802.11a/b/g Outdoor/Indoor Wireless Mesh Network Access Point

MAP-3020 / MAP-3100 / MAP-3120

Web Management

&

Configuration Manual

Copyright

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance. (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure

Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

Potential Restrictive Use

France: Only channels 10,11,12 and 13

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

Web Interface User's Manual for PLANET Wireless Mesh Access Point

Model: MAP-3100 / MAP-3120/MAP-3020

Rev: 4.0 (July, 2009)

Part No. EM-MAP3K_webv4.doc

Table of Content

1 Overview

Thank you for choosing the PLANET MAP-3100/MAP-3120/MAP-3020 Wireless Mesh Access Point. The MAP-3100 / MAP-3120/MAP-3020 allows a wireless mesh network to be rapidly deployed with minimal configuration required by the end user. This user's guide describes the detailed web interface configuration options.

1.1 MAP-3100 Variants

Currently, there are two MAP-3100 variants available:

MAP-3100: supports both Layer 2 and Layer 3 operations.
MAP-3120/MAP-3020: support Layer 2 operation only.

Throughout the manual, the MAP-3100 will be used to collectively refer to both models. Where the functionality of the variance, the actual model name will be used.

1.2 Package Content

The MAP-3100 / MAP-3120 following items should be included:

- Indoor Mesh AP x 1
- Power Adapter x 1
- 2.4/5GHz Dipole Antenna x 2
- Quick Start Guide x 1
- Management Utility and User's manual CD x 1

If any of the above items are damaged or missing, please contact your dealer immediately.
The following information , the terms of Mesh AP will mean MAP-3120/MAP-3020. unless it is specified.

The MAP-3020 following items should be included:

- Outdoor Mesh AP x 1
- Power adapterx1 with Power cord x1
- POE-152-MESH x1
- Mounting kit x1
- 25 Meter cable CAT5 with RJ-45 plug and ODU connector x1
- 1.5 Meter N –type to N type connector cable x2
- Quick Start Guide x 1
- Management Utility and User's manual CD x 1

If any of the above items are damaged or missing, please contact your dealer immediately.

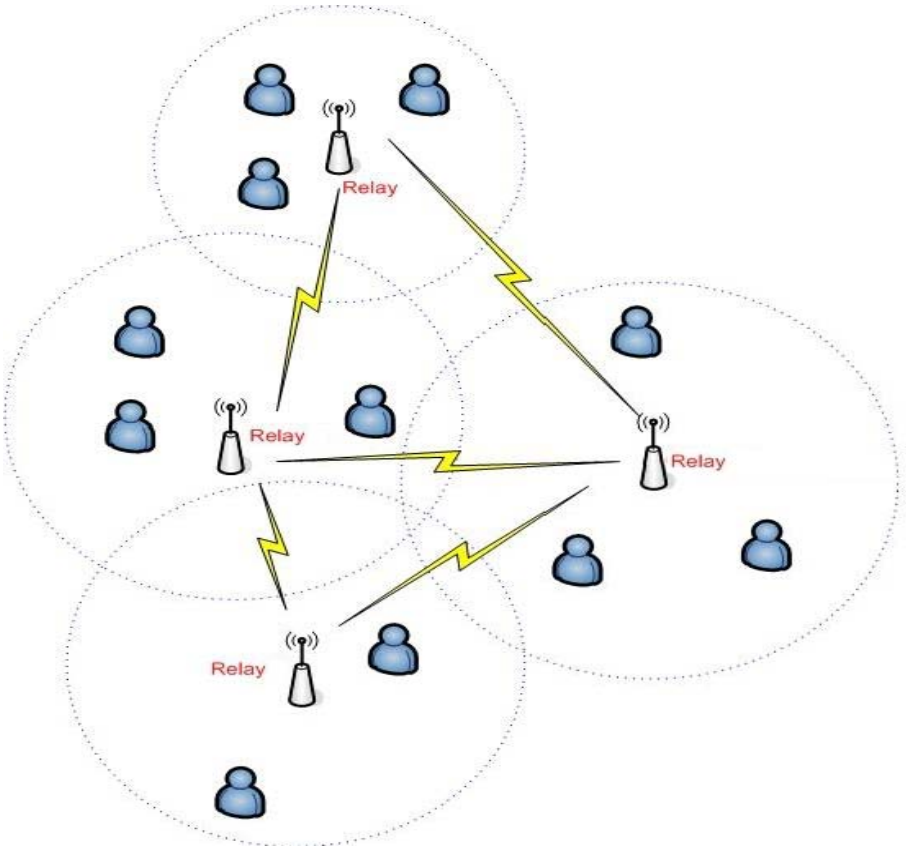
1.3 Features

- Dual wireless interfaces for independent Backhaul link and local clients connection
  - 2 x IEEE 802.11a/b/g adapters
  - 2 x reverse SMA connector
- Supports full dynamic routing (layer 3) among all node APs (MAP-3100)
  - OLSR, optimized link state routing protocol
  - Self-healing and Self-configuration, Plug and Play installation
- Supports layer 2 operation (MAP-3100 / MAP-3120/MAP-3020)
- Adjustable output power
- Central management software
  - AES backhaul communication
- IEEE 802.1q VLAN, multiple VLAN/SSID supports
- IEEE 802.1x, IEEE 802.1i WPA/ WPA2, and VPN pass-through mechanisms
- Supports Wireless Separation, Watchdog mechanism
- QoS for bandwidth control or traffic prioritizing
- Supports SNMP v2c, v3
- IEEE 802.3af Power over Ethernet capable
- Operating temperature: -20~70 degree C (MAP-3020)
- IP-68 protection housing (MAP-3020)

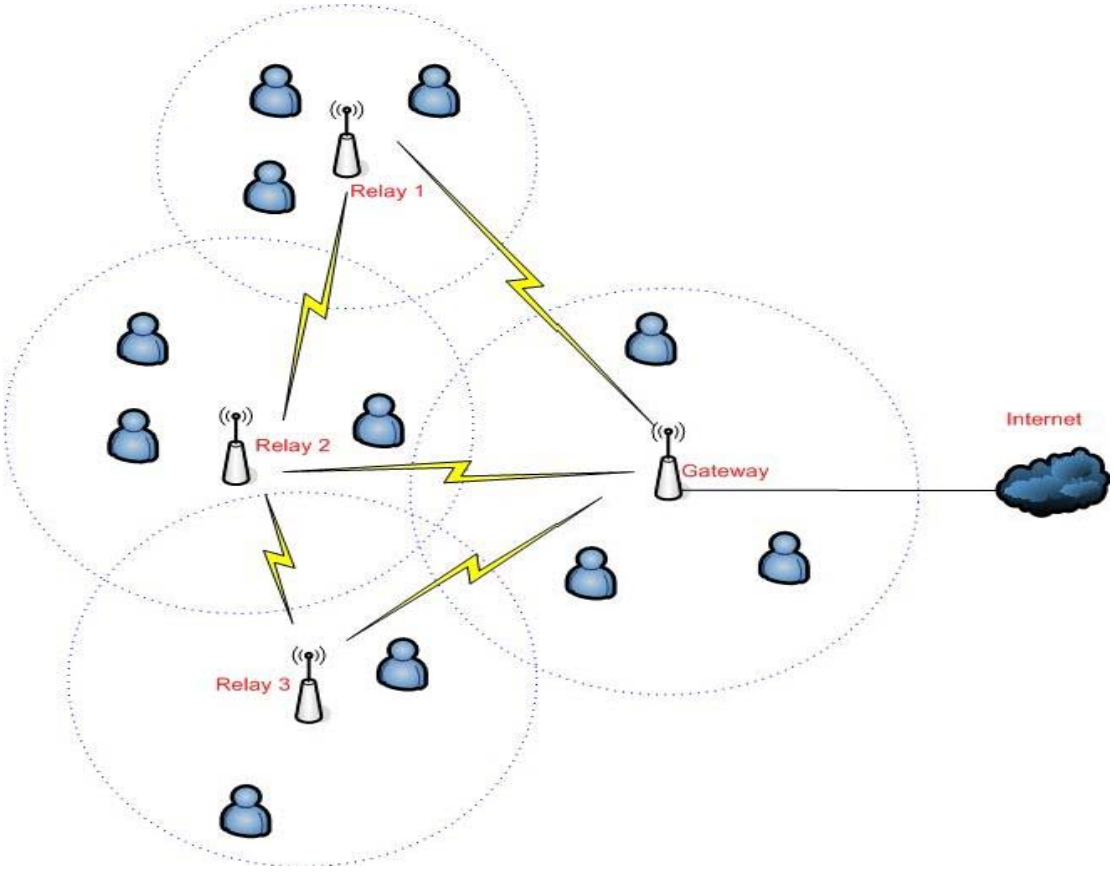
1.4 Network Topology

MAP-3100s can be used to create two network topologies: a closed network or an Internet access network that attaches to a network with connectivity to the Internet.

In a closed network infrastructure, as shown in figure below, all devices are configured to operate in the same mode (Relay mode). This network configuration is suitable for applications where the clients using the mesh only need to communicate with each other and do not need to access the Internet or other remote network resources that are not directly connected to the mesh.



An Internet access network, as shown in figure below, is typically used to provide Internet availability to a number of clients that connect to the mesh network. Alternatively, this configuration can be used to provide access for client devices to remote resources on a private network. There must be one or more gateway devices in such infrastructure that provides access from the mesh network to an external network.



Note

1. The MAP-3100 supports 5 operating modes. Three for Layer 3, two for Layer 2.
2. At Layer 3 mode, multiple Gateways are allowed. At Layer 2 mode, only one Gateway is allowed.
3. At the view of Mesh backhaul network, Layer 2 mode and Layer 3 mode device can not co-existing to each other.

1.5 Wireless Performance

The following information will help you utilizing the wireless performance, and operating coverage of MAP-3100.

1. **Site selection**

   To avoid interferences, please locate MAP-3100 and wireless clients away from transformers, microwave ovens, heavy-duty motors, refrigerators, fluorescent lights, and other industrial equipments. Keep the number of walls, or ceilings between AP and clients as few as possible; otherwise the signal strength may be seriously reduced.

   It is suggested to carry out a site survey prior to installation to determine what devices are operating in the two bands that the MAP-3100 uses. To detect the presence of other 802.11 devices, a tool such as Network Stumbler (http://www.netstumbler.com/downloads/) can be used.

2. **Environmental factors**

   The wireless network is easily affected by many environmental factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operating range of MAP-3100 in a specific location without testing.

3. **Antenna adjustment**

   The bundled antenna of MAP-3100 is adjustable. Firstly install the antenna pointing straight up, then smoothly adjust it if the radio signal strength is poor. But the signal reception is definitely weak in some certain areas, such as location right down the antenna.

   Moreover, the original antenna of MAP-3100 can be replaced with other external antennas to extend the coverage. Please check the specification of the antenna you want to use, and make sure it can be used on MAP-3100.

2 Hardware Installation

2.1 Procedures

Before you proceed with the installation, it is necessary that you have enough information about the MAP-3100.

1. Locate an optimum location for the MAP-3100. Plan for the output frequency of the MAP-3100, 2.4GHz or 5GHz.
2. Assemble the antennas to MAP-3100 follow the frequency band plan. Try to place them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity. When installing antenna(s), follow these general tips:
   - For most elevated antenna installations, we recommend you to ask the professional installers for proper installation and safety.
   - For the safety reasons, you are recommended never to touch a high-gain antenna when it is transmitting or point it at any part of your body.
   - Please, follow carefully the instructions with your antenna.
   - Keep antennas away from metal objects / obstructions (heating and air-conditioning ducts, large ceiling trusses, building superstructures, and major power cabling runs).
   - Use a directional antenna when you establish a link between two buildings. A directional antenna must be properly aligned to the point at the other antenna, line-of-sight.
   - Locate an omni-directional antenna in the middle of the desired coverage area if possible.
   - Place the antenna as high as possible to increase the coverage area.
   - Outdoor antennas should be mounted at a sufficient height to prevent the radio path from above the obstructions such as trees and buildings.
   - Antenna towers should keep a safe distance from overhead power lines. The recommended safe distance is twice the tower height.
3. Using Category 3 or higher UTP or STP cable, connect the LAN port of MAP-3100 to a 10Mbps or 10/100Mbps Ethernet hub or switch, and connect the management station to a hub or switch on the same LAN.
4. Connect the power adapter to the receptor on MAP-3100 and plug the other end to a wall outlet or power strip.

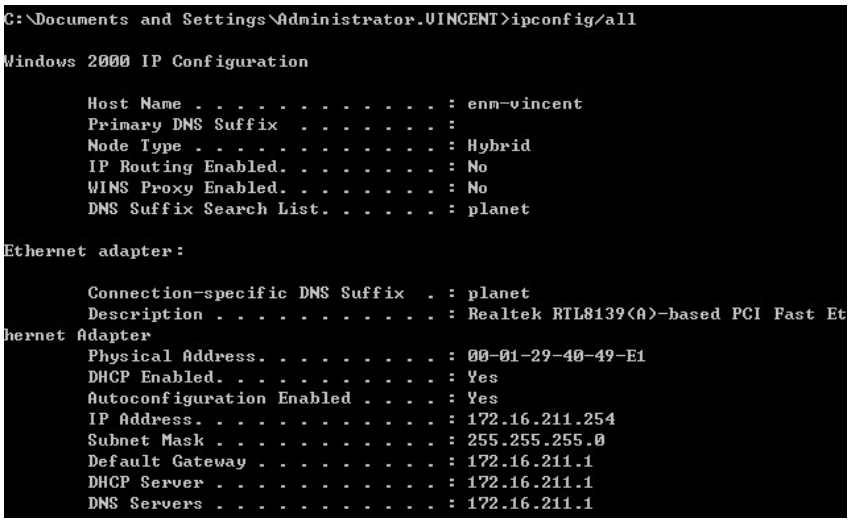
Note

- ONLY use the power adapter supplied with the MAP-3100. Otherwise, the product may be damaged.
- The LAN or WAN / Public port of MAP-3100 / MAP-3120/MAP-3020 supports 802.3af POE. The pins for supplying the electricity are **1, 2, 3, 6**. If the MAP-3100 is powered from POE, you can skip the step 4 above.
- If IEEE802.3af is the planned power source, Only one is allowed, i.e. either LAN#1 or WAN/Public port. Connect two IEEE802.3af power sources to the system at the same time will make the device malfunction permanently.

2.2 Startup the MAP-3100

To get the initial management of the MAP-3100, please follow the steps.

1. Connect the MAP-3100's LAN port to an active network.
2. Connect the PC to the network as well. This PC must be configured as a DHCP client.
3. Open PC Command Prompt and type "ipconfig /all" to check DHCP Server's IP as shown in figure below. In this case, DHCP Server's IP is 172.16.211.1.



4. Launch web browser and enter MAP private IP (DHCP Server's IP), for example, https://172.16.211.1 into URL field. Certificate warning page will display as below.

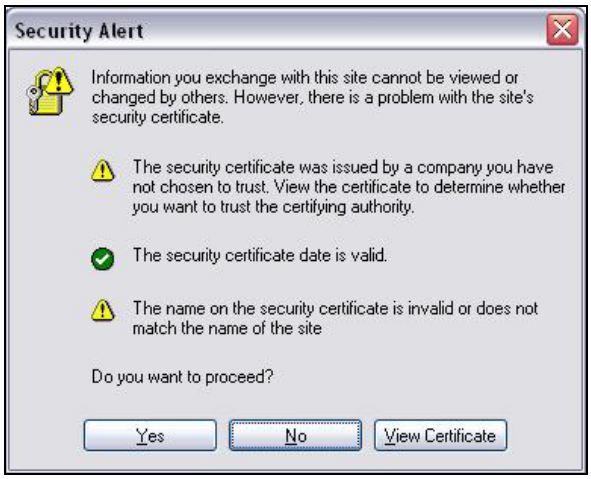
5. Press “Yes” button to accept the MAP web certificate. Authentication page will display.

6. Enter default username “**admin**” and password “**admin**”, then press “OK” button.
7. Now, the MAP-3100 is ready for services.

2.3 Startup the Mesh AP

To get the initial management of the Mesh AP, please follow the steps.

1. Connect the Mesh AP’s LAN port to an active network.
2. Connect the PC to the network as well. This PC must be configured with a fixed IP in 192.168.0.x/255.255.255.0.
3. Launch web browser and enter MAP-3120 default IP , https://192.168.0.1 into URL field. Certificate warning page will display as below.



4. Press “Yes” button to accept the MAP web certificate. Authentication page will display.

5. Enter default username “**admin**” and password “**admin**”, then press “OK” button.
6. Now, the MAP-3120 is ready for services.

3 Web Based Management

3.1 Configuration Menu Overview

MAP-3100 has six main menus: System, Network, Services, Management, Tools and Status.

Each main menu also will have its submenu.

Welcome	
System	
System	
Syslog	
Advance	
Profile	
Network	
DNS settings	
WAN	(MAP-3100 only)
VLAN	
Mesh	
Wireless	
Route	
IPSEC	(MAP-3100 only)
L2TPC	(MAP-3100 only)
OLSR	(MAP-3100 only)
Services	
DHCPD	(MAP-3100 only)
Firewall	(MAP-3100 only)
MAC Access	
Virtual Server	(MAP-3100 only)
NTP	
Traffic Shaping	(MAP-3100 only)
PPTP Server	(MAP-3100 only)
AutoIP	(MAP-3100 only)
Captive Portal	(MAP-3100 only)
RADIUS	
Dynamic DNS	
Zero Config	(MAP-3100 only)
Mobile IP	(MAP-3100 only)

- Route Watchdog (MAP-3100 only)
- System Watchdog

Management

- HTTPD
- Configuration
- SNMPD
- Firmware
- Trap
- User Group (MAP-3100 only)
- Database (MAP-3100 only)
- Webspace (MAP-3100 only)
- Customize Login (MAP-3100 only)
- NMS Addresses
- Reboot

Tools

- Ping
- TFTP
- Remove Clients (MAP-3100 only)

Status

- Status
- Interfaces
- Services
- Ifconfig
- Route
- Users (MAP-3100 only)
- System Log
- Topology (MAP-3100 only)
- Mobile IP (MAP-3100 only)
- DHCP Client Info (MAP-3100 only)
- Neighbor

Help

3.2 System

3.2.1 System > System

System Information page is shown in Figure 3.2.1.1.

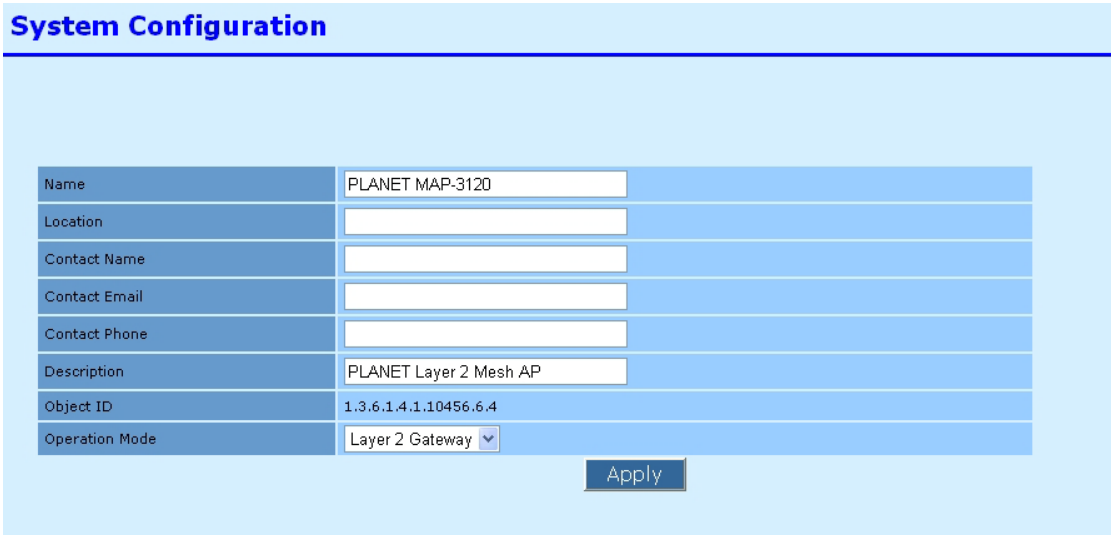


Figure 3.2.1.1: System Information page

To configure System Information:

a. Enter the name of device.

b. Enter the location name that device located.

c. Enter the contact person name for consulting about the device.

d. Enter the contact person Email address.

e. Enter the contact person phone number.

f. Enter the description of the device.

g. Object ID displays SNMP MIB object identification (OID) of system.

h. Click on **"Operation Mode"** to select "Gateway", "Relay", "Client Relay", "Layer 2 Gateway", or "Layer 2 Relay".

Gateway (MAP-3100 only)	Layer 3 Gateway Mode. In a Mesh network Gateway mode is the path to the Internet for the whole Mesh network behind. WAN port is active and will be used for Internet Connection. Three types of Internet connection will be available, please refer to section 3.3.2 for more.

Relay (MAP-3100 only)	Layer 3 Relay Mode. Relay mode can help to route between mesh backhaul and local WiFi/LAN network. Also, a Relay mode Mesh AP can help to route the packets from other Relay node to the destination IP subnet or Gateway. WAN port is disabled at this mode. At the same time no WAN setting is required.
Client-Relay (MAP-3100 only)	Layer 3 Client-Relay Mode. At this mode, the Mesh node can only route between local WiFi/LAN network to mesh backhaul. It will not help to route packets from other Relay node. This mode can be used to reduce the unnecessary routing especially if this Mesh node is in the edge of the whole mesh topology.
Layer 2 Gateway	Layer 2 Gateway Mode. At this mode, the Mesh AP can be viewed as a bridge. This bridge can bridge between WAN, LAN, Mesh backhaul, and WiFi. As a Gateway, the WAN interface will turns into the public bridge port that connects to the existing Ethernet network. Be noted, only ONE Gateway is allowed in the same Mesh network.
Layer 2 Relay	Layer 2 Relay Mode. At this mode, the Mesh node act as a mesh relay that can bridge between WAN, LAN, Mesh backhaul and WiFi.

i. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

⚠ ***Note***	For MAP-3000, if set to Layer 2 mode without any change to the IP settings, it will still remains at its default IP address instead of change to 192.168.0.1 that is being used for MAP-3020 by default. If you plan to set your MAP-3000 to Layer 2 mode, remember to write down the default IP address before you reboot the system.

3.2.2 System > Syslog

Syslog configuration page is shown in Figure 3.2.2.1.

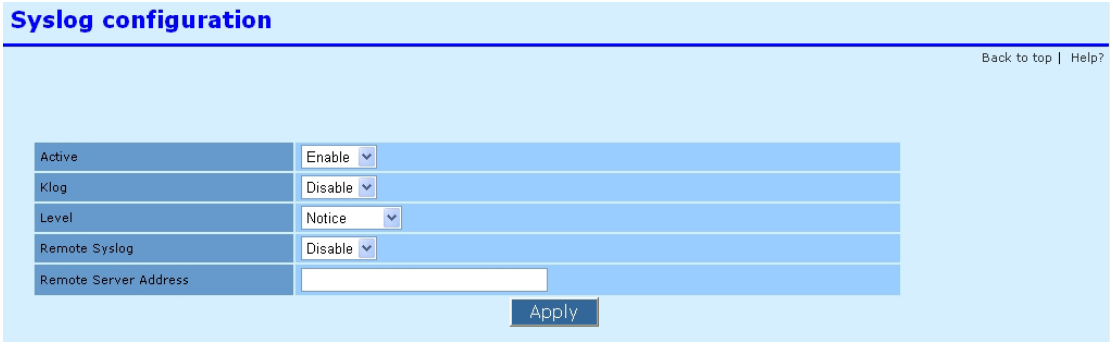


Figure 3.2.2.1: Syslog configuration page

To use Syslog:

a. Click on **"Active"** drop down menu to enable or disable System Logging service.

b. Click on **"Klog"** drop down menu to enable or disable Kernel Logging service.

c. Select the logging level. There are 8 levels. If "Debug" is selected, all messages will be recorded.

d. Click on **"Remote Syslog"** drop down menu to enable or disable remote syslog server.

e. Enter the remote syslog server address.

f. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.2.3 System > Advance

Advance configuration page is shown in Figure 3.2.3.1.

Networking-CONNTRACK	
Maximum session	212368 (4096~200000)
Generic Timeout	600 (50~1200s)
ICMP Timeout	30 (10~60s)
TCP Close Timeout	10 (5~30s)
TCP Close Wait Timeout	60 (10~120s)
TCP Established Timeout	3600 (600~864000s)
TCP Finished Wait Timeout	120 (10~3600s)
TCP Last ACK Timeout	30 (10~60s)
TCP SYN Receive Timeout	60 (10~120s)
TCP SYN Sent Timeout	120 (10~240s)
TCP Time Wait Timeout	120 (10~240s)
UDP Timeout	30 (10~60s)
UDP Stream Timeout	180 (10~360s)

Wireless	
Radio 1 distance	400 (100~30000m)
Radio 1 ack timeout	25
Radio 2 distance	400 (100~30000m)
Radio 2 ack timeout	25
Country	United States
Outdoor Mode	Enable
External Channel Mode	Disable
Preamble Type	Short
Extended Range Mode	Enable (Hardware not supported)
Fast Frame Mode	Enable
Compression Mode	Enable
Bandwidth Mode	Normal (20Mhz)
Mesh Minimum Signal Strength:	15

Figure 3.2.3.1: Advance configuration page

The parameters in “Networking-CONNTRACK” field are for performance fine-tuning. They are not suggested to be altered unless you have fully understood the meaning and effect of every parameter.

Maximum session	Maximum allowable IP connection tracking session. Range: 4096 ~ 212368; Default: 10000 sessions

Generic Timeout	Timeout value in seconds (s) for generic connection track entry. Range: 50 ~ 1200; Default: 600 seconds.
ICMP Timeout	Timeout value in seconds (s) for ICMP entry. Range: 10 ~ 60; Default: 30 seconds.
TCP Close Timeout	Timeout value in seconds (s) for TCP close. Range: 5 ~ 30; Default: 10 seconds.
TCP Close Wait Timeout	Timeout value in seconds (s) for TCP close wait. Range: 10 ~ 120; Default: 60 seconds.
TCP Established Timeout	Timeout value in seconds (s) for established TCP. Range: 600 ~ 864000; Default: 3600 seconds.
TCP Finished Wait Timeout	Timeout value in seconds (s) for TCP finished wait. Range: 10 ~ 3600; Default: 120 seconds.
TCP Last ACK Timeout	Timeout value in seconds (s) for TCP last acknowledgement. Range: 10 ~ 60; Default: 30 seconds.
TCP SYN Receive Timeout	Timeout value in seconds (s) for TCP SYN receive. Range: 10 ~ 120; Default: 60 seconds.
TCP SYN Sent Timeout	Timeout value in seconds (s) for TCP SYN sent. Range: 10 ~ 240; Default: 120 seconds.
TCP Time Wait Timeout	Timeout value in seconds (s) for TCP time wait. Range: 10 ~ 240; Default: 120 seconds.
UDP Timeout	Timeout value in seconds (s) for UDP. Range: 10 ~ 60; Default: 30 seconds.
UDP Stream Timeout	Timeout value in seconds (s) for UDP stream. Range: 10 ~ 360; Default: 180 seconds.
Radio 1 distance	Specify the operating radius in meter (m) of radio 1. Range: 100 ~ 10000; Default: 400 meters.
Radio 2 distance	Specify the operating radius in meter (m) of radio 2. Range: 100 ~ 10000; Default: 400 meters.
Country	Select the operating country of the wireless interface.
Outdoor Mode	Enable or Disable the outdoor mode for the wireless interface. Default: Enable.
External Channel Mode	Enable or Disable the external channel mode for the wireless interface. Default: Disable.
Preamble Type	The default is "Short" setting takes less time when used in a good environment.
Fast Frame Mode	Enable to support super G mode Default: Enable.

Bandwidth Mode	Setup the bandwidth for Wireless Transmission, Normal 20 MHz and Turbo 40MHz Bandwidth Default: 20MHz
Mesh Minimum Signal Strength	Mesh Backhaul Filter. With this numerical value, the Mesh system will filter the weak connection accorginly. Range from 0 to 60.. Default: 0 (disable)

3.2.4 System > Profile

Profile settings page is shown in Figure 3.2.4.1.

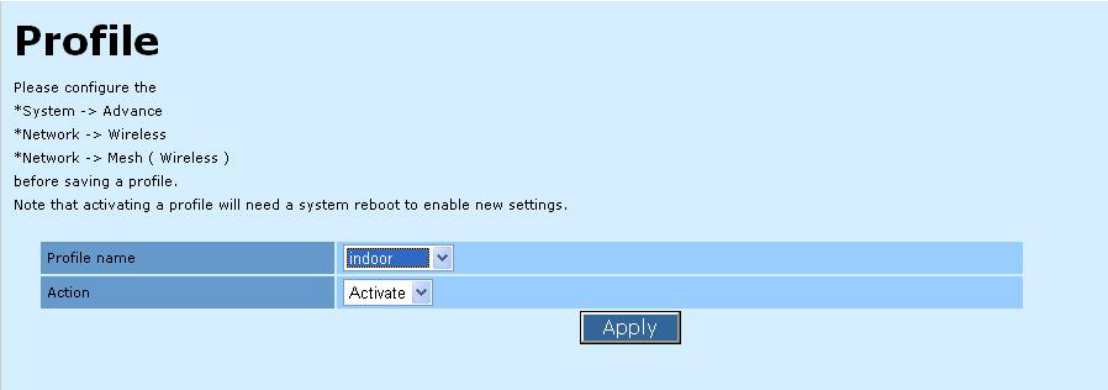


Figure 3.2.4.1: Profile settings page

There are 4 pre-defined profiles in mesh AP. Select the proper profile according to real operating condition, then click **Apply**. The profile will be activated after system reboot.

The four modes are:

Indoor	Indoor Mode For indoor operation, operating range around 100 meters
OutdoorLR	Outdoor Long Range Mode For distance above 10km between Mesh nodes. Be noted, long distance connectivity will effect the overall performance. Unless there is demand for long distance node to node bridging, it is not suggested to use this mode for mass installation.
OutdoorMR	Outdoor Middle Rang Mode For distance above 1km.
OutdoorSR	Outdoor Short Range Mode For distance above 400 meters and below 1 kilometers.

3.3 Network

3.3.1 Network > DNS Setting

Network configuration page is shown in Figure 3.3.1.1.

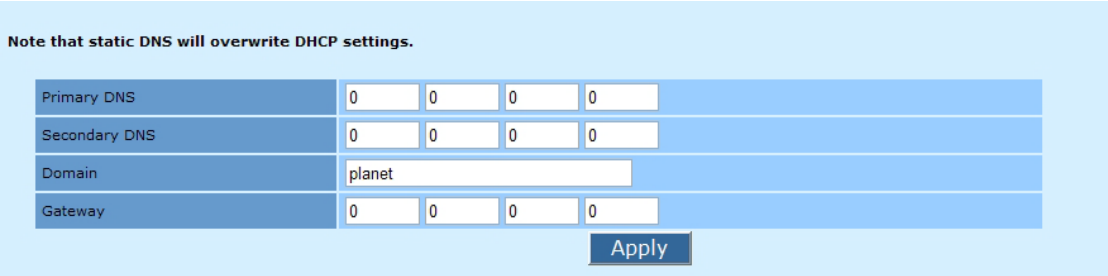


Figure 3.3.1.1: Network configuration page

Primary DNS	Primary Domain Name Server is used to translate domain names to IP addresses. Edit this field to match your ISP DNS address. It is suggested to fill in this field no matter in gateway or relay mode.
Secondary DNS	[optional field] Secondary Domain Name Server is a backup DNS address to primary DNS.
Domain	Domain names for this device.
Gateway	WAN Port Gateway IP Address

3.3.2 Network > WAN (MAP-3100 only)

WAN (Wide Area Network) are used to connect local area networks (LANs) to other networks through your ISP (Internet Service Provider). WAN configuration page is shown in Figure 3.3.2.1.

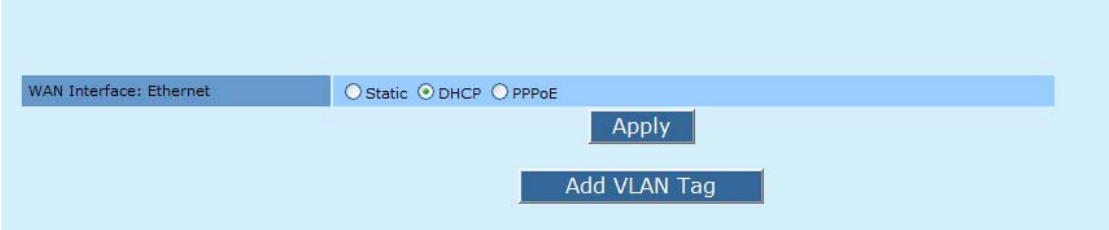


Figure 3.3.2.1: WAN configuration page

To configure WAN:

1. Choose option either for **Static**, **DHCP** or **PPPoE**.
2. Click on **"Apply"** button.
3. If you choose for **Static** option, Static IP configuration page will display as shown in Figure 3.3.2.2.

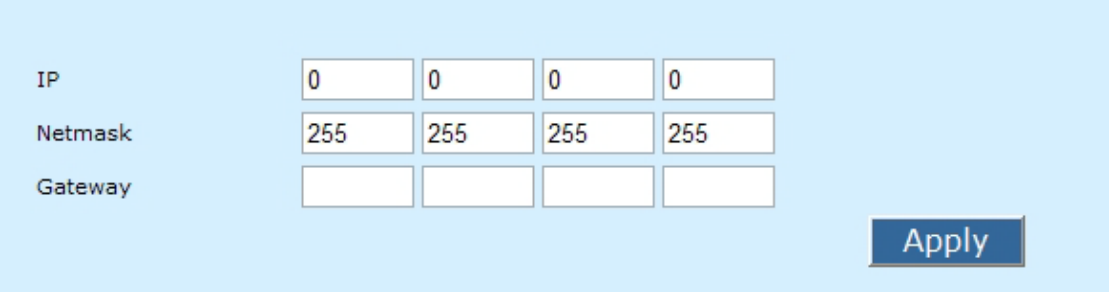


Figure 3.3.2.2: Static IP configuration page

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.
-

- **"Apply"** button – Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

4. If ISP or network assigns the IP address dynamically using a DHCP server, select "**DHCP**" radio button and press **Apply**. Using this option, all the network related configuration will be provided by ISP or network.

Figure 3.3.2.3: DHCP Client configuration page

5. **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 3.3.2.4.

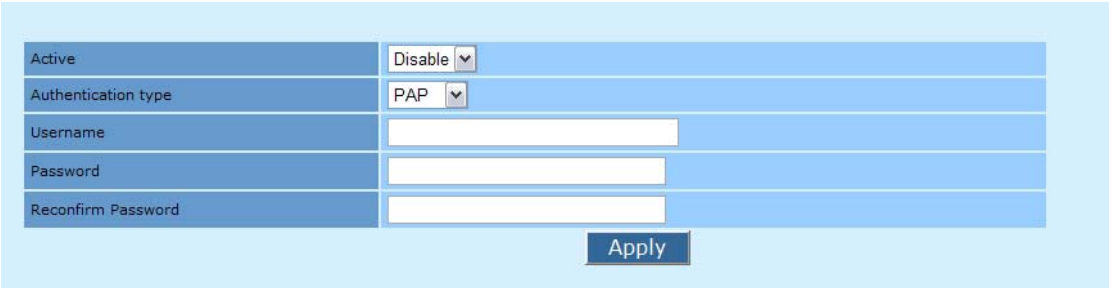


Figure 3.3.2.4: PPPoE configuration page

PPPoE configuration page contain the following parameter:

- **"Active"** - Click on **"Active"** drop down menu to select enable or disable PPPoE service.
- Authentication type- Choose the "PAP/CHAP" PPP control protocols.
- **Username** – Specify PPPoE service username.
- **Password** – Specify PPPoE service password.

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

⚠ ***Note***	1. If your Ethernet network that connect to WAN port supports VLAN tagging and you plan to make the Mesh Network route for different purpose, you can use the "Add VLAN Tag" button to create different VLAN for WAN interface. 2. Only the **default WAN** is **un-tagged**. Any other newly inserted WAN interface will be tagged follow the ID setting that range from 1 to 4095. Maximum is 15 virtual WAN interfaces are allowed.

3.3.3 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. VLAN configuration page is shown in Figure 3.3.3.1. The default VLAN IP of every layer 3 node is different. However, when the device is in layer 2 mode, its default VLAN IP is always 192.168.0.1.

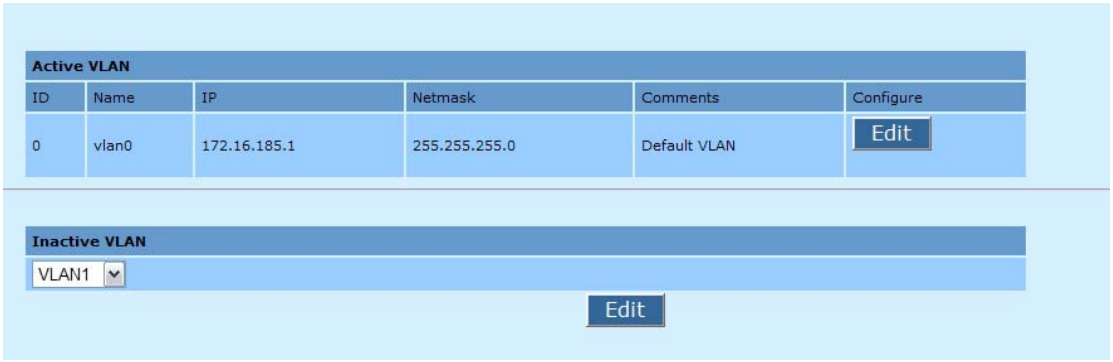


Figure 3.3.3.1: VLAN configuration page

To configure VLAN:

- "Active VLAN" list all activated VLAN. By default, only VLAN0 is active. Click on top **"Edit"** button to edit active VLAN.
- VLAN0 – edit page will display as shown in Figure 3.3.3.2.

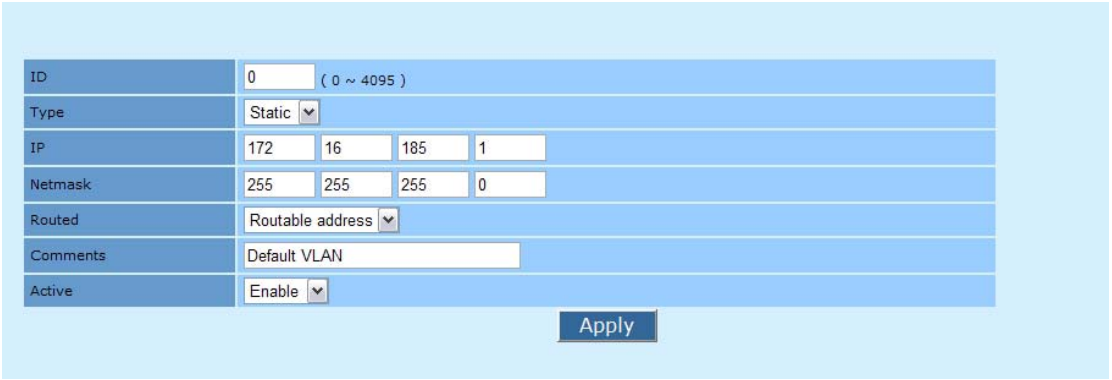


Figure 3.3.3.2: VLAN0 – edit page

VLAN0 - edit page contain the following parameter:

- **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 "Routable 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 - Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

g. 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.

h. VLAN1 – edit page will display as shown in Figure 3.3.3.3.

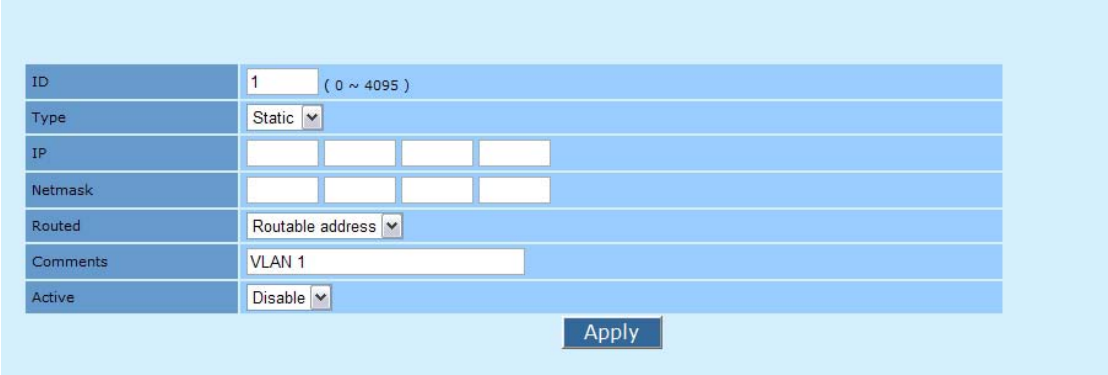


Figure 3.3.3.3: VLAN1 – edit page

VLAN1 - edit page contain the following parameter:

a. Type – Click on **"Type"** drop down menu to select "Static" or "DHCP".

b. Routed – Click on **"Routed"** drop down menu to select "Routable address" or "NAT address".

c. Comments – Specify the VLAN1 comments.

d. Active – Click on **"Active"** drop down menu to enable or disable VLAN1.

e. **"Apply"** button – Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

⚠ ***Note***	1. ONLY VLAN 0, the default VLAN, is un-tagged packets. For VLAN 1 to VLAN 15, it will be tagged packets at LAN interface after it is enabled. And for Wireless interface, different SSID are required for different VLAN. 2. The connected LAN device should support VLAN tagging if you plan to connect wired device for different VLAN.

3.3.4 Network > Mesh

⚠ ***Note***	Only when device is in layer 3 mode, the Mesh interface requires an isolated IP address. When device is in layer 2 mode, its Mesh interface uses the same IP address as its default VLAN.

The layer 3 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 layer 3 devices have 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. You can edit the following Mesh configuration page is shown in Figure 3.3.4.1.

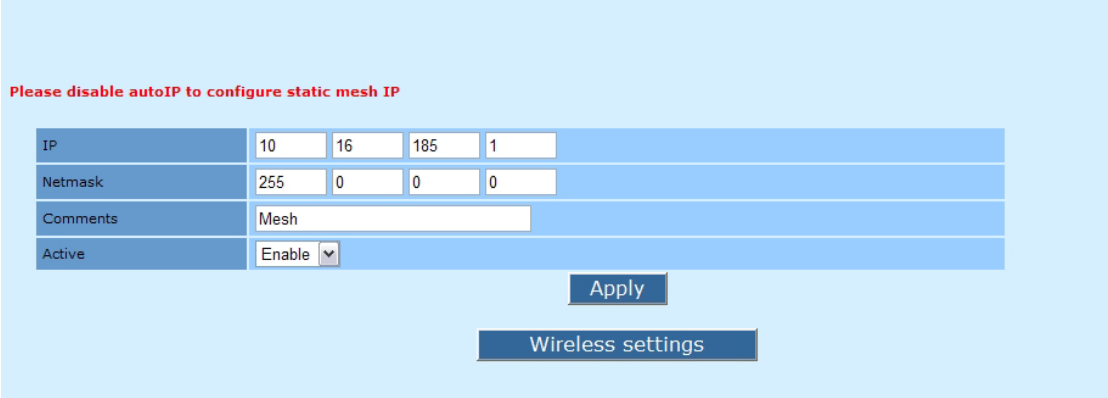


Figure 3.3.4.1: Mesh configuration page

To configure Mesh:

- Specify the Mesh IP address.
- Specify the Network mask for this IP.
- Specify the Mesh comments.
- Click on **"Active"** drop down menu to enable or disable Mesh.
- Click on **"Apply"** button if you have made any changes. 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 3.3.4.2.

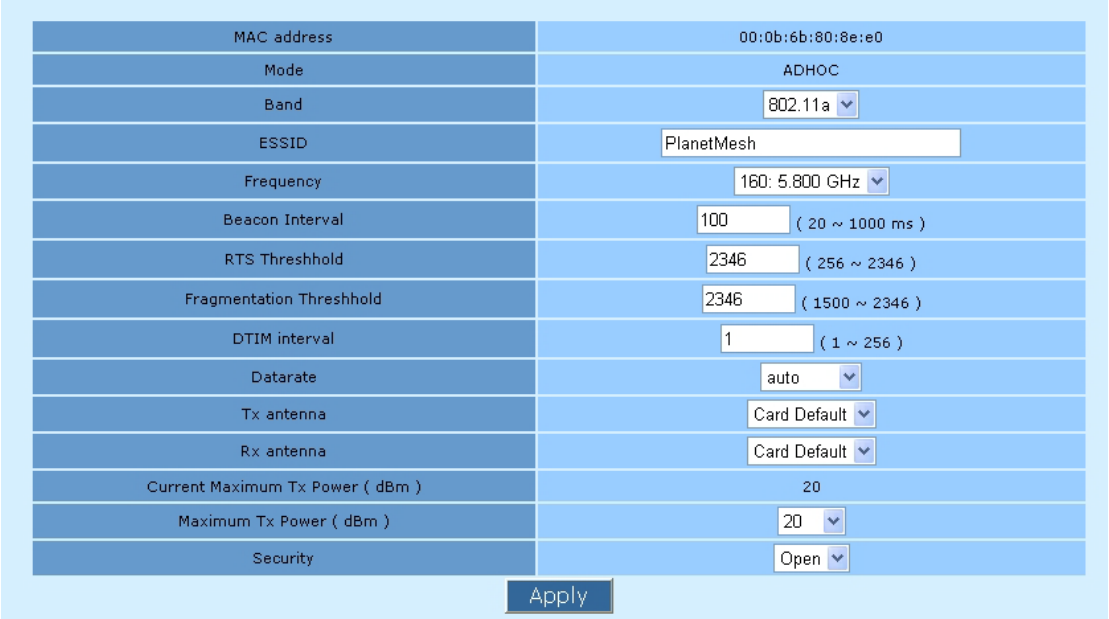


Figure 3.3.4.2: Mesh - wireless configuration page

Mesh – wireless page contain the following parameter:

- **MAC address** – Display the MAC address of Mesh – wireless interface.
- **Mode** – **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.
- **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 2.4GHz spectrum 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".
- **Security** – Add security features to the wireless network. Click on **"Security"** drop down button to select "Open", "WEP" or "AES".
    - 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.
    - AES: Advanced Encryption Standard. A encryption scheme that uses 128-bit to encrypt the network packets.
- **"Apply"** button – Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.3.5 Network > Wireless

AP configuration page is shown in Figure 3.3.5.1.

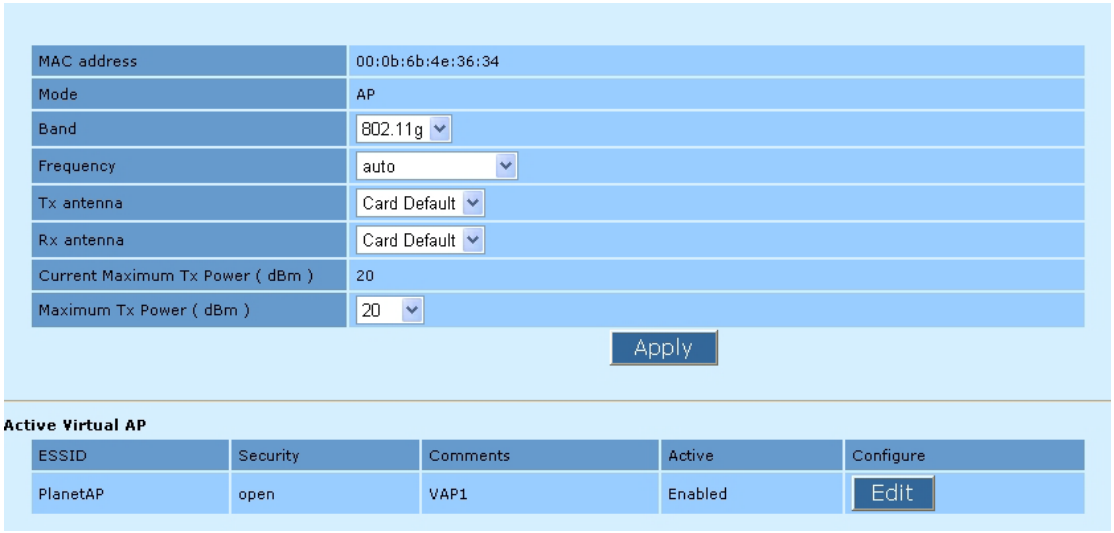


Figure 3.3.5.1: AP configuration page

To configure wireless AP interface:

A. Mac address displays the MAC address of interface.

B. Mode displays the operating mode: AP.

C. Click on **"Band"** drop down menu to select "802.11a", "802.11b" or "802.11g" operating band.

D. Click on **"Frequency"** drop down menu to select operating frequency of the wireless network in Mhz.

E. Click on **"Tx antenna"** drop down menu to select "Diversity", "Port 1", "Port 2" or "Card Default".

F. Click on **"Rx antenna"** drop down menu to select "Diversity", "Port 1", "Port 2" or "Card Default".

G. Current Tx Power shows current transmit power of the wireless card due to regulatory limitation

H. Select Tx Power of the AP wireless card.

I. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

J. Click on **"Edit"** button to edit Active Virtual AP. AP configuration – edit page is shown in Figure 3.3.5.2.

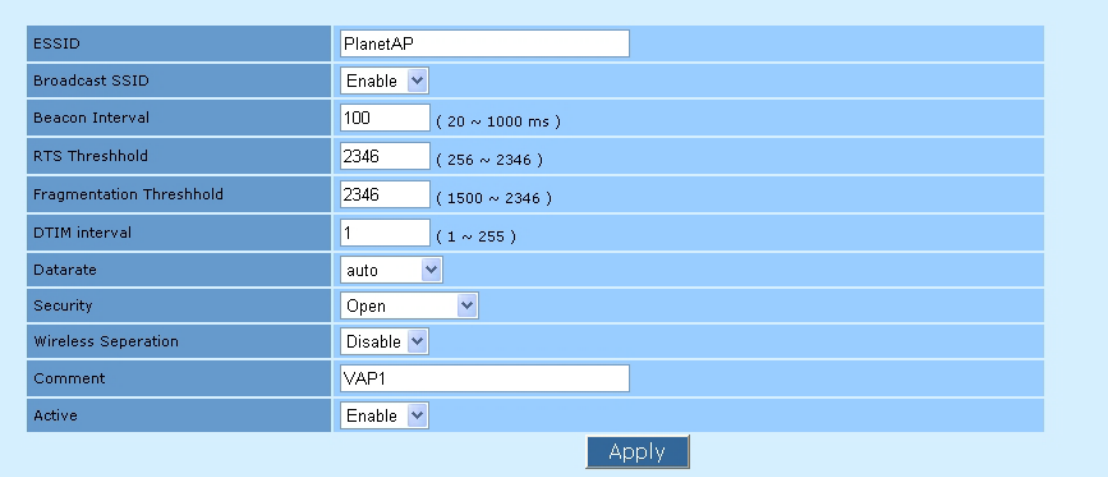


Figure 3.3.5.2: AP configuration – edit page

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", or "AES".
    - Open: no encrytion 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.
    - AES: Advanced Encryption Standard. A encryption scheme that uses 128-bit to encrypt the network packets.

- Wireless Separation-Prevent the Wireless users to access each other.
- **“Apply”** button – Click on **“Apply”** button if you have made any changes. New settings are active after the device reboot.

3.3.6 Network > Route

Routing refers to selecting paths in a network along which to send data. Route configuration page is shown in Figure 3.3.6.1.

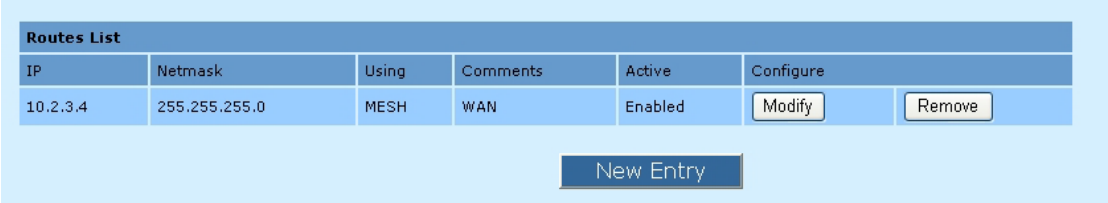


Figure 3.3.6.1: Route configuration page

To configure Route:

a. To modify or remove specified route, click the button from "**Configure**" field.

b. If you want to add new route, click "**New Entry**" button. Routes – add page will display as shown in Figure 3.3.6.2.

Figure 3.3.6.2: Routes – add 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.
- **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** – Click on **"Active"** drop down menu to enable to disable this interface.

- **"Apply"** button – Click on **"Apply"** button to confirm add route. New settings are active after the device reboot.

c. If you select to edit existing route, a page similar to Figure 3.3.6.2 with configured settings will be displayed.

⚠ ***Note***	In default, the gateway for MAP-3120 should be configured in DNS Setting page

3.3.7 Network > IPSEC (MAP-3100 only)

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. IPSEC configuration page is shown in Figure 3.3.7.1.

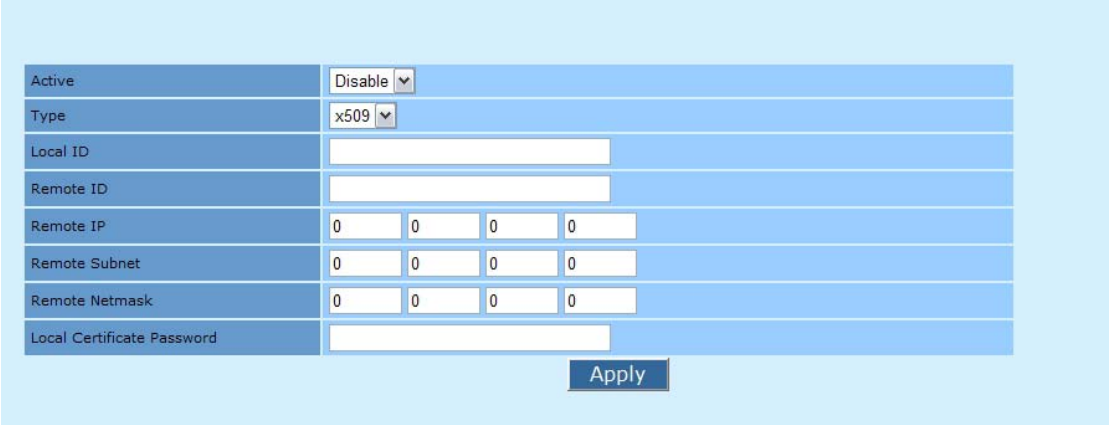


Figure 3.3.7.1: IPSEC configuration page

To configure IPSEC:

a. Click on **"Active"** drop down menu to enable or disable IPSEC service.

b. Click on **"Type"** drop down menu to select "x509", "RSA", or "PSK" type of IPSEC service.

c. Enter the local identity.

d. Enter the remote identity.

e. Enter the IP address of remote IP.

f. Enter the IP address of remote Subnet.

g. Enter the network mask.

h. Enter local certificate password.

i. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.3.8 Network > L2TPC (MAP-3100 only)

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). L2TPC serves as a L2TP client that creates a tunnel through existing network to the designated peer computer or network. L2TCP configuration page is shown in Figure 3.3.8.1.

Figure 3.3.8.1: L2TPC configuration page

To configure L2TPC:

- Click on **"Active"** drop down menu to enable or disable L2TPC service.
- Enter the L2TP LNS address.
- Enter L2TP username.
- Enter L2TP password.
- Re-enter L2TP password to confirm it.
- Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.3.9 Network > OLSR (MAP-3100 only)

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. OLSR configuration page is shown in Figure 3.3.9.1.

Figure 3.3.9.1: OLSR configuration page

To configure OLSR:

a. Click on **"Active"** drop down menu to enable or disable OLSR service.

b. 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)

c. Click on **"Willingness"** drop down menu to enable or disable Willingness. Willingness will be calculated dynamically if disabled

d. Enter the Willingness level.

e. Hysteresis adds more robustness to the link sensing but delays neighbor registration. Click on **"Hysteresis"** drop down menu to enable or disable Hysteresis.

f. Enter the Hysteresis Scaling.

g. Enter the Hysteresis THR High value.

h. Enter the Hysteresis THR Low value.

i. Enter the Link Quality Type.

j. Enter the Link Quality Size.

k. Enter the Poll rate.

l. 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.

m. Specify how many MPRs a node should try select to reach every 2 hop neighbor. Default is 1.

n. Specify a pre-shared key for the control traffic. Control traffic with different shared key will be discarded.

o. Re-enter the Shared Key to confirm it.

p. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

⚠ ***Note***	Unless you are familiar with the setting, otherwise we would suggest to keep the value unchanged, or press Reset to set back to default. These settings should fit for the most application.

3.4 Service

3.4.1 Service > DHCPD (MAP-3100 only)

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. DHCPD configuration page is shown in Figure 3.4.1.1.

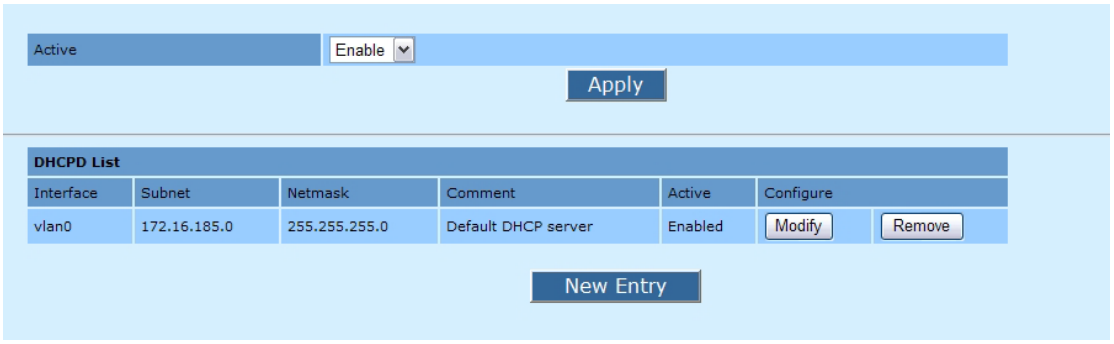


Figure 3.4.1.1: DHCPD configuration page

To configure DHCPD:

a. To modify or remove specified DHCPD entry, click the button from "**Configure**" field.

b. If you select to add new DHCPD entry, DHCPD – add page will display as shown in Figure 3.4.1.2.

Figure 3.4.1.2: DHCPD – add page

DHCPD – add page contain the following parameter:

a. **Interface** – Click on **"Interface"** drop down menu to select interface.

b. **Subnet** – Enter the interface network address.

c. **IP Start** – Enter the IP address of IP start.

d. **IP End** – Enter the IP address of IP end.

e. **Netmask** – Enter the network mask for this network address.

f. **Max Lease** – Enter the value of Max Lease.

g. **Lease** – Enter the value of Lease.

h. **Domain** – Enter the name of Domain.

i. **DNS** – Enter the network address of DNS.

j. **Router** – Enter the network address of Router.

k. **Comments** – Enter the DHCPD comments.

l. **Active** – Click on **"Active"** drop down menu to select enable or disable this interface.

m. **"Apply"** button – Click on **"Apply"** button to confirm add DHCPD. New settings are active after the device reboot.

n. If you select to edit existing DHCPD, a page similar to Figure 3.4.1.2 with configured settings will be displayed.

3.4.2 Service > Firewall (MAP-3100 only)

Firewall is used to allow or deny data either in or out. Firewall configuration page is shown in Figure 3.4.2.1.

Figure 3.4.2.1: Firewall configuration page

To configure Firewall:

a. Click on **"Active"** drop down menu to enable or disable Firewall service.

b. Click on top **"Apply"** button to confirm enable or disable Firewall service. New settings are active after the device reboot.

c. From "**Configure**" field, you can "**Modify**" or "**Remove**" Firewall.

d. If you select to add new Firewall entry, Firewall – add page will display as shown in Figure 3.4.2.1

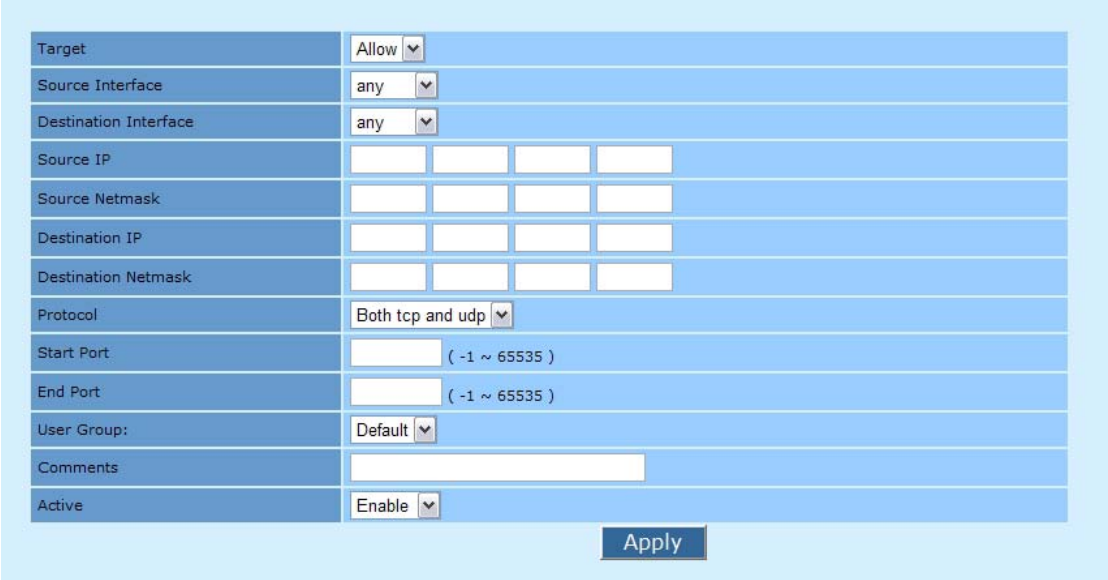


Figure 3.4.2.1: Firewall – add page

Firewall - add page contain the following parameter:

- **Target** – Click on **"Target"** drop down menu to allow or deny 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 – Click on **"Apply"** button to confirm add Firewall. New settings are active after the device reboot.

e. If you select to edit existing Firewall, a page similar to Figure 3.4.2.1 with configured settings will be displayed.

3.4.3 Service > MAC Access

MAC Access provides another level of security by filtering the packets coming into the device. MAC Access configuration page is shown in Figure 3.4.3.1.

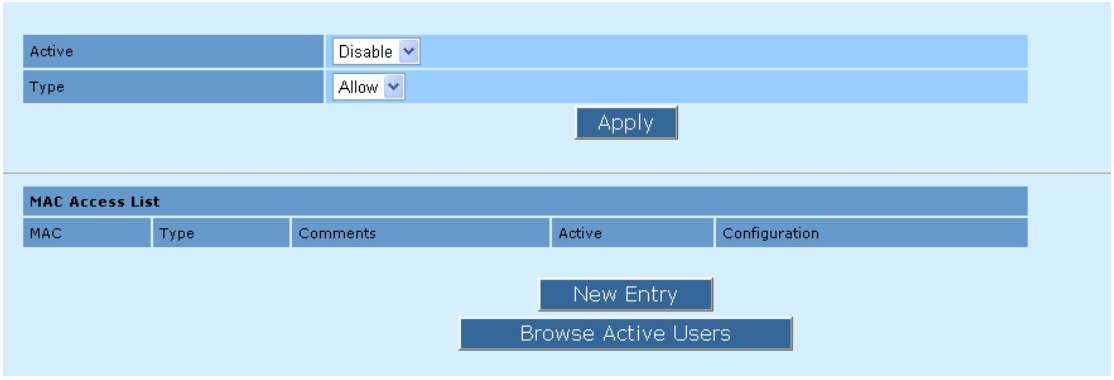


Figure 3.4.3.1: MAC Access configuration page

To configure MAC Access:

a. Click on **"Active"** drop down menu to enable or disable MAC Access control.

b. Click on **"Type"** drop down menu to allow or deny access to the listed MAC.

c. Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.

d. From "**Configure**" field, you can "**Modify**" or "**Remove**" MAC Access.

e. If you select to add new MAC Access entry, MAC Access – add page will display as shown in Figure 3.4.3.2.

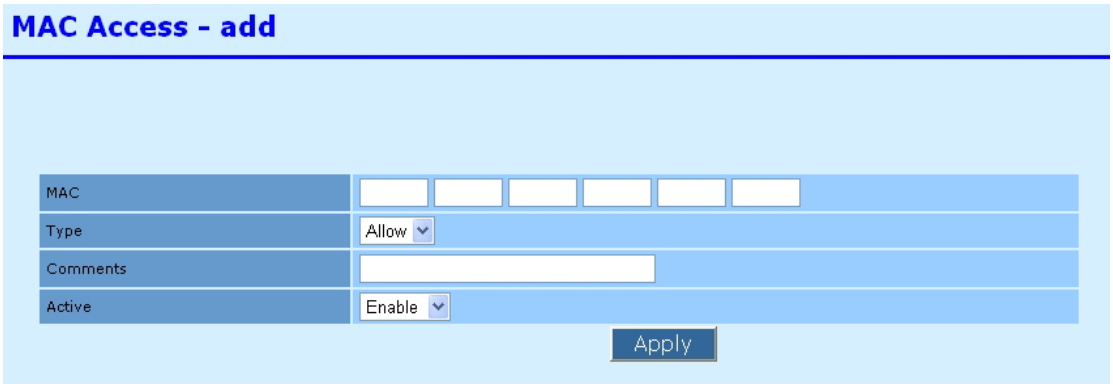


Figure 3.4.3.2: MAC Access – add page

MAC Access - add page contain the following parameter:

- **MAC** – Enter the MAC address.
- **Comments** – Enter MAC Access comments.
- **Active** – Click on **"Active"** drop down menu to enable or disable MAC Access.
- **"Apply"** button – Click on **"Apply"** button to confirm add MAC Access. New settings are active after the device reboot.

f. If you select to edit existing MAC Access, a page similar to Figure 3.4.3.2 with configured settings will be displayed.

Note

1. Turn on the MAC Filter with Type "Deny", it will block all the accessing from WiFi or LAN. Be sure to key in, at least the manager's MAC address or one known MAC address from "MAC Access List" with Type "Allow" before your reboot to make this feature active.
2. If you would like to BLOCK some certain backhaul route, you can Turn on MAC filter with "Allow". Yet, in the "MAC Access List", key in the desired Mesh node's MAC address (that can be found in Neighbor in section 3.7.10) with Type "Deny". Then, you can stop some unnecessary route to make the network more efficient. However, this also will effect the self-healing once the backhaul node to node relationship is broken.

3.4.4 Service > Virtual Server (MAP-3100 only)

Virtual Server involves re-writing the source and/or destination address of IP packets as they pass through this device. Virtual Server configuration page is shown in Figure 3.4.4.1.

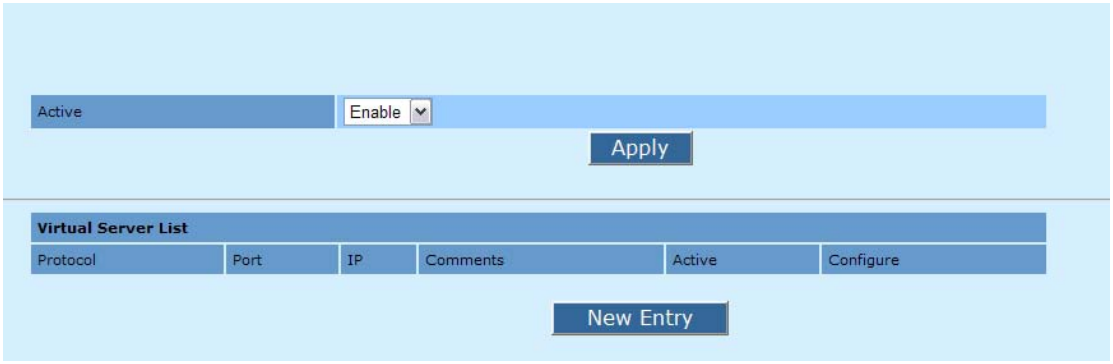


Figure 3.4.4.1: Virtual server configuration page

To configure Virtual Server:

a. Click on **"Active"** drop down menu to enable or disable service.

b. Click on top **"Apply"** button to confirm enable or disable service. New settings are active after the device reboot.

c. From "**Configure**" field, you can to select "**Modify**", or "**Remove**" virtual server.

d. If you select to add new entry, Virtual Server – add page will display as shown in Figure 3.4.4.2.

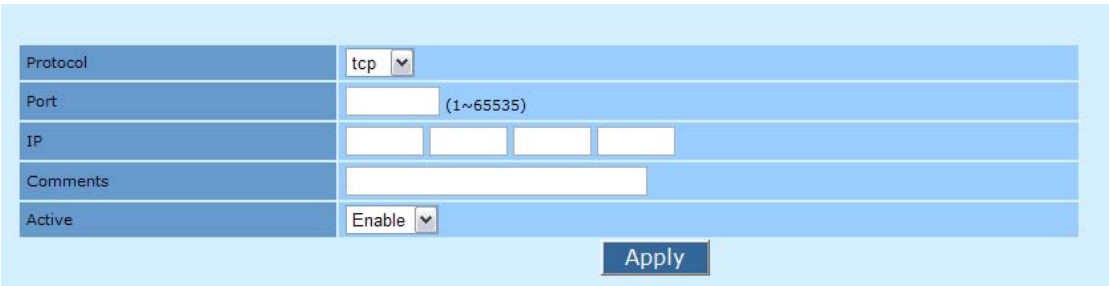


Figure 3.4.4.2: Virtual server – add page

Virtual server - add page contain the following parameter:

- **Protocol** – Click on **"Protocol"** drop down menu to select protocol.
- **Port** – Enter the Port number.
- **IP** – Enter the virtual server IP address.

- **Comments** – Enter proper comments.
- **Active** – Click on **"Active"** drop down menu to enable or disable this virtual server.
- **"Apply"** button – Click on **"Apply"** button to confirm add record. New settings are active after the device reboot.

e. If you select to edit existing virtual server, a page similar to Figure 3.4.4.2 with configured settings will be displayed.

3.4.5 Service > NTP

Network Time Protocol (NTP) is a protocol for synchronizing the system clocks over data networks. NTP configuration page is shown in Figure 3.4.5.1.

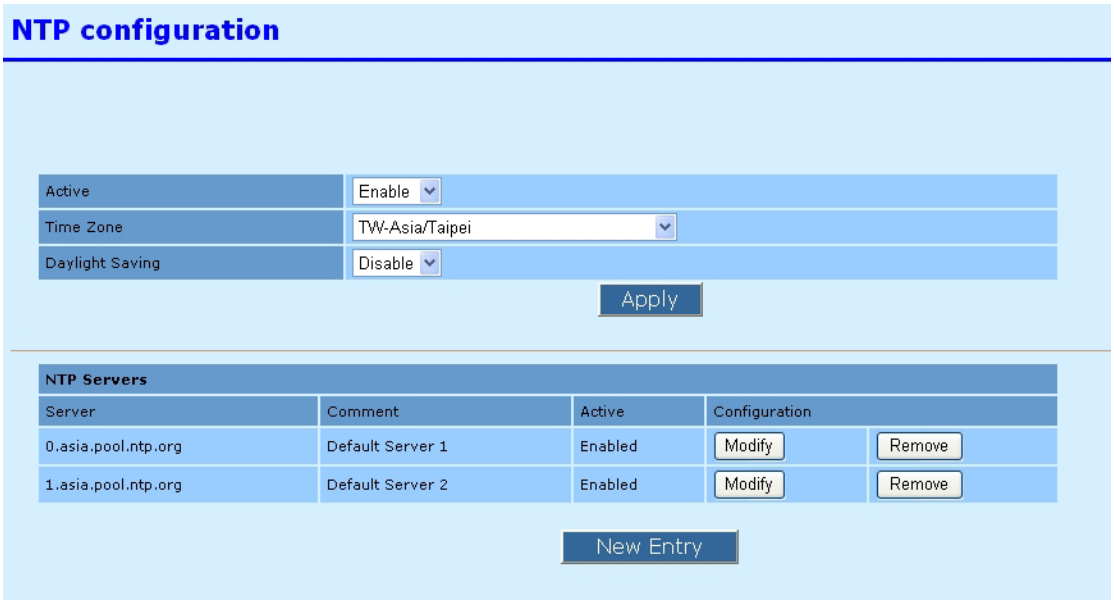


Figure 3.4.5.1: NTP configuration page

To configure NTP:

a. Click on **"Active"** drop down menu to enable or disable NTP service.

b. Click on **"Time Zone"** drop down menu to select suitable time zone.

c. Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.

d. From **"Configuration"** field, you can select **"Modify"** or **"Remove"** NTP server.

e. If you select to add new NTP server entry, NTP server – add page will display as shown in Figure 3.4.5.2.

Note	Please also make sure “DNS settings” in section 3.3.1 is well configured to make this feature functions.

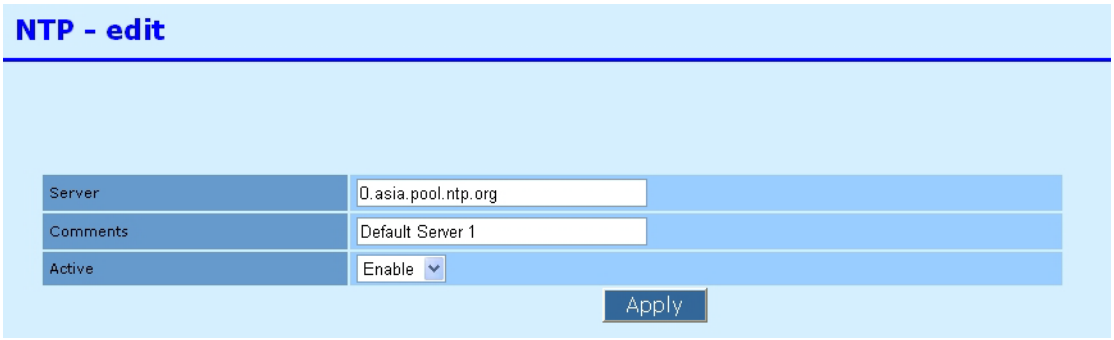


Figure 3.4.5.2: NTP – add page

NTP server - add page contain the following parameter:

- **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 – Click on **“Apply”** button to confirm add NTP server. New settings are active after the device reboot.

f. If you select to edit existing NTP server, a page similar to Figure 3.4.5.2 with configured settings will be displayed.

3.4.6 Service > Traffic Shaping (MAP-3100 only)

Traffic Shaping will limit bandwidth allocated to each user. Traffic Shaping configuration page is shown in Figure 3.4.6.1.

Figure 3.4.6.1: Traffic Shaping configuration page

To configure Traffic Shaping:

a. Click on **"Active"** drop down menu to enable or disable traffic shaping.

b. Enter the WAN Uplink Speed in Mbps.

c. Enter the WAN Downlink Speed in Mbps.

d. Enter the User Uplink Speed in kbps.

e. Enter the User Downlink Speed in kbps.

f. Click on top **"Apply"** button if you have made any changes.

g. From **"Configuration"** field, you can select **"Modify"** or **"Remove**" Traffic Shaping rule.

h. If you select to add new Traffic Shaping entry, Traffic Shaping – add page will display as shown in Figure 3.4.6.2.

Figure 3.4.6.2: Traffic Shaping – add page

Traffic Shaping - add 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 – Click on **"Apply"** button to confirm add Traffic Shaping. New settings are active after the device reboot.

i. If you select to edit existing Traffic Shaping, a page similar to Figure 3.4.6.2 with configured settings will be displayed.

3.4.7 Service > PPTP Server (MAP-3100 only)

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPNs). PPTP Server configuration page is shown in Figure 3.4.7.1.

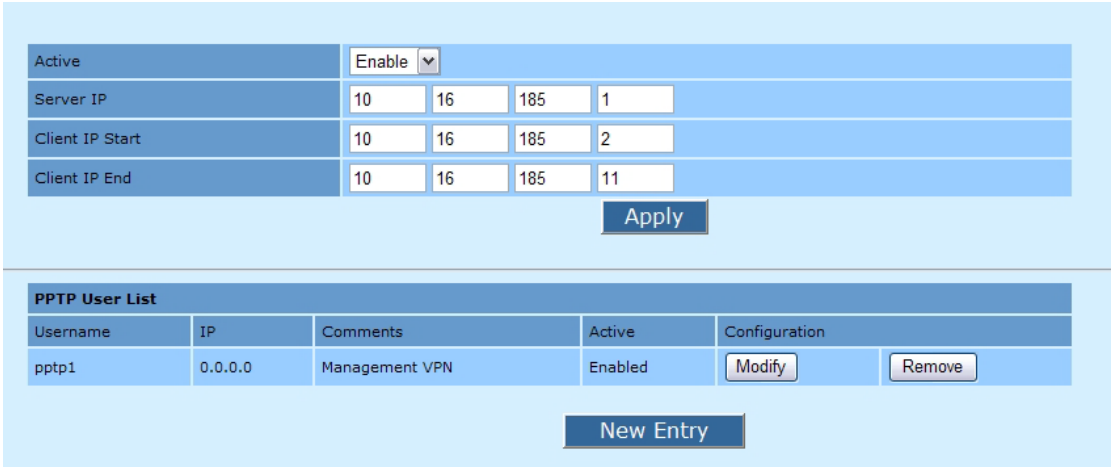


Figure 3.4.7.1: PPTP Server configuration page

To configure PPTP Server:

a. Click on **"Active"** drop down menu to enable or disable PPTP Server service.

b. Enter the PPTP Server IP address.

c. Enter Client Start address.

d. Enter Client End address.

e. Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.

f. From **"Configuration"** field, you can select **"Modify"** or **"Remove"** PPTP user.

g. If you select to add new PPTP user entry, PPTP User – add page will display as shown in Figure 3.4.7.2.

Figure 3.4.7.2: PPTP User – add 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 IP address assigned to this user.
- **Comments** – Enter the PPTP comments.
- **Active** – Click on **"Active"** drop down menu to enable or disable this PPTP.
- **"Apply"** button – Click on **"Apply"** button to confirm add new PPTP User. New settings are active after the device reboot.

h. If you select to edit existing PPTP User, a page similar to Figure 3.4.7.2 with configured settings will be displayed.

3.4.8 Service > AutoIP (MAP-3100 only)

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. Configuration page is show in Figure 3.4.8.1.

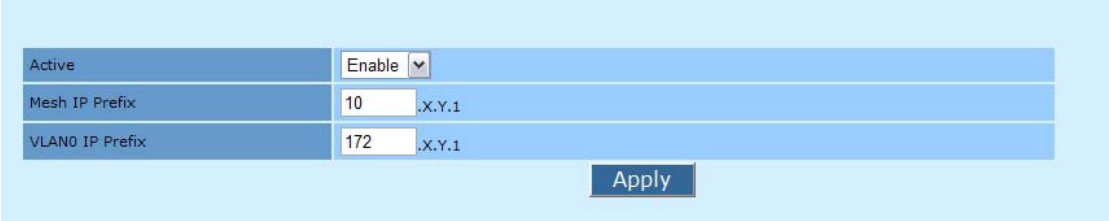


Figure 3.4.8.1

To configure AutoIP,

- Click on Active drop down menu to enable or disable autoIP.
- Assign a Mesh IP Prefix to it. Default is 10.
- Assign a VLAN0 IP Prefix to it. Default is 172.
- Click “Apply” to save any changes made. New settings will be active after reboot.

3.4.9 Service > Captive Portal (MAP-3100 only)

Captive portal forces an HTTP client on a network to see a special authentication web page before surfing the Internet normally. Captive Portal configuration page is shown in Figure 3.4.9.1.

Figure 3.4.9.1: Captive Portal configuration page

To configure Captive Portal:

- Click on **"Webbased Authentication"** drop down menu to enable or disable Web based Authentication.
- Enter the URL to redirect users to this URL on success.
- Click on **"POP3 Email Push"** drop down menu to enable or disable Push email to not authenticated users.
- Click on **"External Login Server"** drop down menu to enable or disable External Login Server.
- Enter the External Server URL.
- Enter the Default Idle Timeout.
- Enter the Default Session Timeout.
- Click on **"Login using HTTP"** drop down menu to enable or disable login with HTTP.

- Enter the HTTP port number used in captive login.
- Click on **“Login using HTTPS”** drop down menu to enable or disable login with HTTPS.
- Enter the HTTPS port number used in captive login.
- Click on **“Internal Web Space”** drop down menu to enable or disable internal web space.
- Enter the port number of Web Space.
- Enter the default login language
- Click on **“Apply”** button if you have made any changes. New settings are active after the device reboot.

3.4.10 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. RADIUS client configuration page is shown in Figure 3.4.10.1.

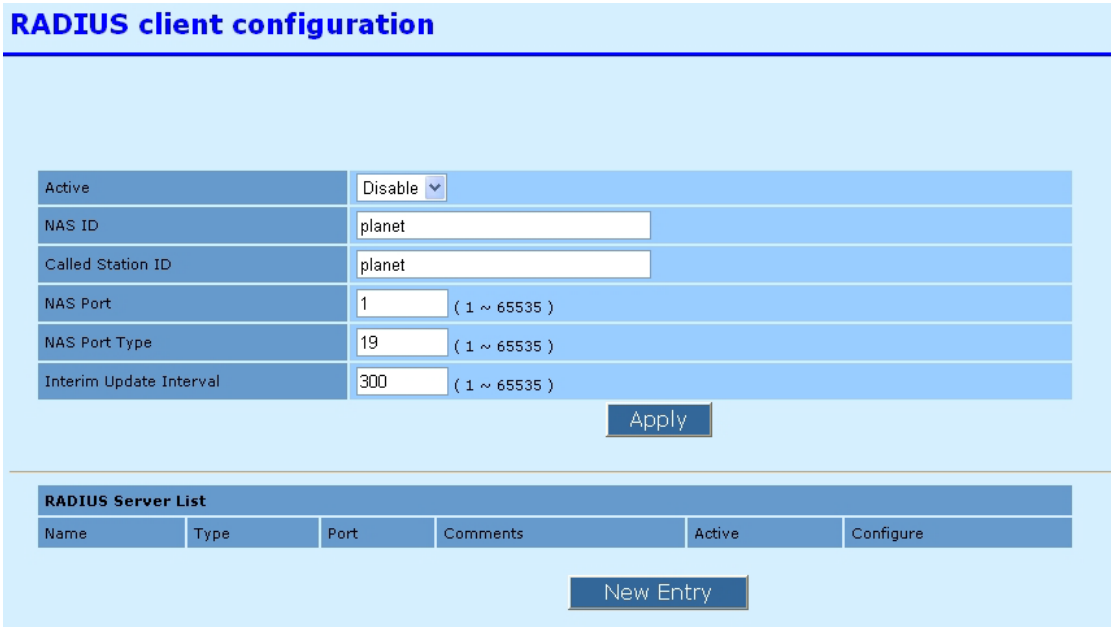


Figure 3.4.10.1: RADIUS client configuration page

To configure RADIUS client:

a. Click on **"Active"** drop down menu to enable or disable RADIUS client.

b. Enter the NAS ID.

c. Enter the Called Station ID.

d. Enter the NAS Port number.

e. Enter the NAS Port Type.

f. Enter the value of Interim Update Interval.

g. Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.

h. From "Configure" field, you can select "Modify" or "Remove" RADIUS server.

i. If you select to add new RADIUS server entry, RADIUS server – add page will display as shown in Figure 3.4.10.2.

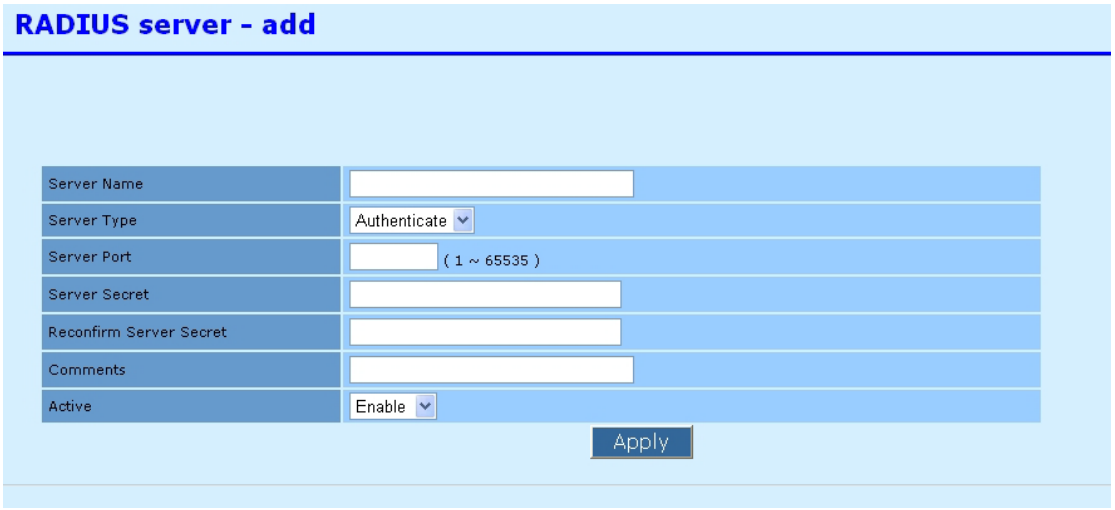


Figure 3.4.10.2: RADIUS server – add page

RADIUS server - add page contain the following parameter:

a. **Server Name** – Enter the RADIUS server name.

b. **Server Type** – Click on **"Server Type"** drop down menu to select "Authenticate" or "Accounting" server type.

c. **Server Port** – Enter the number of Server Port.

d. **Server Secret** – Enter the Server Secret key.

e. **Reconfirm Server Secret** – Re-enter the Server Secret key to confirm it.

f. **Comments** – Enter RADIUS server comments.

g. **Active** – Click on **"Active"** drop down menu to select enable or disable this entry.

h. **"Apply"** button – Click on **"Apply"** button to confirm add new RADIUS server. New settings are active after the device reboot.

i. If you select to edit existing RADIUS server, a page similar to Figure 3.4.10.2 with configured settings will be displayed.

3.4.11 Service > Dynamic DNS

Dynamic DNS allows an Internet domain name to be assigned with a dynamic IP address. Dynamic DNS configuration page is shown in Figure 3.4.11.1.

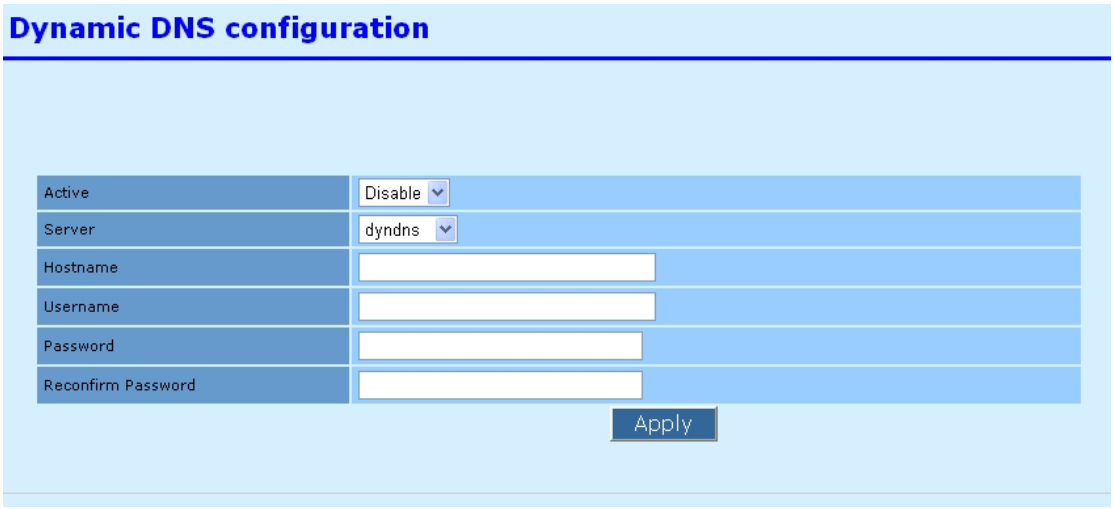


Figure 3.4.11.1: Dynamic DNS configuration page

To configure Dynamic DNS:

a. Click on **"Active"** drop down menu to enable or disable Dynamic DNS.

b. Click on **"Server"** drop down menu to select "dyndns", "easydns", "zoneedit", or "tzo" dynamic DNS provider.

c. Enter the Hostname that associated with the service provide.

d. Enter the Dynamic DNS username.

e. Enter the Dynamic DNS password.

f. Re-enter Dynamic DNS password to confirm

g. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.4.12 Service > Zero Config (MAP-3100 only)

Zero Config configuration page is shown in Figure 3.4.12.1.

Figure 3.4.12.1: Zero Config configuration page

To configure Zero Config:

a. Click on **"Active"** drop down menu enable or disable Zero Config service.

b. Click on **"Handle Client Proxy"** drop down menu to enable or disable it.

c. Enter the port number used in Proxy Login.

d. Click on **"Handle Static IP Client"** drop down menu to enable or disable it.

e. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.4.13 Service > Mobile IP (Future Feature for MAP-3100 only)

Mobile IP configuration page is shown in Figure 3.4.13.1.

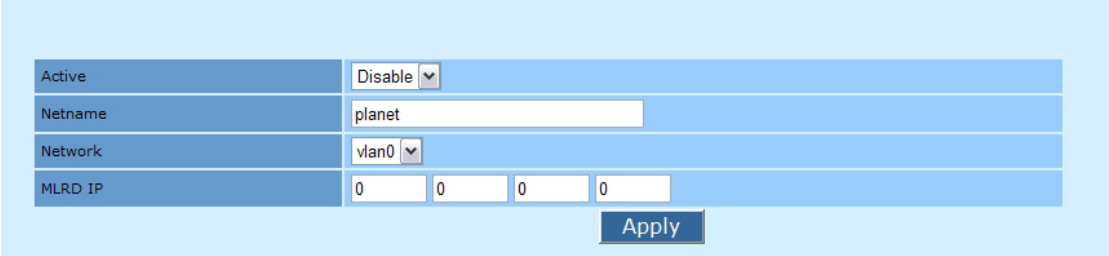


Figure 3.4.13.1: Mobile IP configuration page

To configure Mobile IP:

a. Click on **"Active"** drop down menu to enable or disable Mobile IP service.

b. Enter the Mobile IP network name.

c. Enter the IP address of the Mobile Location Register server.

d. Click on **"Apply"** button if you have made any changes. New settings are active after the device reboot.

3.4.14 Service > Route Watchdog (MAP-3100 only)

Route watchdog will probe for default route periodically. If default route is missing, it'll change the SSID of active wireless radio to a desired value such as "ServiceDown". If the default route still cannot be restored after specified number of interval, the system will be rebooted.

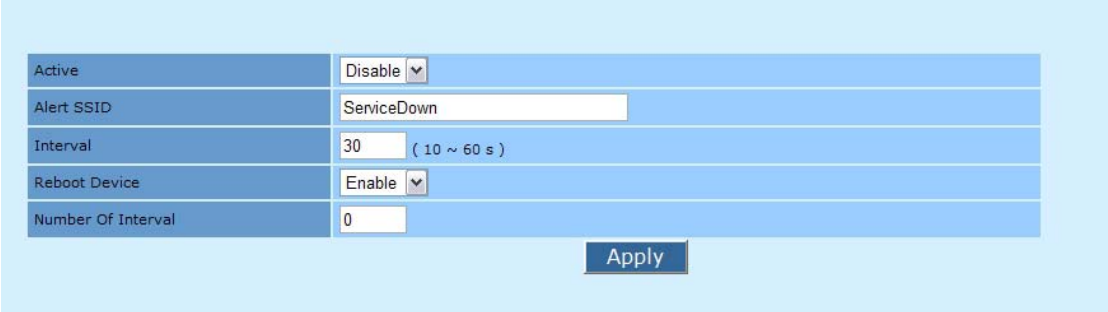


Figure 3.4.14.1: Route watchdog configuration page

To configure Route watchdog service:

- Click on "**Active**" drop down menu to enable or disable route watchdog service.
- Please specify the desired alert SSID.
- Please specify the interval for the route watchdog to check for the default route.
- Click on **"Reboot device"** drop down menu to enable or disable system reboot.
- Specify the number of retry interval before system reboot.
- Click on "**Apply**" to save new settings. Please reboot to enable new settings.

3.4.15 Service > System Watchdog

System 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.

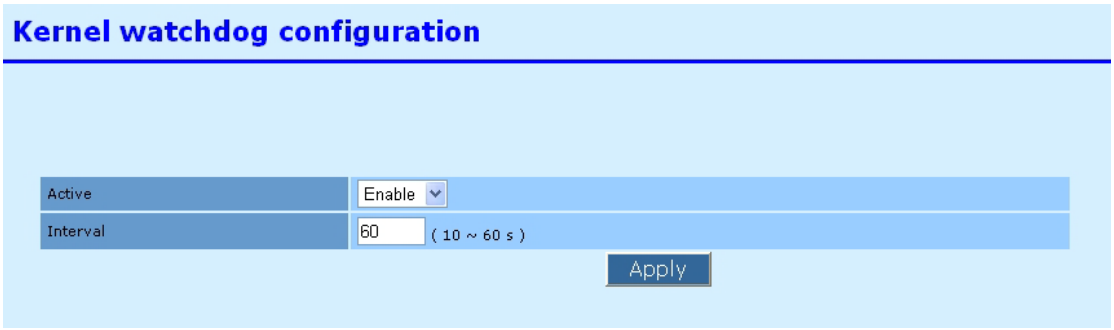


Figure 3.4.15.1: System watchdog configuration page

To configure System watchdog service:

- Click on "**Active**" drop down menu to enable or disable this service
- Specify the interval watchdog will pull for system status.
- Click on "**Apply**" button to save settings. Please reboot to enable new settings.

3.5 Management

3.5.1 Management > HTTPD

Webbased configuration management is done through the secure HTTP. HTTPD server configuration page is shown in Figure 3.5.1.1.

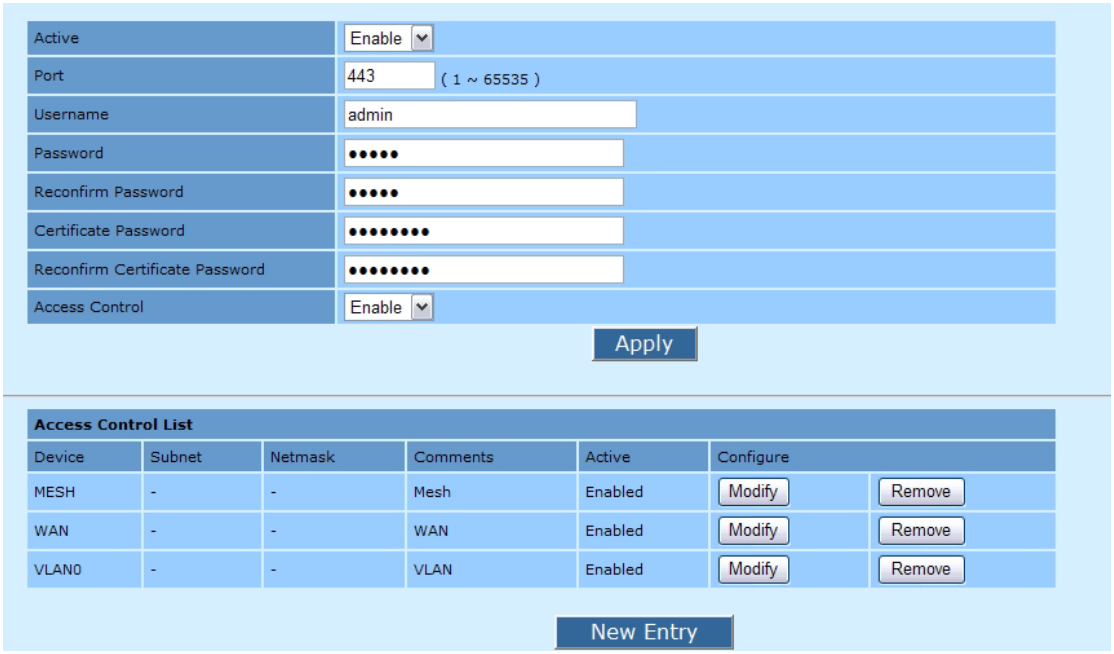


Figure 3.5.1.1: HTTPD server configuration page

To configure HTTPD server:

- Click on **"Active"** drop down menu to enable or disable HTTPD.
- Enter the HTTPD port number.
- Enter the HTTPD username.
- Enter the HTTPD password.
- Re-enter password to confirm it.
- Enter the certificate password.
- Re-enter certificate password to confirm it.
- Click on **"Access Control"** drop down menu to enable or disable access control.
- Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.

- From **“Configure”** field, you can select **“Modify”** or **“Remove”** HTTPD.
- Add new HTTPD Access control page is as shown in Figure 3.5.1.2.

Figure 3.5.1.2: HTTPD Access Control – add page

HTTPD Access Control page contains the following parameters:

a. **Device** – Click on **“Device”** drop down menu to select device. For example WAN, MESH, VLAN0……

b. **Using** – Click on **“Using”** drop down menu to select using “Device” or “Network”.

c. **Comments** – Enter comments for this entry.

d. **Active** – Click on **“Active”** drop down menu to enable or disable this entry.

e. **“Apply”** button – Click on **“Apply”** button to confirm add new HTTPD. New settings are active after the device reboot.

f. If you select to edit existing HTTPD, a page similar to Figure 3.5.1.2 with configured settings will be displayed.

3.5.2 Management > Configuration

Under this configuration menu, you can perform the following action. Configuration page is shown in Figure 3.5.2.1.

Figure 3.5.2.1: Configuration page

To use Configuration:

a. Click on Restore Factory Settings **"Default"** button to restore factory default settings.

b. Click on Backup configuration settings **"Backup"** button to save configuration settings file (config.cfg).

c. Click on Restore configuration **"Browse…"** button to browse and select configuration file (config.cfg) to restore. After selected configuration file, click on Restore configuration **"Upload"** button to upload this file.

d. Click on Upload New Webserver Certificate **"Browse…"** button to browse and select certificate file (*.pem). Then, click on Upload New Webserver Certificate **"Upload"** button to upload this file.

e. Click on IPSEC Management **"Manage RSA"** button, IPSEC Management – RSA page will display as shown in Figure 3.5.2.2.

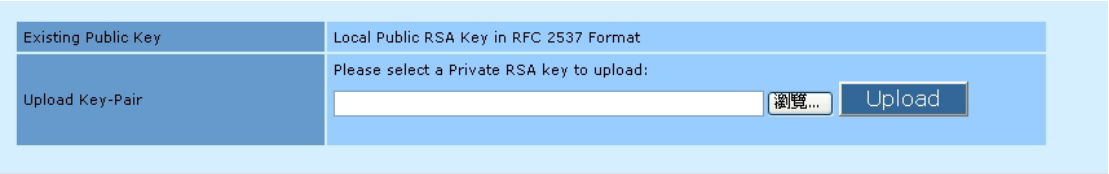


Figure 3.5.2.2: IPSEC Management – RSA page (MAP-3100 only)

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.

f. Click on IPSEC Management **"Manage x509"** button, IPSEC Management – x509 page will display as shown in Figure 3.5.2.3.

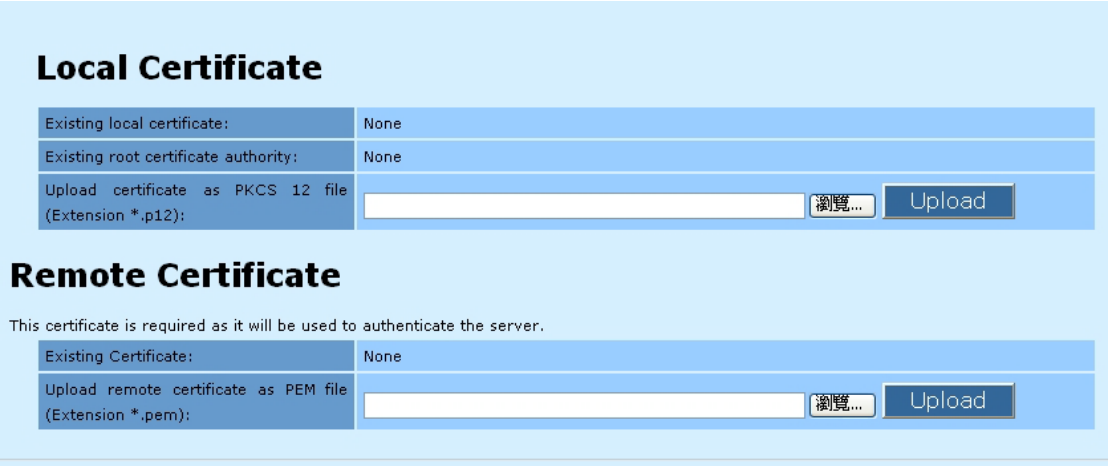


Figure 3.5.2.3: IPSEC Management – x509 page (MAP-3100 only)

IPSEC Management – x509 page contain the following parameter:

g. **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.

h. **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.

3.5.3 Management > SNMPD

Simple Network Management Protocol (SNMP) used to monitor devices for conditions that warrant administrative attention. SNMP configuration page is shown in Figure 3.5.3.1.

Figure 3.5.3.1: SNMP configuration page

To configure SNMP:

- Click on **"Active"** drop down menu to enable or disable SNMP management.
- Click on **"Version"** drop down menu to select "v1 or v2c", "v3", or "all" SNMP version.
- Enter the SNMP port number.
- Enter the v2 Read Community" public " .
- Re-enter v2 Read Community to confirm it.
- Enter the v2 Read-write Community" private " .
- Re-enter v2 Read-write Community to confirm it.
- Enter the v3 Read Username " snmpv3rouser ".

- Enter the v3 Read-write Username" snmpv3rwuser ".
- Enter the v3 Password" snmpv3password ".
- Re-enter v3 Password to confirm it.
- Enter the v3 Passphrase" snmpv3passphrase ".
- Re-enter v3 Passphrase to confirm it" snmpv3passphrase ".
- Click on **"Access control"** drop down menu to enable or disable access control.
- Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.
- From **"Configure"** field, you can select **"Modify"** or **"Remove"** SNMP.
- If you select to add new SNMP entry, SNMP Access Control – add page will display as shown in Figure 3.5.3.2.

Figure 3.5.3.2: SNMP Access Control – add page

SNMP Access Control – add page contain the following parameter:

a. **Device** - Click on **"Device"** drop down menu to select device. For example, WAN, MESH, VLAN0……

b. **Using** - Click on **"Using"** drop down menu to select "Device" or "Network".

c. **Comments** - Enter comments for this entry.

d. **Active** - Click on **"Active"** drop down menu to enable or disable this entry.

e. **"Apply"** button - Click on **"Apply"** button to confirm add new SNMP. New settings are active after the device reboot.

i. If you select to edit existing SNMP, a page similar to Figure 3.5.3.2 with configured settings will be displayed.

3.5.4 Management > Firmware

On firmware upgrade management page, 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. Firmware Upgrade page is shown in Figure 3.5.4.1.

Figure 3.5.4.1: Firmware Upgrade page

To use Firmware Upgrade:

- 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.

3.5.5 Management > Trap

Trap used to report an alert or other asynchronous event about managed system. Trap configuration page is shown in Figure 3.5.5.1.

Figure 3.5.5.1: Trap configuration page

To configure Trap:

a. Click on **"Active"** drop down menu to enable or disable Trap.

b. Click on **"Configuration"** drop down menu to enable or disable configuration.

c. Click on **"Security"** drop down menu to enable or disable security.

d. Click on **"Wireless"** drop down menu to enable or disable wireless.

e. Click on **"Operational"** drop down menu to enable or disable operational.

f. Click on **"Flash"** drop down menu to enable or disable flash.

g. Click on **"Tftp"** drop down menu to enable or disable Tftp.

h. Click on **"Image"** drop down menu to enable or disable image.

i. Click on **"Auth failure"** drop down menu to enable or disable authentication failure.

j. Click on top **"Apply"** button if you have made any changes. New settings are active after the device reboot.

k. From **"Configure"** field, you can select **"Modify"** or **"Remove"** Trap

l. If you select to add new Trap, Trap server – add page will display as shown in Figure 3.5.5.2.

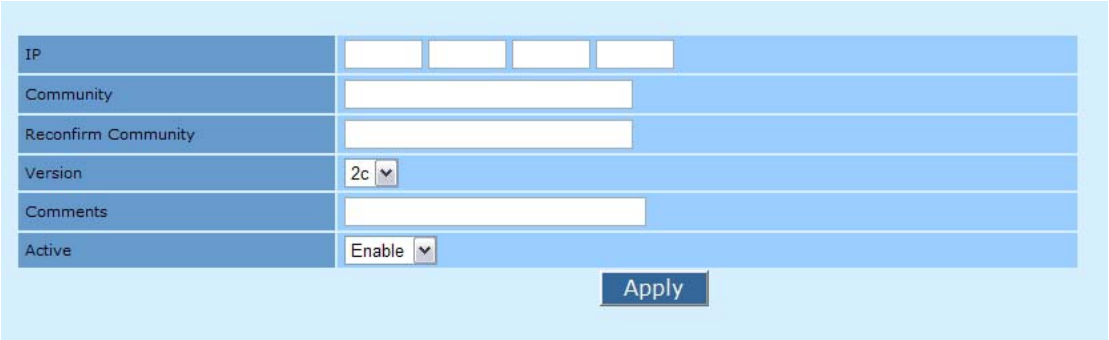


Figure 3.5.5.2: Trap server – add page

Trap server – add page contain the following parameter:

a. **IP** – Enter destination IP to send trap.

b. **Community** – Enter community of trap.

c. **Reconfirm Community** – Re-enter community to confirm it.

d. **Version** – SNMP Version

e. **Comments** – Enter Trap comments.

f. **Active** – Click on **"Active"** drop down menu to enable or disable this entry.

g. **"Apply"** button –Click on **"Apply"** button to confirm add new Trap. New settings are active after the device reboot.

m. If you select to edit existing Trap server, a page similar to Figure 3.5.5.2 with configured settings will be displayed.

3.5.6 Management > User Group (MAP-3100 only)

Figure 3.5.6.1: User group page

User group page pre-defines user bandwidth profiles.

Upload Speed Limit	upload speed limit. Default: 256 kbps.
Download Speed Limit	download speed limit. Default: 256 kbps.
Idle Timeout	idle timeout. Default: 300 seconds.
Session Timeout	session timeout. Default: 65000 seconds.
Redirect to URL	Redirect to URL after login success. Default: Empty.

3.5.7 Management > Database (MAP-3100 only)

Database contains list of local users that are currently configured to the database. Database - Users page is shown in Figure 3.5.7.1.

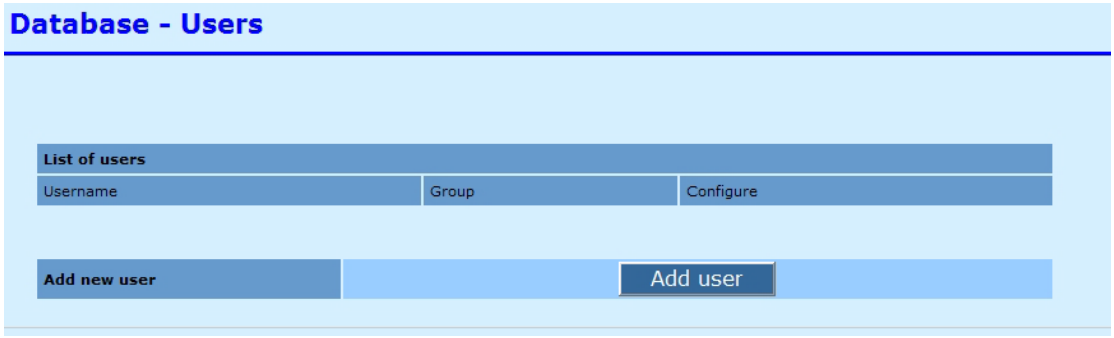


Figure 3.5.7.1: Database - Users page

To configure Database – Users:

a. User name display list of users.

b. Click on **"Remove"** button to delete user.

c. Click on **"Modify"** to edit user data.

d. Click on Add new user **"Add user"** button to add new device user. Database - Add Users page will display as shown in Figure 3.5.7.2.

Figure 3.5.7.2: Database – Add Users page

3.5.8 Management > Webspace (MAP-3100 only)

PLANET Mesh AP's Captive portal is capable to store local web content. Webspace management is used to manage local web content.

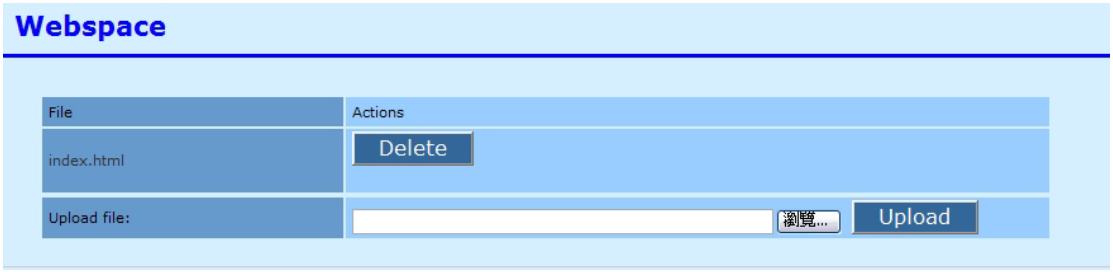


Figure 3.5.8.1: Management –Webspace management

Webspace management page is used to

- lists existing files stored in the device
- delete existing files
- upload new files

3.5.9 Management > Customize Login (MAP-3100 only)

Customize login page is used to modify look and feel for the captive portal login page of PLANET Mesh AP.

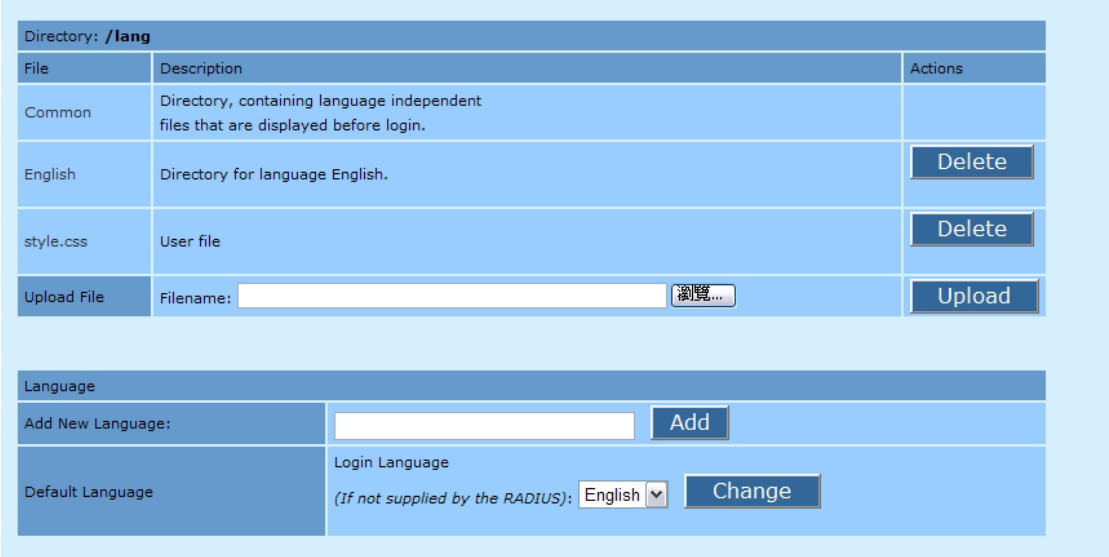


Figure 3.5.9.1: Management –Customize Login

Webspace management page is used to

- lists existing files stored in the device
- delete existing files
- upload new files
- add new language tamplate

3.5.10 Management > NMS Addresses

NMS address is used for the system to report back to Network Management System located outside of the network. Figure 3.5.10.1 shows the list of active NMS server address.

Figure 3.5.10.1 NMS Address List

To configure the NMS address:-

- Select action of “Modify” or “New Entry” to call out the details configuration as shown in figure 3.5.10.2.

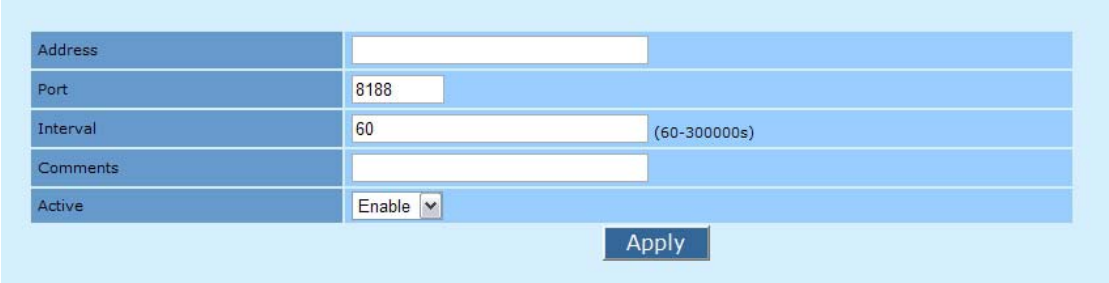


Figure 3.5.10.2 NMS address parameter page.

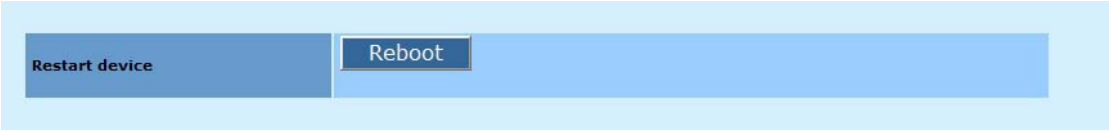
- **Address –** specify the IP address of the NMS server
- **Port –** specify the port of the NMS server which is waiting for the report
- **Interval –** specify the interval of report to NMS server
- **Comments –** additional comments for the entry
- **Active –** Enable or Disable this entry.
- Press “**Save changes**“ to save the configuration
- Reboot to enable new settings

Note

1. At Layer 2 mode, the NMS Server IP address is required. Otherwise, the NMS server can never poll the device information once this Mesh node existed in the network.
2. At Layer 3 mode, the NMS Server IP address is not required. However, to make the management more secured, we would suggest to key in at least one manger’s IP address for secured access.

3.5.11 Management > Reboot

You can perform system reboot from this page.



3.6 Tools

3.6.1 Tools > Ping

Ping page is shown in Figure 3.6.1.1.

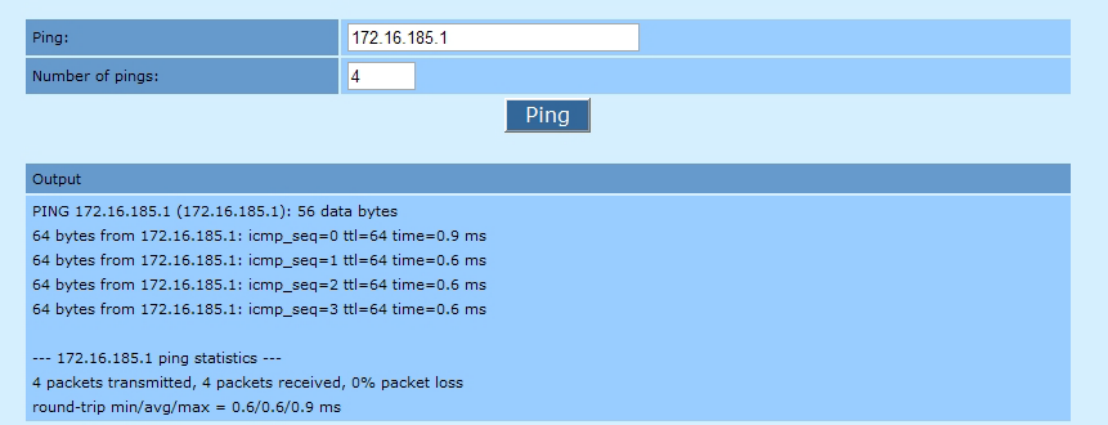


Figure 3.6.1.1: Ping page

To use Ping:

a. Enter the IP address to Ping.

b. Enter the number of pings to send.

c. Click on **"Ping"** button to display output of Ping command.

3.6.2 Tools > TFTP

TFTP page is shown in Figure 3.6.2.1.

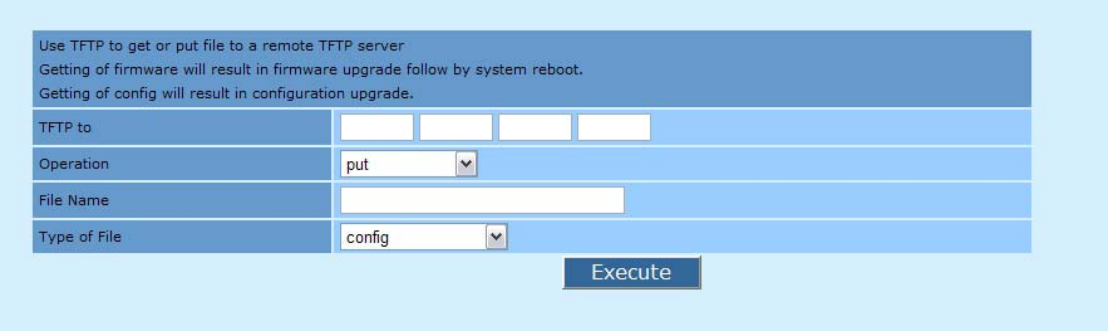


Figure 3.6.2.1: TFTP page

To use TFTP:

a. Enter the destination IP address of remote TFTP server.

b. Click on **"Operation"** drop down menu to select "put", "get" or "get and reboot" file to remote TFTP server.

c. Enter the File Name to put or get.

d. Click on **"Type of File"** drop down menu to select "config", "firmware", "ipsec x509 local", "ipsec x509 remte", or "ipsec rsa" file.

e. Click on **"Execute"** button to confirm operation.

3.7 Status

3.7.1 Status > Status

System Status page is shown in Figure 3.7.1.1.

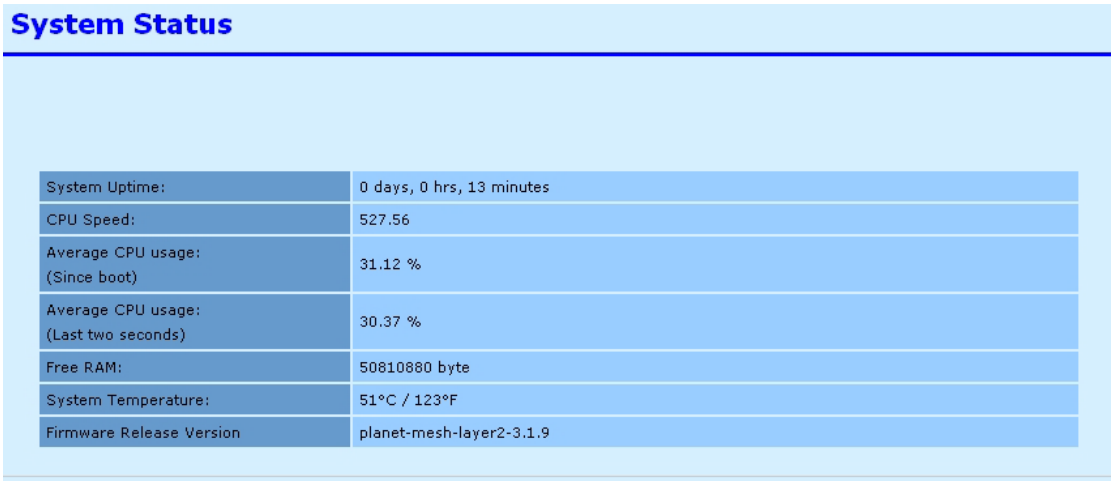


Figure 3.7.1.1: System Status page

3.7.2 Status > Interfaces

Interface page is shown in Figure 3.7.2.1.

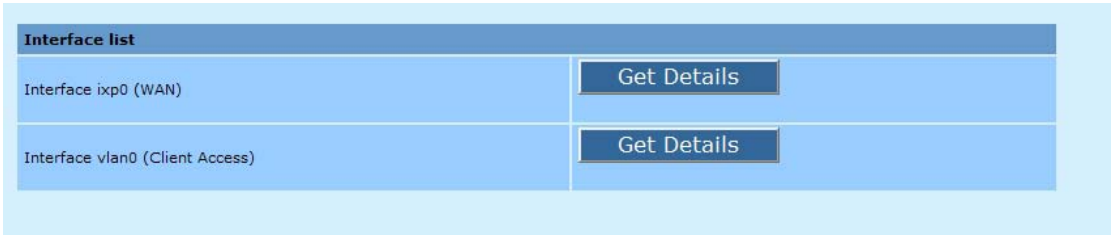
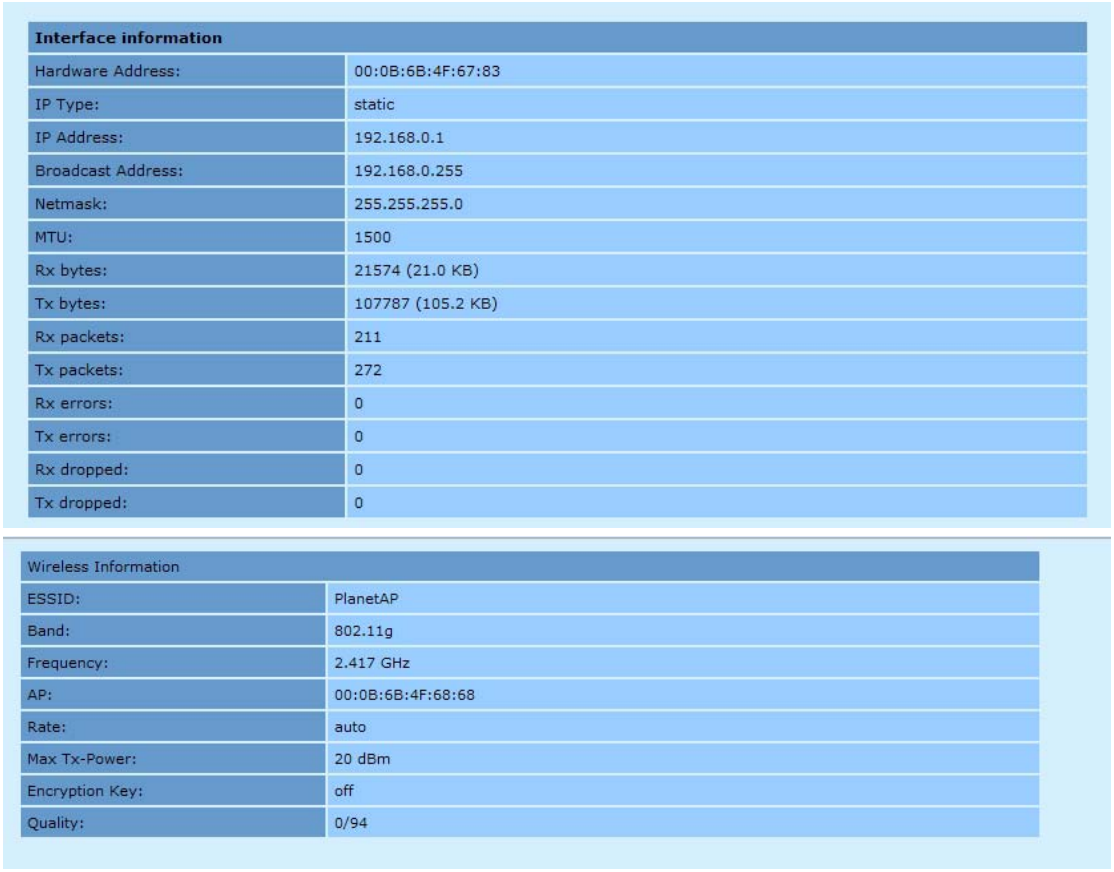


Figure 3.7.2.1: Interface page

Interface page only display activated interface. So the page content will always change depend on activated interface.

To use Interface:

a. Click on Interface MESH **"Get Details"** button to obtain Interface MESH information. The page will display as shown in Figure 3.7.2.2.



Interface information	
Hardware Address:	00:0B:6B:4F:67:83
IP Type:	static
IP Address:	192.168.0.1
Broadcast Address:	192.168.0.255
Netmask:	255.255.255.0
MTU:	1500
Rx bytes:	21574 (21.0 KB)
Tx bytes:	107787 (105.2 KB)
Rx packets:	211
Tx packets:	272
Rx errors:	0
Tx errors:	0
Rx dropped:	0
Tx dropped:	0

Wireless Information	
ESSID:	PlanetAP
Band:	802.11g
Frequency:	2.417 GHz
AP:	00:0B:6B:4F:68:68
Rate:	auto
Max Tx-Power:	20 dBm
Encryption Key:	off
Quality:	0/94

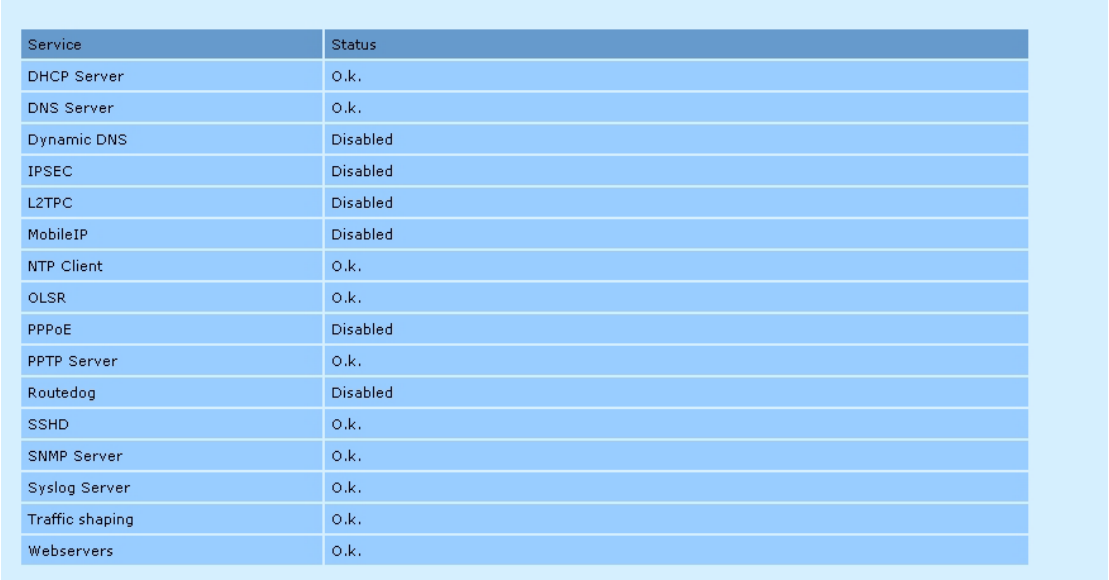
Figure 3.7.2.2: Interface ath0 (MESH) page

Interface ixp1 page contain the following parameter:

- **Hardware Address**: Display the hardware address of interface.
- **IP Type**: Display the IP type of this interface.
- **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.
- **Back**: Click on **"Back"** to return to Interface page.

3.7.3 Status > Services

Services page is shown in Figure 3.7.3.1.



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 3.7.3.1: Services page

Services page display status of each service. In layer 3 mode, Services page contain the following parameter:

- DHCP Server
- DNS Server
- Dynamic DNS
- PPPoE
- OLSR
- Routing
- NTP Client
- Traffic shaping
- PPTP Server
- Remote Syslog
- SNMP Server
- Webbased Configuration
- Webservers

In layer 2 mode, Services page contain the following parameter:

- Dynamic DNS
- NTP Client
- SSHD
- SNMP Server
- Syslog Server
- Webservers

3.7.4 Tools > Ifconfig

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

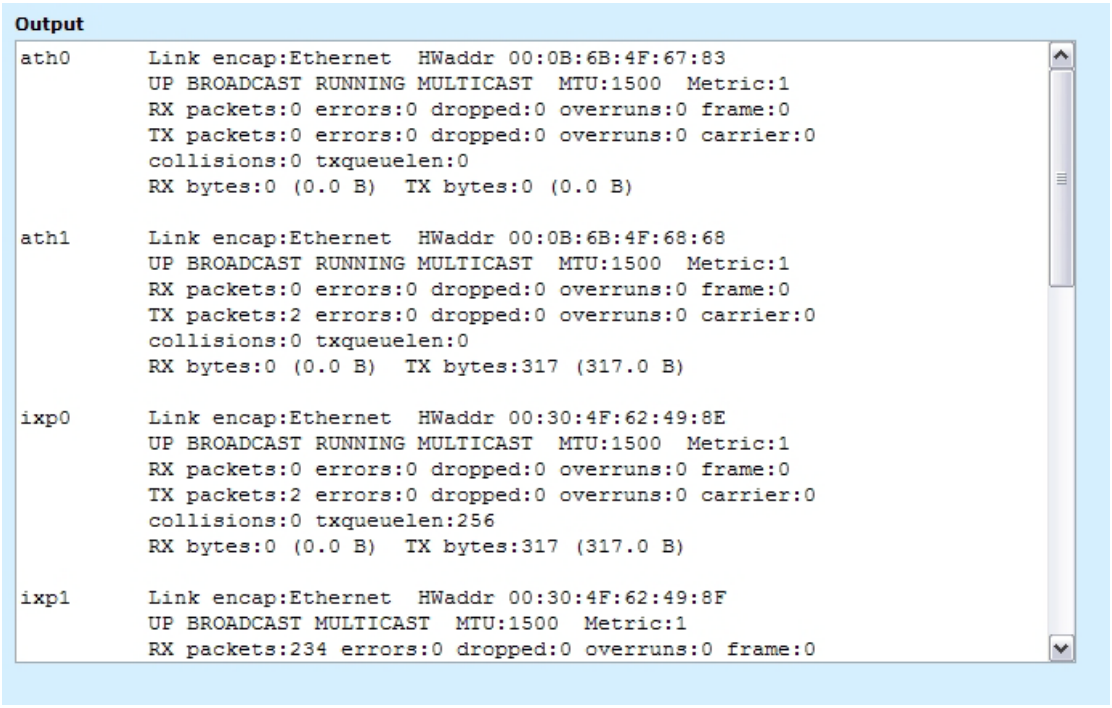


Figure 3.7.4.1: Ifconfig page

To use Ifconfig:

a. Click on **"Ifconfig"** button to display output of ifconfig command.

3.7.5 Tools > Route

Route page is used to collect information about device's routing table.

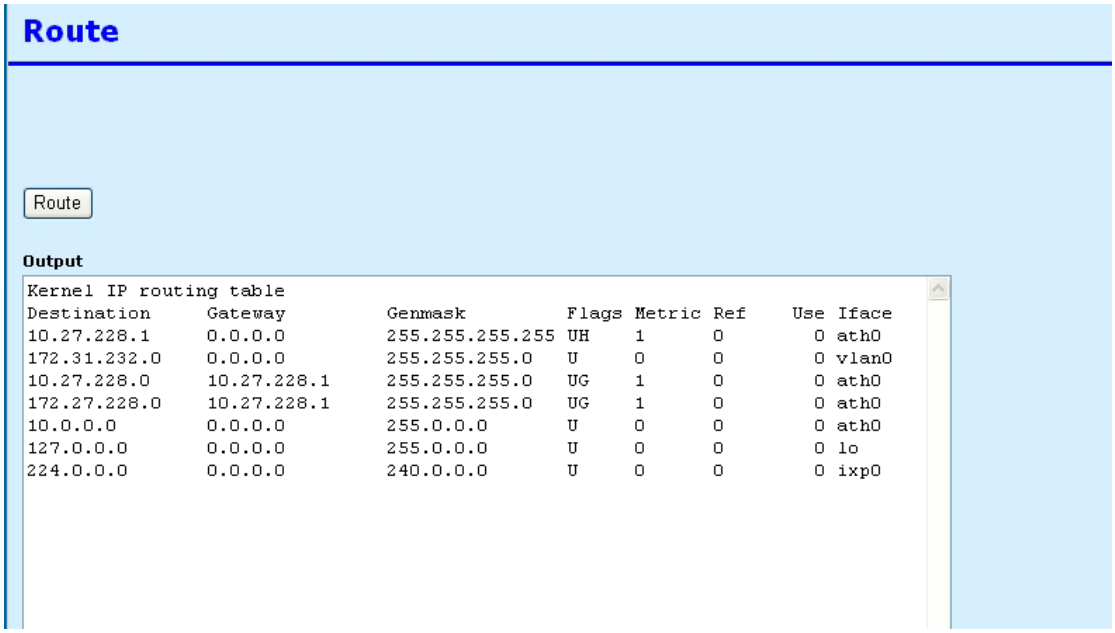


Figure 3.7.5.1: Route page

To use Route:

a. Click on **"Route"** button to display output of route command.

3.7.6 Status > Users (MAP-3100 only)

Figure 3.7.6.1: Users –Online Database page

This page displays list of logged in users.

3.7.7 Status > System Log

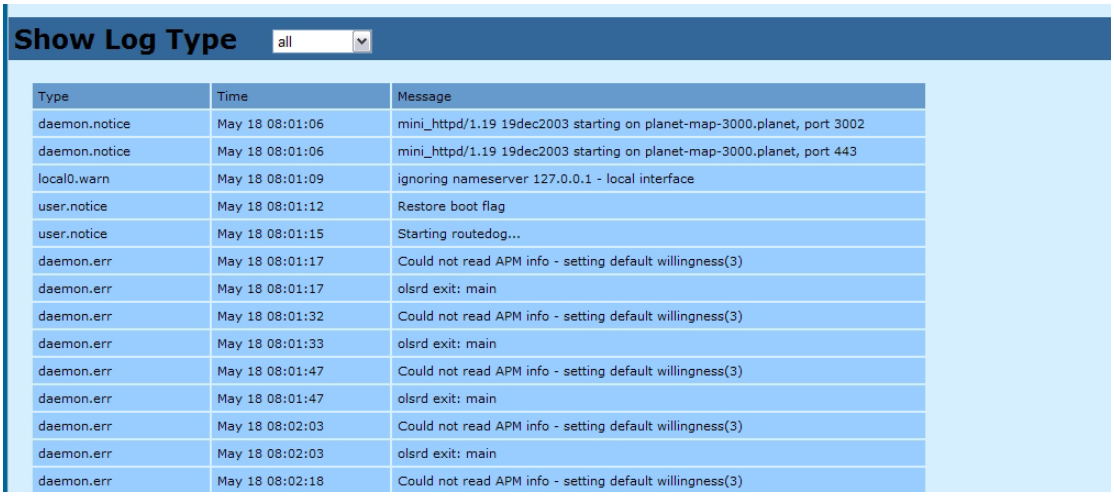


Figure 3.7.7.1: System Log page

To use System Log:

a. Click on **"Get log"** button to display output of system log command.

3.7.8 Status > Topology (MAP-3100 only)

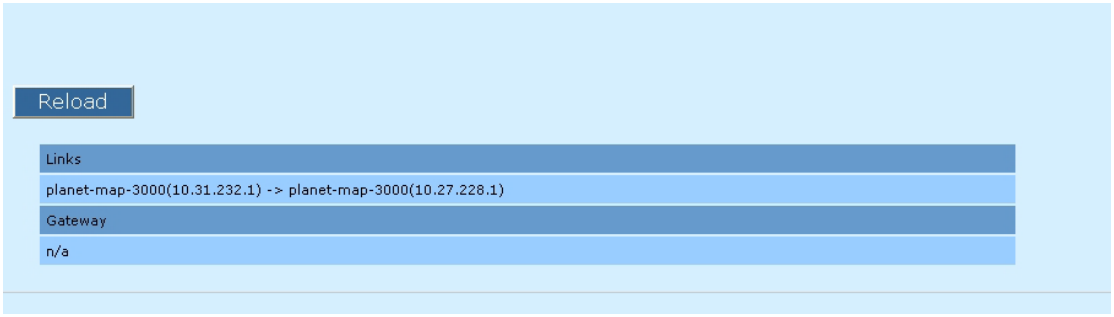


Figure 3.7.8.1: Simple Topology page

To view Topology:

- Click on **"Reload"** button to reload output content of topology command.

3.7.9 Status > Mobile IP (MAP-3100 only)

Figure 3.7.9.1 Mobile IP Status

3.7.10 Status > Neighbor

Neighbor status page will show the mesh node status as in figure 3.7.10.1. It show neighbor with details such as Rate, RSSI, timeout. A click on the "**view"** under the Mac Table column will bring out the details of the specific node. The client's MAC address that's behind the node. The Mac Table page is shown in figure 3.7.10.2.

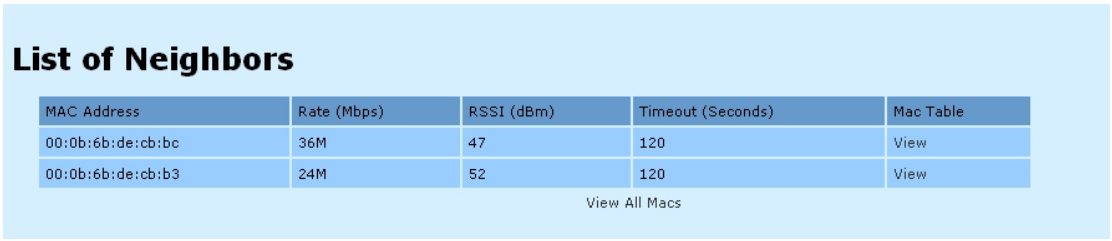


Figure 3.7.10.1 Neighbor Status page

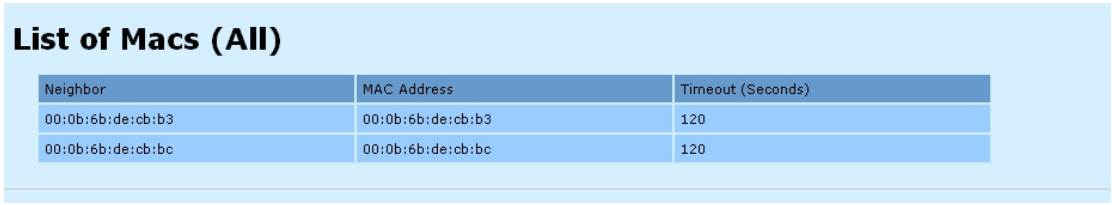


Figure 3.7.10.2 MAC table of the specific nodes.

4 Technical Support

For Technical Support and other related feedback and information request, kindly please send your request to the following email:

Email: support_wireless@planet.com.tw

In your email, please provide the following detail information:

Device Model No :

Distributor :

Date of Purchase :

Device MAC Address :

Brief Description of your Problem or Request :

Capture of Sys Log Info :

Contact Info

Name :

Company :

Email :

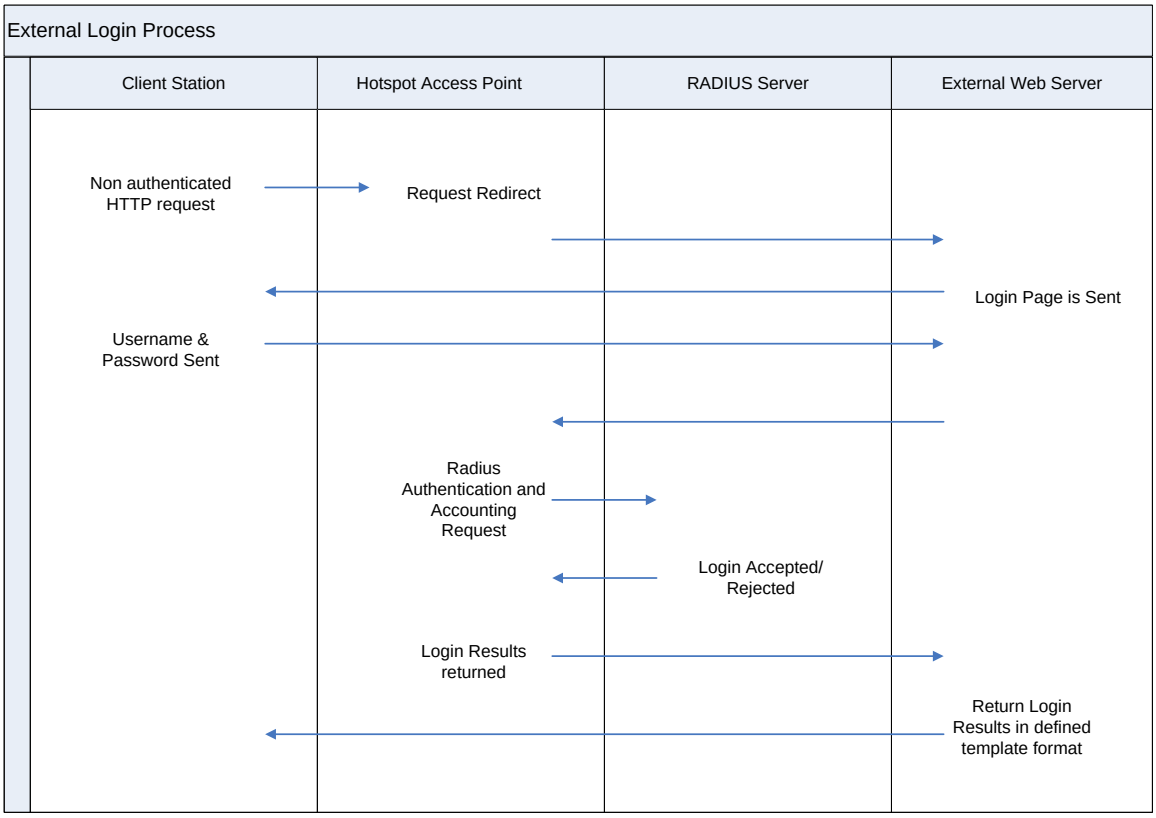
Appendix A Using the External Login Server

MESH AP provides an option that allows administrator to redirect users to a remote server to log in to the public access interface instead of using the internal login page.

The advantages of using the external login server are listed as follow:

- The login page is completely customizable and centralized located at the web server.
- Users can login to the public access interface without exposing their web browsers to the SSL certificate on the MESH AP. Warning messages caused by having an SSL certificate on the MESH AP that is not signed by a well-known certificate authority is eliminated.
- Only a single SSL certificate signed by a well-known certificate authority is required for the remote web server. There is no need to obtain the SSL certificate for every MESH AP.

External Login could be used, for example to deploy a centralized login portal. Following diagram shows the sequence of the login process when a client start access internet using MESH AP Access Point.



A-1 Configuring the MESH AP

Login to the access point configurations, under Login Setup->User Login Parameters, enter the External Login URL (e.g. https://www.server.com/Login.php?client=##CLIENT_IP##).

There are several macros available in order to retrieve information from the access point.

Macro	Description
##CLIENT_IP##	The IP address of the login client
##REQUESTED_URL##	Original URL on which the client is requesting.
##GATEWAY_LOGIN##	The Access Point's external login gateway. (https://<accesspoint-domain>:<https_port>/X_Login.cgi) Where <accesspoint-domain> is the Common Name (CN) found in the Webserver Certificates. <https_port> is the configured Secure login port
##EXT_IP##	Return the WAN IP address of the access point
##NAS_ID##	Return the NAS Identifier of the access point
##DOMAIN##	Return the hostname (CN in the certificates)
##PORT_HTTPS##	Return the secure login port of the access point

Table – Defined Macros in the external login URL

Note that, the external server hostname must be able to resolve by the Access Point for proper Access Control Setup. (This could be verified using the Tools->Ping page in the web based configurations page).

Access Control to the external server is automatically done during startup or after configured the new server address. Thus, **if** the external server is using dynamic IP address, the Access Control will become invalid after the address has changed.

A-2 Gateway Login URL

This is the gateway between the external server and the access point's radius client. External server will have to send back the

- USERNAME,
- PASSWORD,
- CLIENT_IP

information to the access point. All information should be encoded according to the RFC 1738 specification. E.g. for the username 'Donald Duck', the POST should contain USERNAME=Donald%20Duck.

A-3 Gateway Logout URL

External server could, forcing a logged-in station to logout using the logout URL.
https://<accesspoint-domain>:<https_port>/X_Logout.cgi?CLIENT_IP=<client ip address>

A-4 Login Reply

After processing the authentication request, the Access Point will reply the External Server with the following contents:

A-5 Login Success

```
<HTML>
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmeWisp.com/WISPAccessGatewayParam.
xsd">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>50</ResponseCode>
<ReplyMessage>" radius reply message"</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
<!--
<LOGIN>SUCCESS</LOGIN>
<REQUESTED_URL>Original Requested URL </REQUESTED_URL>
<SERVER_NAME>Access Point Hostname </SERVER_NAME>
<INTERNAL_WEBSPACE_URL>Access Point Internal Webspace URL
</INTERNAL_WEBSPACE_URL>
<USER_STATUS_URL>Access Point Internal url to check user status
</USER_STATUS_URL>
<USER_IP>client IP address </USER_IP>
<USER_MAC>client machine MAC address </USER_MAC>
<USER_LOGINNAME>login name </USER_LOGINNAME>
<USER_AUTH_MODE>authentication mode </USER_AUTH_MODE>
<USER_AUTH_MSG>radius reply message </USER_AUTH_MSG>
<USER_IDLE_TIMEOUT>user idle timeout </USER_IDLE_TIMEOUT>
<USER_SESSION_TIMEOUT>user session timeout</USER_SESSION_TIMEOUT>
<USER_CUSTOM>radius custom reply attributes</USER_CUSTOM>
<LOGIN_DNS_KEYWORDS>dns shortcut to the access point logout
url</LOGIN_DNS_KEYWORDS>
-->
<body>LOGIN SUCCESS</body>
</html>
```

A-6 Already Logged In

```
<HTML>
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmeWisp.com/WISPAccessGatewayParam.
xsd">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>100</ResponseCode>
<ReplyMessage>" radius reply message"</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
<!--
<LOGIN>ERROR</LOGIN>
<USER_STATUS_URL>Access Point Internal url to check user status
</USER_STATUS_URL>
<USER_IP>client IP address </USER_IP>
<USER_MAC>client machine MAC address </USER_MAC>
<USER_LOGINNAME>login name </USER_LOGINNAME>
<USER_AUTH_MODE>authentication mode </USER_AUTH_MODE>
<USER_AUTH_MSG>radius reply message </USER_AUTH_MSG>
<USER_IDLE_TIMEOUT>user idle timeout </USER_IDLE_TIMEOUT>
<USER_SESSION_TIMEOUT>user session timeout</USER_SESSION_TIMEOUT>
<USER_CUSTOM>radius custom reply attributes</USER_CUSTOM>
<LOGIN_DNS_KEYWORDS>dns shortcut to the access point logout
url</LOGIN_DNS_KEYWORDS>
-->
<body>ALREADY LOGGED IN</body>
</html>
```

A-7 Login Denied

```
<HTML>
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmeWisp.com/WISPAccessGatewayParam.
xsd">
<AuthenticationReply>
```

```
<MessageType>120</MessageType>
<ResponseCode>100</ResponseCode>
<ReplyMessage>“ radius reply message”</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
<!--
<LOGIN>ERROR</LOGIN>
<REQUESTED_URL> Original Requested URL </REQUESTED_URL>
<SERVER_NAME> Access Point Hostname </SERVER_NAME>
<USER_LOGINNAME> login name </USER_LOGINNAME>
<USER_AUTH_MSG> radius reply message </USER_AUTH_MSG>
-->
<body>LOGIN DENIED</body>

</html>
```

A-8 Certificates and hostname

The Access Point will use the subject CN field in the installed certificates as its default hostname (provided the CN field contains a valid hostname, only [.-a-zA-Z] character is allowed).

AP returns the hostname as GATEWAY_LOGIN URL by default. External server could use the ##EXT_IP## or using the REMOTE_ADDR variable from the HTTP server, to obtain the AP IP address, if the hostname is not a known to the server.