutes ppp0
Jan 16 17:47:32 ow-3000 user.notice root: Adding routes for interface ppp0
Jan 16 19:27:05 ow-3000 daemon.notice pppd[9734]: Modem hangup
Jan 16 19:27:05 ow-3000 daemon.err pppd[9734]: MPPE disabled
Jan 16 19:27:05 ow-3000 daemon.notice pppd[9734]: Connection terminated.
Jan 16 19:27:05 ow-3000 daemon.err pptpd[9733]: CTRL: Asked to free call when no
```

Figure 9.4.1: 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.

## 9.5 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:4d:9c:5e             | 36M         | 11         | 0                 | <a href="#">View</a> |
| <a href="#">View All Macs</a> |             |            |                   |                      |

**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:4d:9c:5e) |                   |                   |
|----------------------------------|-------------------|-------------------|
| Neighbor                         | MAC Address       | Timeout (Seconds) |
| 00:0b:6b:4d:9c:5e                | 00:0b:6b:4d:9c:5e | 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..

This Page is intended to leave blank

EnGenius CONFIDENTIAL