

802.11a/b/g MESH Outdoor Router



User's Manual

Version: 1.0

Table of Contents

1	INTRODUCTION	5
1.1	FEATURES & BENEFITS	5
1.2	PACKAGE CONTENTS	6
1.3	SAFETY GUIDELINES	6
1.4	MESH ROUTER DESCRIPTION	7
1.5	SYSTEM REQUIREMENTS	7
1.6	APPLICATIONS	7
1.7	NETWORK CONFIGURATION.....	8
2	UNDERSTANDING THE HARDWARE	10
2.1	HARDWARE INSTALLATION	10
2.2	MAST / WALL MOUNTING	10
3	WEB CONFIGURATION	11
3.1	LOGGING IN.....	11
3.2	SYSTEM	13
3.2.1	SYSTEM DESCRIPTION & OPERATION MODE	13
3.2.2	AUTO IP – WLAN1 & VLAN	14
3.2.3	ZERO CONFIG	15
3.2.4	ADVANCE	15
3.2.5	SYSTEM BACKUP	17
3.2.6	RESTORE TO FACTORY DEFAULTS	17
3.2.7	RESTORE CONFIGURATION FROM A FILE	18
3.2.8	REBOOT THE MESH ROUTER	18
3.3	NETWORK	19
3.3.1	WLAN CONFIGURATION 1	19
3.3.2	DHCP SERVER	22
3.3.3	WAN SETTINGS	23
3.3.3.1	STATIC IP ADDRESS CONFIGURATION	23
3.3.3.2	DHCP CONNECTION (DYNAMIC IP ADDRESS).....	24
3.3.3.3	PPPoE (POINT-TO-POINT PROTOCOL OVER ETHERNET)	24
3.3.3.4	VLAN TAGGING	25
3.3.3.5	DNS, DOMAIN, AND DEFAULT GATEWAY	27
3.3.3.6	DDNS (DYNAMIC DNS)	27
3.3.4	NAT (NETWORK ADDRESS TRANSLATION).....	28
3.3.5	FIREWALL.....	29
3.3.6	NTP (NETWORK TIMING PROTOCOL)	31
3.3.7	VPN (IPSEC, L2TP).....	32
3.3.8	MESH INTERFACE IP SETTINGS.....	33
3.3.9	ROUTING (STATIC ROUTING, OLSR)	33
3.4	SECURITY	36
3.4.1	MSSID	36
3.4.2	MAC ADDRESS FILTER	38
3.4.3	VLAN.....	39
3.5	SERVICES	41
3.5.1	PPTP SERVER	41
3.5.2	MOBILE IP	42
3.5.3	TRAFFIC SHAPING	43
3.5.4	ROUTE WATCHDOG	43
3.5.5	SYSTEM WATCHDOG.....	44
3.5.6	SSH (SECURE SHELL DAEMON)	44
3.6	QOS	45

Table of Contents

3.6.1	QOS TABLE	45
3.6.2	WMM (WIRELESS MULTIMEDIA)	46
3.7	SYSTEM MANAGEMENT	48
3.7.1	HTTPD	48
3.7.2	SNMP	49
3.7.3	SYSLOG SERVER.....	51
3.7.4	FIRMWARE UPGRADE.....	51
3.7.5	SNMP TRAP	52
3.7.6	WEBSERVER CERTIFICATE / IPSEC MANAGEMENT (RSA, X.509).....	53
3.8	LOGIN SETUP / CAPTIVE PORTAL	55
3.8.1	LOGIN PARAMETERS	55
3.8.2	RADIUS.....	56
3.8.3	LOCAL USERS DATABASE	57
3.8.4	WEBSpace.....	58
3.8.5	CUSTOMIZE LOGIN.....	58
3.9	TOOLS	60
3.9.1	PING	60
3.9.2	IFCONFIG	61
3.9.3	ROUTE	61
3.9.4	TFTP	61
3.10	STATUS	63
3.10.1	SYSTEM STATUS	63
3.10.2	INTERFACE STATUS	64
3.10.2.1	WAN INTERFACE STATUS	64
3.10.2.2	MESH INTERFACE STATUS	64
3.10.3	SERVICES STATUS.....	65
3.10.4	USERS STATUS	66
3.10.5	MOBILE IP STATUS	66
3.10.6	TOPOLOGY STATUS	66
3.10.7	SYSTEM LOG STATUS	67
APPENDIX A – MAST MOUNTING		68
APPENDIX B – WALL MOUNTING.....		69
APPENDIX C – GLOSSARY.....		70
APPENDIX D – SPECIFICATIONS.....		82
APPENDIX E – FCC INTERFERENCE STATEMENT.....		84
APPENDIX F – INDEX		85

Revision History

Version	Date	Notes
1.0	September 23, 2007	Initial Version

1 Introduction

EnGenius Mesh Outdoor Router is designed with IEEE802.11a/b/g standards and addressed on providing high performance mesh network. The product encased in the IP-68 protection enclosure and delivers the maximum scalability, high reliability at outdoor environment. Compared with expensive T1/E1 leased lines, the Mesh network offers a cost-effective last-mile connection.

EnGenius Mesh Outdoor Router provides wireless connection over self-adaptation mesh backhaul (5GHz). The mesh AP can operate at both 2.4GHz for long range and 5GHz to reduce the frequency interference. The detachable antenna design allows users to use various antennas for different deployment.

The advanced OLSR (Optimal Link State Routing) protocol is the industry and scalable mesh routing algorithm. It allows data to be transferred with the optimal path. Included is WAN interface for Internet connection with Gateway mode; Power over Ethernet for both Gateway mode and Relay mode.

EnGenius Mesh Outdoor Router provides the highest security mechanism to protect data information over wireless. The security feature include AES backhaul link, WPA2 client access, SSL for web management. To simplify the administration task throughout the large area, this product also provides centralized management software. This software is built based on SNMP protocol and can be installed in computer.

This chapter describes the features & benefits, package contents, applications, and network configuration.

1.1 Features & Benefits

Features	Benefits
Dual Radio for independent Backhaul and local access	Allow operators to set up at both 2.4GHz for long range and 5GHz to reduce the frequency interference.
Self Configuration and Healing	Automatically search and link with gateway AP and other nearest node Mesh AP for Ease of Deployment & Management
EnGenius Business Class High Power Technology	Get more coverage and distance to save the installation fee
Lightning Protector in both antenna ports and Ethernet port	Prevent a lightning stroke to damage the internal equipments
Wide temperature range and robust mechanical design (IP68)	Delivers reliable, top performance in the most demanding environments to Avoid water invaded and weather corroded
Power over Ethernet (PoE)	Easy installation and cost-effective
Support dynamic routing (layer3)	OLSR protocol provides optimized path of routing. The routing mechanism automatically finds the optimal link once the link status is changed or broken.
Supports NAT (Network Address Translation)/NAPT	Shares single Internet account and provides a type of firewall by hiding internal IP addresses for keeping hacker out
Static Route Support	Forwarding data in a network via a fixed path in

	multi-subnet
Support Multiple SSID for client access mode	Distinguish separate networks within the same wireless space to provide secure connection
Support VLAN (Wired, Wireless)	Reduce the size of each broadcast domain, which in turn reduces network traffic and increases network security
Support 802.1x (EAP-TLS/TTLS/SIM/PEAP), 802.11i (WPA/WPA2, AES), VPN pass-thru mechanisms	Provide mutual authentication (Client and dynamic encryption keys to enhance security
Hide SSID	Avoids unallowable users sharing bandwidth, increases efficiency of the network
Support MAC Address access control list	Ensures secure network connection
Support WMM Extension	Improve the user experience for audio, video, and voice applications by prioritizing data traffic
Bandwidth control	Enables operators to specify the maximum line bandwidth that a particular transfer operation can use
Support SNMP v2c/v3	Allow users to operate with existing network management tools
Centralized management software	Easy to manage volume Mesh AP via central control system to save the management cost

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

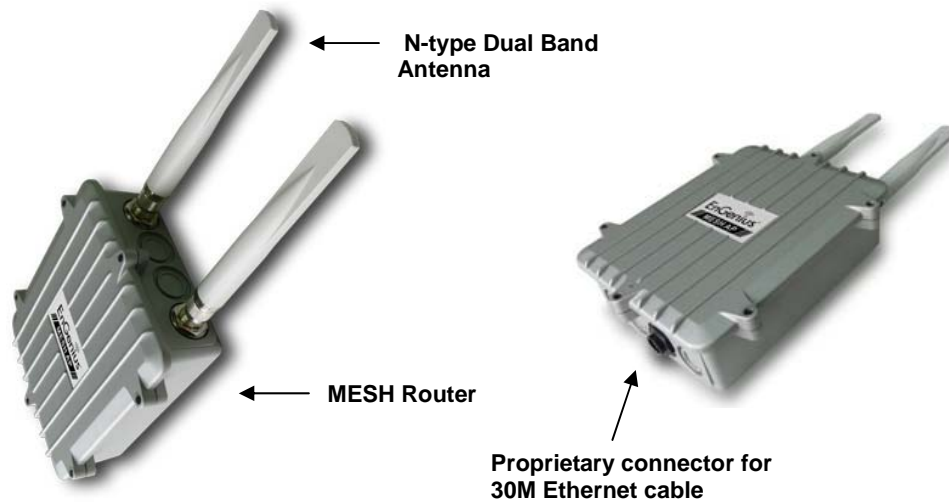
- One 30M Ethernet cable with proprietary connector
- Two N-Type dual band antennas
- One mounting kit (Wall mount and Mast mount)
- One Ground Cable
- One proprietary PoE injector
- On 48V/ 0.375A power adapter
- One CD (User's Manual and Management software)

1.3 Safety Guidelines

In order to reduce the risk of fire, electric shock and injury, please adhere to the following safety guidelines.

- Carefully follow the instructions in this manual; also follow all instruction labels on this device.
- Except for the power adapter supplied, this device should not be connected to any other adapters.
- Do not spill liquid of any kind on this device.
- Do not place the unit on an unstable stand or table. This unit may drop and become damaged.
- Do not place any heavy objects on top of this unit.
- Do not use liquid cleaners or aerosol cleaners. Use a soft dry cloth for cleaning.

1.4 MESH Router Description



1.5 System Requirements

The following are the minimum system requirements in order to configure the device.

- PC/AT compatible computer with a Ethernet / Wireless interface.
- Operating system that supports HTTP web-browser

1.6 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
- b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
- c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
- d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
- e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.
- f) **Wireless extensions to Ethernet networks**

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

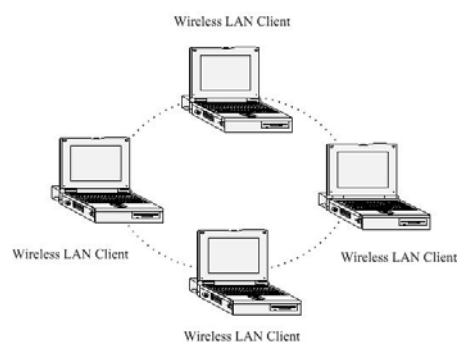
1.7 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) Infrastructure for enterprise LANs.
- c) Wi-Fi Mesh Networks

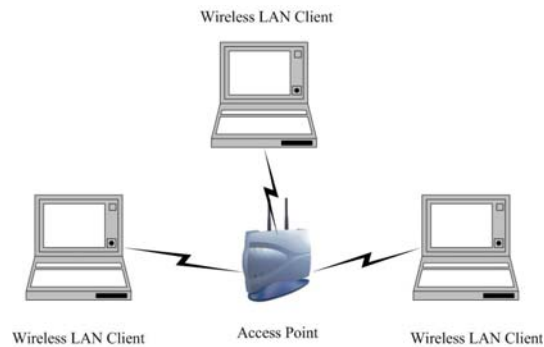
a) Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

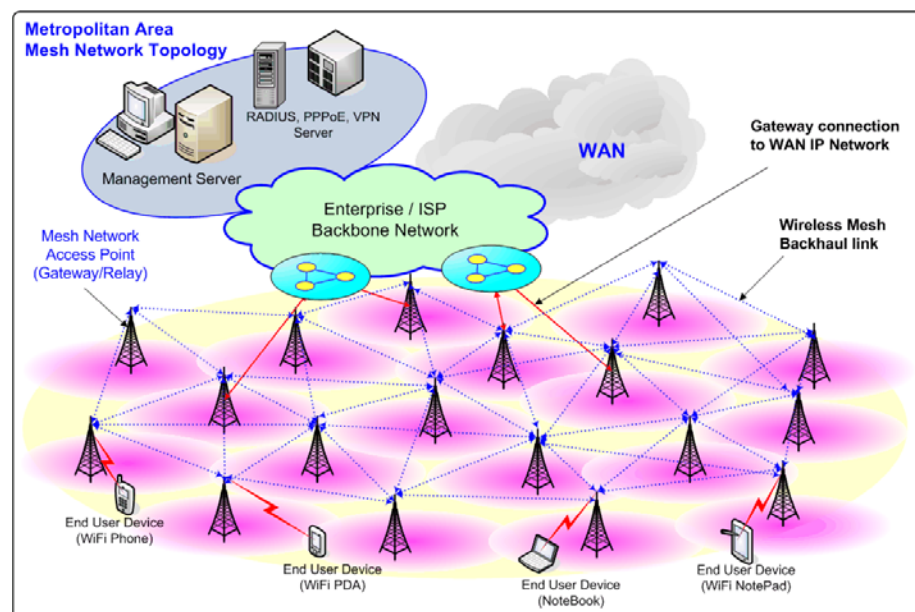
The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



c) Wi-Fi Mesh Networks

A Wireless Mesh Network constructed from WiFi Technology alleviate a number of roaming challenges from laptops, IP phones, PDAs, and IP base devices:

- **No geographical limitations** – User can take a handheld or laptop computer anywhere without losing the connection in their home
- **No physical connection required** – Mobile IP connect automatically and obtain local IP router information
- **Supports security** – Authentication is performed to ensure that rights are being protected
- **Access Anytime, Anywhere** – Network access is assured at all times and from all locations. No missed E-mails and increase productivity due to constant connectivity.
- **Emergencies** – Rapidly deployable and robust communications between each member when emergencies are involved in difficult operations inside buildings, towers, or surrounded in forest fires
- **Military Usage** – Soldiers in a battlefield are exchanging information about their position and giving and receiving orders, or the instructions

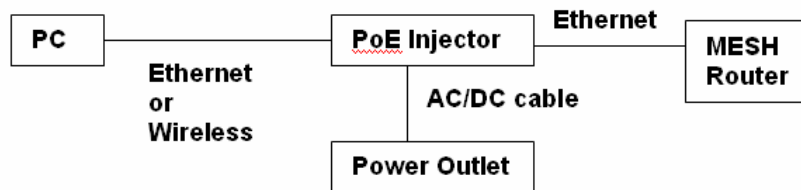


2 Understanding the Hardware

2.1 Hardware Installation

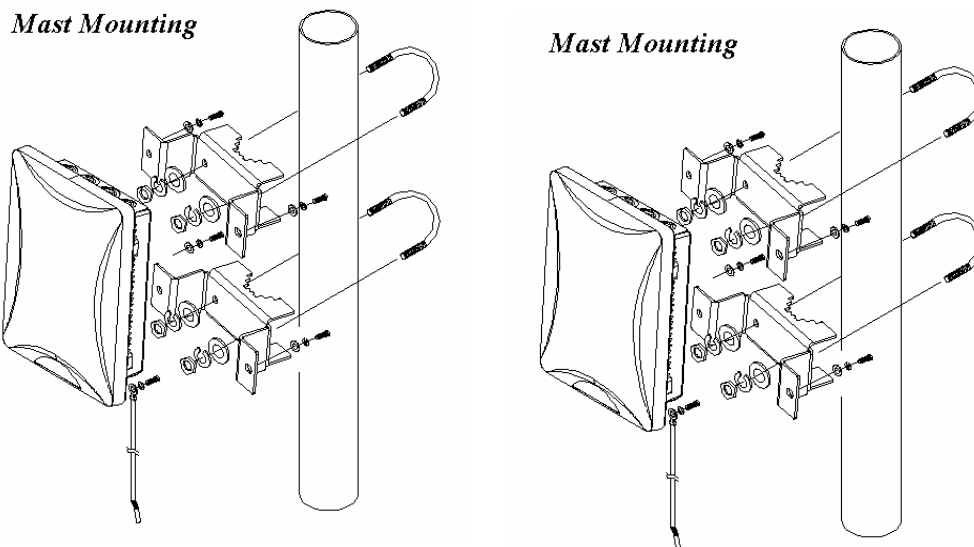
1. Tighten the two N-type Dual Band antennas onto the top of the device.
2. Plug one end of the Ethernet cable into the AP port of the PoE Injector and the other end into the Bridge/AP.
3. Place one end of another Ethernet cable into the Network port of the PoE Injector and another end into your PC/Notebook.
4. Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.
5. The DHCP server function is enabled on the device, and your PC will receive an IP address from the device. Ensure that the TCP/IP settings on your computers are configured as **Obtain IP address automatically**.
6. Place the unit in an appropriate place after conducting a site survey. Refer to the mounting instructions in the next section.

This diagram depicts the hardware configuration



2.2 Mast / Wall Mounting

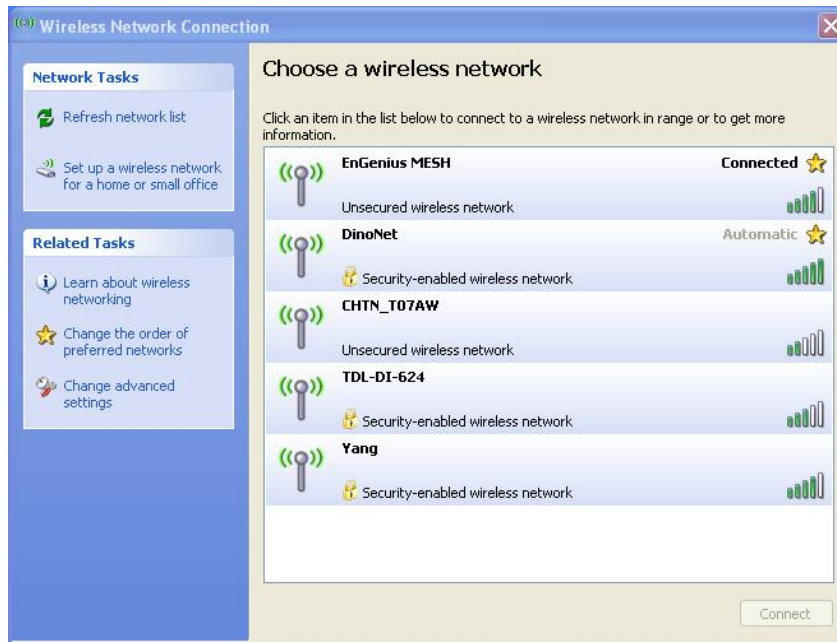
This device can be mounted on a Mast or the Wall. The mounting kit is included in the package. Refer to the image below for mounting instructions.



3 Web Configuration

3.1 Logging In

- The MESH router must be configured through the wireless interface. Associate your PC to the MESH router by selecting **EnGenius MESH** from the list. The MESH router will automatically assign an IP address to the PC.



- Once you have connected to the MESH router through the wireless interface. Check the IP address that has been assigned. In Microsoft Windows, click **Start**, **Run**, and type **cmd** in the address bar. This will launch the MS-DOS window.
- In the MS-DOS window, type **ipconfig**. This will display the IP address, subnet mask, and default gateway.
- The IP address of the default gateway is the IP address of the MESH router.

Ethernet Adapter Wireless Network Connection

Connection Specific DNS Suffix: EnGenius

IP Address: 172.20.215.254 (this is the IP address that has been assigned to the PC)

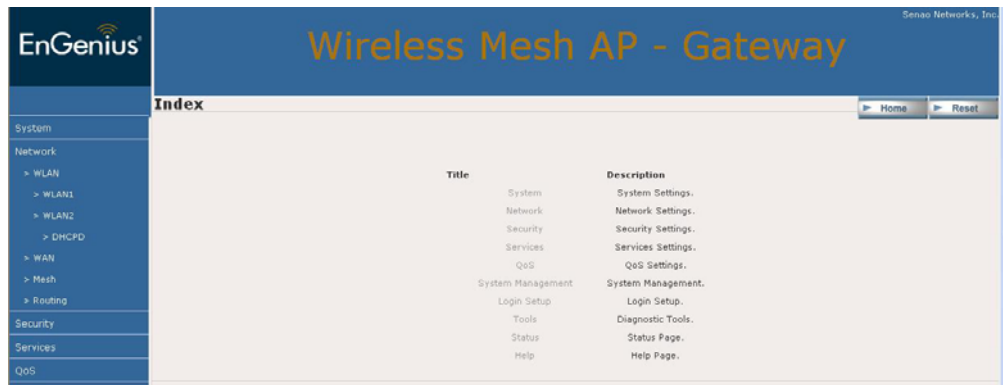
Subnet Mask: 255.255.255.0

Default Gateway: 172.20.215.1 (This is the IP address of the MESH Router)

- Launch the web-browser and specify the IP address followed by **https://**. For example, you would type <https://172.20.215.1>



- After connecting to the IP address, specify the **admin** as the User Name and **admin** as the password. Then click on the **OK** button. After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into ten main sections:
 1. **System:** This section includes the WLAN & VLAN Auto IP, Zero Config, Advanced networking/wireless, System, Backup, Restore, and Reset. Refer to section 3.2 for details.
 2. **Network:** This section includes DHCP, WAN type, NAT, Firewall, NTP, VPN, Mesh, and Routing. Refer to section 3.3 for details.
 3. **Security:** This section includes the SSID, MAC Address Filter, and VLAN. Refer to section 3.4 for details.
 4. **Services:** This section includes PPTP Server, Mobile IP, Traffic Shaping, Router Watchdog, System Watchdog, and SSHD. Refer to section 3.5 for details.
 5. **QoS:** This section includes QoS Table and WMM. Refer to section 3.6 for details.
 6. **System Management:** This section includes HTTPD, SNMP, SysLog Server, and Firmware upgrade. Refer to section 3.7 for details.
 7. **Login Setup:** This section includes Login Parameters, RADIUS, Users Database, Web-space, and Login Customization. Refer to section 3.8 for details.
 8. **Tools:** This section includes Ping, Ifconfig, Routing, and TFTP. Refer to section 3.9 for details.
 9. **Status:** This section includes System, Interfaces, Services, Users, Mobile IP, Topology, and System Log. Refer to section 3.10 for details.
 10. **Help:** Displays the help for configuring the device.



3.2 System



- Click on the **System** link on the navigation drop-down menu. This menu includes the WLAN & VLAN Auto IP, Zero Config, Advanced networking / wireless configuration, System Backup, Restore, and Reset. The configuration steps for each option are described below.

3.2.1 System Description & Operation Mode

- Click on the **System** link on the navigation drop-down menu. On this page, you may specify the description and contact information of the MESH router. You may also select the operating mode such as gateway, relay, and client relay.

Configuration saved. Please reboot to enable new settings

Name	<input type="text" value="EnGenius"/>
Location	<input type="text" value="Unknown"/>
Contact Name	<input type="text" value="Unknown"/>
Contact Email	<input type="text" value="Unknown"/>
Contact Phone	<input type="text" value="Unknown"/>
Description	<input type="text" value="EnGenius Mesh AP"/>
Object ID	1.3.6.1.4.1.14125.1
Operation Mode	<input type="button" value="Gateway"/> <ul style="list-style-type: none"> <input type="button" value="Gateway"/> <input type="button" value="Relay"/> <input type="button" value="Client-Relay"/>

[Back to top](#) | [Help?](#)

- **Name:** Specify a name for the MESH Router
- **Location:** Specify the physical or geographical location of the MESH Router.
- **Contact Name:** Specify the name of the technical administrator of the owner of the MESH Router.
- **Contact Email:** Specify the email address of the contact name.
- **Contact Phone:** Specify the phone number of the contact name.
- **Description:** Specify a description for the MESH Router.
- **Operation Mode:** Select an operation mode from the drop-down list: Gateway, Relay, or Client-Relay.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.2.2 Auto IP – WLAN1 & VLAN

- 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 saved. Please reboot to enable new settings

Active	<input type="button" value="Enable"/>
Mesh IP Prefix	<input type="text" value="10"/> .X.Y.1
VLAN0 IP Prefix	<input type="text" value="172"/> .X.Y.1

- **Active:** Choose to enable or disable this feature.
- **Mesh IP Prefix:** Assign a Mesh IP prefix. The default is 10
- **VLAN0 IP Prefix:** Assign a VLAN0 IP Prefix. The default is 172.

- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.2.3 Zero Config

- Click on the **Zero Config** link on the navigation drop-down menu. This section will allow you to configure the proxy service.

Configuration saved. Please reboot to enable new settings

Active	Enable ▼
Handle Client Proxy	Enable ▼
Proxy Login Port	8080
Handle Static IP Client	Enable ▼

- **Active:** Choose to enable or disable the service.
- **Handle Client Proxy:** Choose to enable or disable client proxy handling.
- **Proxy Login Port:** Specify the proxy login port. The default is 8080.
- **Handle Static IP Client:** Choose to enable or disable the static IP client handling service.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.2.4 Advance

- Click on the **Advance** link on the navigation drop-down menu. On this page, you may manually specify the TCP, UDP, ICMP connection settings. You may also configure the wireless distance, country settings, and channel mode.

Configuration saved. Please reboot to enable new settings

Networking-CONNTRACK

Maximum session:	<input type="text" value="212368"/>
Generic Timeout:	<input type="text" value="600"/>
ICMP Timeout:	<input type="text" value="30"/>
TCP Close Timeout:	<input type="text" value="10"/>
TCP Close Wait Timeout:	<input type="text" value="60"/>
TCP Established Timeout:	<input type="text" value="3600"/>
TCP Finished Wait Timeout:	<input type="text" value="120"/>
TCP Last ACK Timeout:	<input type="text" value="30"/>
TCP SYN Receive Timeout:	<input type="text" value="60"/>
TCP SYN Sent Timeout:	<input type="text" value="120"/>
TCP Time Wait Timeout:	<input type="text" value="120"/>
UDP Timeout:	<input type="text" value="30"/>
UDP Stream Timeout:	<input type="text" value="180"/>

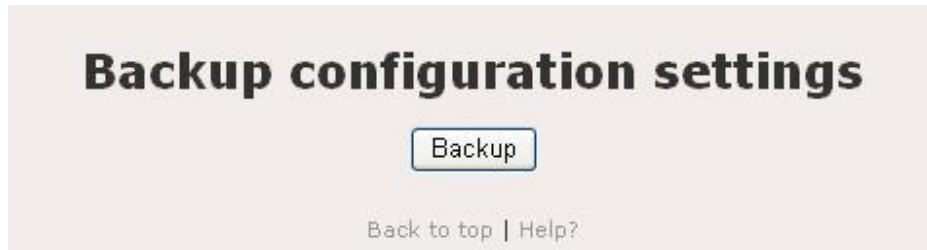
Wireless

Radio 1 distance (m)	<input type="text" value="1"/>
Radio 2 distance (m)	<input type="text" value="1"/>
Country	<input type="text" value="United Kingdom"/> ▼
Outdoor Mode	<input type="text" value="Enable"/> ▼
External Channel Mode	<input type="text" value="Enable"/> ▼

- **Maximum session:** Specify the maximum session time.
- **Generic Timeout:** Specify the generic session timeout.
- **ICMP Timeout:** Specify the ICMP timeout.
- **TCP Close Timeout:** Specify the TCP close timeout.
- **TCP Close Wait Timeout:** Specify the TCP close wait timeout.
- **TCP Established Timeout:** Specify the TCP established timeout.
- **TCP Established Wait Timeout:** Specify the TCP established wait timeout.
- **TCP Last ACK Timeout:** Specify the TCP last ACK timeout.
- **TCP SYN Receive Timeout:** Specify the TCP SYN receive timeout.
- **TCP SYN Sent Timeout:** Specify the TCP SYN sent timeout.
- **TCP Time Wait Timeout:** Specify the TCP time wait timeout.
- **UDP Timeout:** Specify the UDP timeout.
- **UDP Stream Timeout:** Specify the UDP stream timeout.
- **Radio1 distance:** Specify the radio distance in meters.
- **Radio2 distance:** Specify the radio distance in meters.
- **Country:** Select your country from the drop-down list.
- **Outdoor Mode:** Choose to enable or disable outdoor mode.
- **External Channel Mode:** Choose to enable or disable external channel mode.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.2.5 System Backup

- Click on the **Backup** link on the navigation drop-down menu. This option allows you to save the current configuration of the device into a file.



- Click on the **Backup** button to begin.
- Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



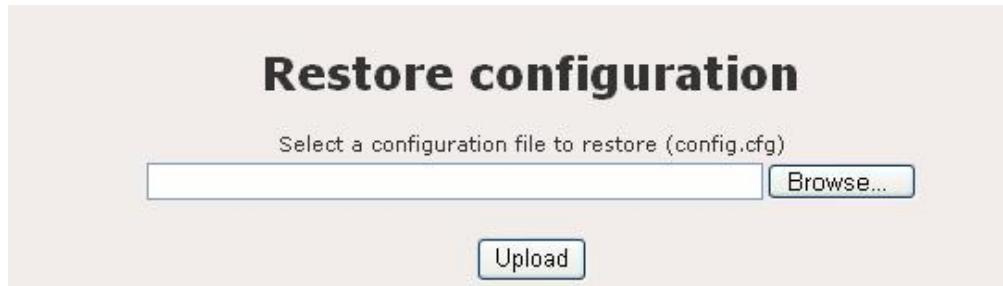
3.2.6 Restore to Factory Defaults

- Click on the **Reset** link on the navigation drop-down menu. This option allows you to restore the device back to the factory default settings. Click on the **Default** button.



3.2.7 Restore Configuration from a File

- Click on the **Restore** link on the navigation drop-down menu. This option allows you to restore the configuration from a file that is stored on a local disk.



The screenshot shows a web interface titled "Restore configuration". Below the title, there is a prompt: "Select a configuration file to restore (config.cfg)". This is followed by a text input field and a "Browse..." button. Below the input field is an "Upload" button.

- Click on the **Browse** button and select the restoration file, and then click on the **Upload** button to restore the configuration.

3.2.8 Reboot the MESH Router

- Click on the **Reboot** link on the navigation drop-down menu. This option allows you to reboot the device in order for the current settings to take effect. Click on the **Reboot** button.



The screenshot shows a web interface titled "Restart device". Below the title, there is a single "Reboot" button.

3.3 Network



- Click on the **Network** link on the navigation drop-down menu. WLAN, WAN, NAT, Firewall, NTP, VPN, MESH, and routing. The configuration steps for each option are described below.

3.3.1 WLAN Configuration 1

- Click on the **WLAN1** link on the navigation drop-down menu. This page allows you to configure the wireless mode, wireless band, SSID, frequency, fragmentation threshold, RTS threshold, beacon period, transmit power, DTIM interval data rate, antenna diversity, and security settings.

MAC address	00:02:6F:49:45:31
Mode	ADHOC
Band	802.11a
ESSID	EnGenius Backhaul
Frequency	auto
Beacon Interval	100
RTS Threshold	2346
Fragmentation Threshold	2346
DTIM interval	1
Datarate	auto
Diversity	Enable
Tx antenna	Diversity
Rx antenna	Port 1
Base Datarate Max Tx Power (dBm)	18
Current Datarate Max Tx Power (dBm)	18
Security	WEP
Encryption key	

Save changes

- **MAC:** Displays the MAC address of the wireless interface.
- **Mode:** Select a wireless mode from the drop-down list. AP, Ad-hoc STA, or WDH.
- **Band:** Select a wireless band from the drop-down list: 802.11a, 802.11b, or 802.11g.
- **ESSID:** The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters
- **Frequency:** Select a frequency/channel from the drop-down list. The channels available are based on the country's regulation. A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.
- **Beacon Period:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 1 and 65535. The default value is 2346.
- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **DTIM Interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.
- **Datarate:** Select a data rate from the drop-down list or select auto.
- **Diversity:** A method for improving the reliability of a message signal by utilizing two or more communication channels with different characteristics, in order to combat fading and interference. Click on **"Diversity"** drop down button to select **"Card Default"**, **"Enable"** or **"Disable"**.
- **Tx Antenna:** Click on **"Tx antenna"** drop down button to select **"Diversity"**, **"Card Default"**, **"Port 1"**, or **"Port 2"**.
- **Rx antenna:** Click on **"Rx antenna"** drop down button to select **"Diversity"**, **"Card Default"**, **"Port 1"**, or **"Port 2"**
- **Current Datarate max Tx power:** You may control the output power of the device by selecting a value from the drop-down list.
- **WEP Security:** You may select WEP or WPA security. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.
- **Encryption Key:** Specify the WEP encryption key.

Configuration saved. Please reboot to enable new settings

MAC address	00:02:6F:49:45:32
Mode	AP
Band	802.11g
ESSID	EnGenius MESH
Broadcast SSID	Enable
Frequency	auto
Beacon Interval	100
RTS Threshold	2346
Fragmentation Threshold	2346
DTIM interval	1
Datarate	auto
Diversity	Enable
Tx antenna	Diversity
Rx antenna	Port 2
Base Datarate Max Tx Power (dBm)	24
Current Datarate Max Tx Power (dBm)	24
Security	WPA (1 & 2)
WPA Type	AES
802.1x	True
Encryption key	

- **WPA Security:** You may select WEP or WPA security. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **WPA Type:** The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. The device negotiates the cipher type with the access point, and uses AES when available.
- **802.1x:** This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.
- **Encryption Key:** Specify the WPA encryption key.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.2 DHCP Server

- Click on the **DHCPD** link on the navigation drop-down menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP server/client. DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). In most situations, the router provides DHCP services, and you can leave this option disabled. However, if for any reason the router does not provide DHCP services, enable this option. The device's DHCP Server will then manage the IP addresses and other network configuration information for wireless clients associated with the AP. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.

Active:

DHCPD List											
Interface	Subnet	IP Start	IP End	Netmask	Max Lease	Lease	Domain	DNS	Router	Comment	Active
<input checked="" type="radio"/> vlan0	172.20.215.0	172.20.215.2	172.20.215.254	255.255.255.0	3600	1200	EnGenius	172.20.215.1	172.20.215.1	Default DHCP server	Enabled

Action:

- Select **Add** from the drop-down list in order to add a DHCP server entry.

Interface:

Subnet:

IP Start:

IP End:

Netmask:

Max Lease:

Lease:

Domain:

DNS:

Router:

Comments:

Active:

[Back to top](#) | [Help?](#)

- Interface:** Select an interface from the drop-down list.
- Subnet:** Specify the subnet of the network.
- IP Start/End:** You may limit the number of IP addresses that are distributed on the network. Specify a starting and ending range that is part of the same subnet.
- Netmask:** Specify the subnet mask for the IP address.
- Max Lease:** Specify the max lease time (minutes) for the IP address.

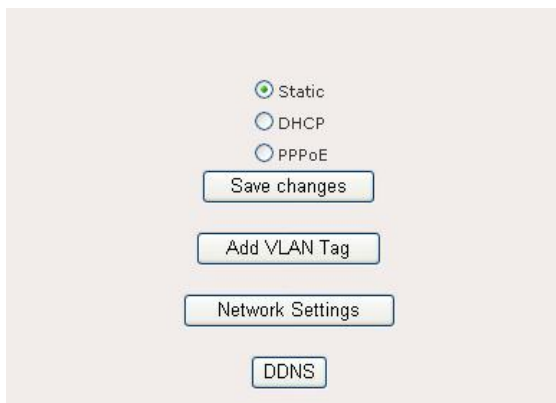
- **Lease:** Specify the number of IP addresses that can be leased.
- **DNS:** Specify the IP address of the DNS server.
- **Router:** Specify the IP address of the router or default gateway.
- **Domain Name:** Specify a domain name for this device/network.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable this entry.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- **Note:** If you change the IP address here, you may need to adjust your PC's network settings to access the network again. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.

3.3.3 WAN Settings

- The device offers several types of WAN connections in order to connect to the Internet.
 - Static IP Address
 - Dynamic IP Address (DHCP Client)
 - PPPoE
- In this section, you may also configure the VLAN tag, networking settings, and DDNS.

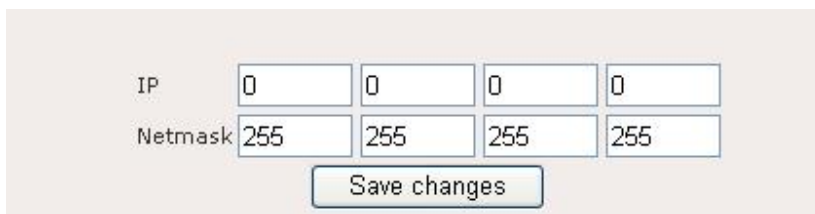
3.3.3.1 Static IP Address Configuration

- The WAN interface can be configured as Static IP address. In this type of connection, your ISP provides you with a dedicated IP address.



The screenshot shows a configuration page with three radio buttons: Static, DHCP, and PPPoE. Below the radio buttons are four buttons: Save changes, Add VLAN Tag, Network Settings, and DDNS.

- Select the **Static** radio button, and then click on the **Save Changes** button.

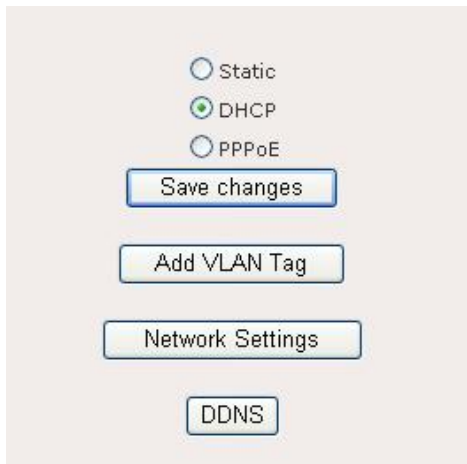


The screenshot shows two rows of input fields. The first row is labeled 'IP' and contains four boxes, each containing the number '0'. The second row is labeled 'Netmask' and contains four boxes, each containing the number '255'. Below the input fields is a button labeled 'Save changes'.

- **IP Address:** Specify the IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.3.2 DHCP Connection (Dynamic IP Address)

- The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.



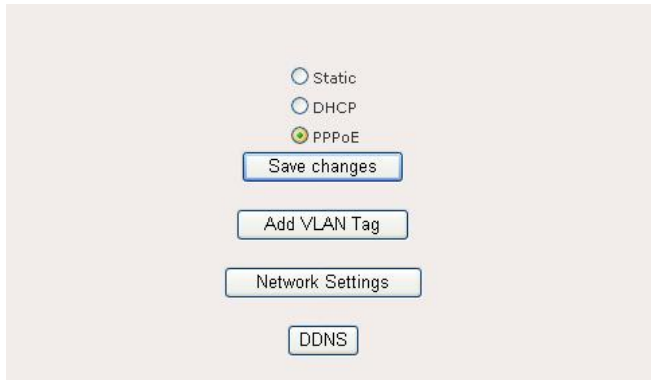
- Select the **DHCP** radio button, and then click on the **Save Changes** button.

Configuration saved. Please reboot to enable new settings.
Warning: An early DNS servers configuration found. Please remove those settings in network menu if dns server assigned by DHCP server is needed.
Warning: An early default gateway configuration found. Please remove the settings in network menu if gateway assigned by DHCP server is needed.

- The configuration has been saved; please reboot the device in order for the changes to take effect.

3.3.3.3 PPPoE (Point-to-Point Protocol over Ethernet)

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.



○ Static
○ DHCP
● PPPoE

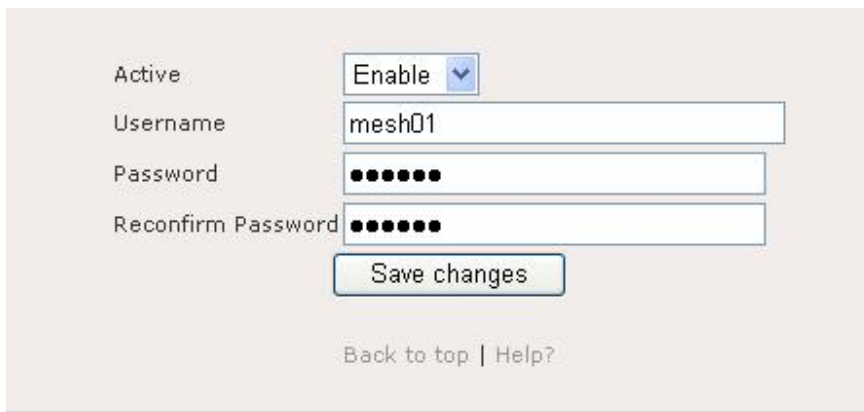
Save changes

Add VLAN Tag

Network Settings

DDNS

- Select the **PPPoE** radio button, and then click on the **Save Changes** button.



Active: Enable ▾

Username: mesh01

Password: ●●●●●●

Reconfirm Password: ●●●●●●

Save changes

Back to top | Help?

- **Active:** Choose to enable or disable the WAN type.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.3.4 VLAN Tagging

- This device also supports VLAN tagging. A Virtual LAN is a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which make them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Static
 DHCP
 PPPoE

Save changes

Add VLAN Tag

Network Settings

DDNS

- Click on the **Add VLAN Tag** button.

VLAN Tag Table

ID	IP	Netmask	Comments	Active

Action: Add

Save changes

- The table will list the current VLAN tag entries. Select Add from the drop-down list and then click on the **Save Changes** button to insert another VLAN tag entry.

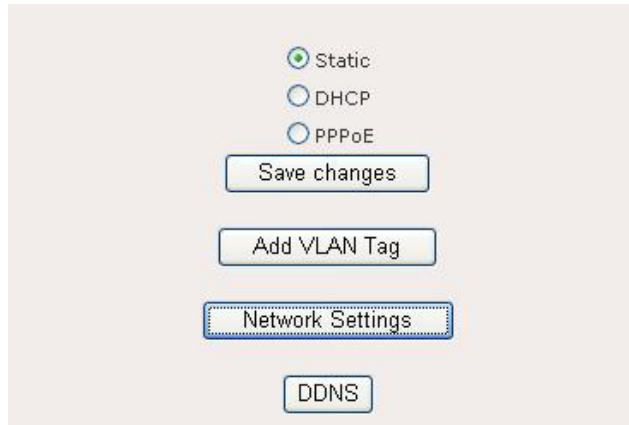
ID: 3
 Type: Static
 IP: 172.20.215.55
 Netmask: 255.255.255.0
 Comments: vlan tag 03
 Active: Enable

Save changes

- ID:** Specify the VLAN tag ID.
- Type:** Select the VLAN type from the drop-down list.
- IP:** Specify the IP address for the VLAN tag.
- Netmask:** Specify the subnet mask for the IP address.
- Comments:** You may include comments or a description.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

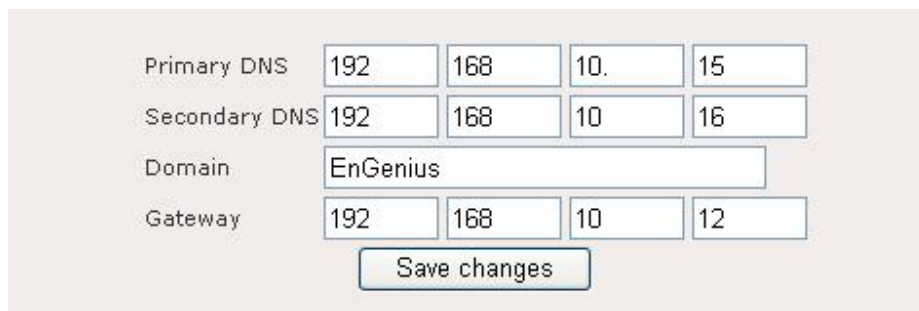
3.3.3.5 DNS, Domain, and Default Gateway

- In this section you may configure the primary/secondary DNS, domain name, and default gateway. If the WAN interface is configured as DHCP or PPPoE, you may not need to specify this information, as it will be assigned by the ISP.



The screenshot shows a vertical menu of options. At the top, there are three radio buttons: 'Static' (selected), 'DHCP', and 'PPPoE'. Below these are four buttons: 'Save changes', 'Add VLAN Tag', 'Network Settings' (highlighted with a blue border), and 'DDNS'.

- Click on the **Network Settings** button.



The screenshot shows the configuration page for Network Settings. It includes four rows of input fields: 'Primary DNS' (192, 168, 10, 15), 'Secondary DNS' (192, 168, 10, 16), 'Domain' (EnGenius), and 'Gateway' (192, 168, 10, 12). A 'Save changes' button is located at the bottom.

- **Primary DNS:** Specify the IP address of the primary DNS server.
- **Secondary DNS:** Specify the IP address of the secondary DNS server.
- **Domain:** Specify the domain name.
- **Gateway:** Specify the IP address of the default gateway.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.3.6 DDNS (Dynamic DNS)

- The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your host name to connect to your server, no matter what your IP address is.

Static
 DHCP
 PPPoE

Save changes

Add VLAN Tag

Network Settings

DDNS

- Click on the **DDNS** button.

Active: Enable ▾
 Server: dyndns ▾
 Hostname: engenius.com
 Username: engenius
 Password: ●●●●●
 Reconfirm Password: ●●●●●
 Save changes

- **Active:** Choose to enable or disable the DDNS feature.
- **Server:** Select a DDNS service provider from the drop-down list. DynDNS is a free service while.
- **Host Name:** Specify the website URL.
- **User Name:** Specify the user name for the DDNS service.
- **Password:** Specify the password for the DDNS service and verify it once again in the next field.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.4 NAT (Network Address Translation)

- In computer networking, network address translation (NAT, also known as network masquerading or IP-masquerading) is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall. It is most commonly used to enable multiple hosts on a private network to access the Internet using a single public IP address.

Active ▾

NAT List

Protocol	Port	IP	Comments	Active
(Empty row)				

Action ▾

- Select **Add** from the drop-down list to insert a new NAT entry.

Protocol ▾

Port

IP

Comments

Active ▾

[Back to top](#) | [Help?](#)

- **Protocol:** Select a protocol from the drop-down list.
- **Port:** Specify the port number.
- **IP:** Specify the IP address.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable the NAT entry.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.5 Firewall

- The device provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attacks. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.

Active:

Firewall List

Target	Source Interface	Destination Interface	Source IP	Source mask	Destination IP	Destination Mask	Protocol	Start port	End port	Comments	Active
<input checked="" type="radio"/> Allow	ath0	any	192.168.2.89	255.255.255.0	172.20.215.1	255.255.255.0	any	80	80	firewall rule	Enabled

Action:

- Select **Add** from the drop-down list to insert a new Firewall entry.

Target:

Source Interface:

Destination Interface:

Source IP:

Source Netmask:

Destination IP:

Destination Netmask:

Protocol:

Start Port:

End Port:

Comments:

Active:

[Back to top](#) | [Help?](#)

- **Target:** Choose to Allow or Deny the rules that are specified in this firewall entry.
- **Source Interface:** Select the source interface from the drop-down list.
- **Destination Interface:** Select the destination interface from the drop-down list.
- **Source IP:** Specify the IP address of the source.
- **Destination IP:** Specify the IP address of the destination.
- **Destination Netmask:** Specify the subnet mask of the destination IP address.
- **Protocol:** Select a protocol from the drop-down list.
- **Start/End Port:** Specify the start and end port.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable the NAT entry.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.6 NTP (Network Timing Protocol)

- This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured by synchronizing with a time server.

The screenshot shows the NTP configuration interface. At the top, there is an 'Active' dropdown menu set to 'Enable' and a 'Time Zone' dropdown menu set to 'TW-Asia/Taipei'. Below these is a 'Save changes' button. The main section is titled 'NTP Servers' and contains a table with the following data:

Server	Min Poll	Max Poll	Comment	Active
0.asia.pool.ntp.org	4	10	Default Server 1	Enabled
1.asia.pool.ntp.org	4	10	Default Server 2	Enabled

Below the table, there is an 'Action' dropdown menu set to 'Add' and another 'Save changes' button.

- Timezone:** Select enable from the drop-down list to activate the time zone feature.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- Select **Add** from the drop-down list to insert a new NTP Server entry.

The screenshot shows the form for adding a new NTP server. It includes the following fields:

- Server:** 0.asia.pool.ntp.org
- Min Poll:** 4
- Max Poll:** 10
- Comments:** Default Server 1
- Active:** Enable

Below the form is a 'Save changes' button and a footer with the text 'Back to top | Help?'.

- Server:** Specify the name of IP address of the NTP server.
- Min Poll:** Specify the minimum number of times that the device should poll the server.
- Max Poll:** Specify the maximum number of times that the device should poll the server.
- Comments:** You may include comments or a description.
- Active:** Choose to enable or disable the NTP Server entry.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.7 VPN (IPSec, L2TP)

- 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.

- Active:** Choose to enable or disable IPSec.
 - Type:** Select the security type from the drop-down list.
 - Local ID:** Specify the local ID.
 - Remote ID:** Specify the remote ID.
 - Remote IP:** Specify the IP address of the remote server.
 - Remote Subnet:** Specify the subnet for the remote server.
 - Remote Netmask:** Specify the subnet mask for the remote server.
 - Local Certificate Password:** Specify the password for the certificate.
 - Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- Layer 2 Tunneling Protocol 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.

- Active:** Choose to enable or disable L2TP.
- L2TP LNS address:** Specify the IP address of the server.
- Username:** Specify the user name.
- Password:** Specify the password and then re-type it in the next field for confirmation.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.8 MESH Interface IP Settings

- This device will form a wireless mesh network with other devices. Each mesh device will have its own IP address.
- For simplicity and easy deployment of the mesh network. Please use the **Auto IP** feature to assign all the IP addresses. If you would like manually assign an IP to the mesh, please disable the Auto IP feature. Refer to section 3.2.2 for more details about Auto IP.

IP: 10 20 215 1

Netmask: 255 0 0 0

Comments: Mesh

Active: Enable

Save changes

- **IP:** Specify an IP address for the mesh interface.
- **Netmask:** Specify the subnet mask for the IP address.
- **Comments:** You may include comments or a description.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.3.9 Routing (Static Routing, OLSR)

- This section displays the current routing table and allows you to add a new static routing entry.

Routes List

IP	Netmask	Using	Comments	Active
172.20.215.2	255.255.255.0	MESH	static route	Enabled

Action: Add

Save changes

- Select **Add** from the drop-down list and then click on the **Save Changes** button.

Subnet: 172 20 215 2

Netmask: 255 255 255 0

Direct: Direct

Device: MESH

Comments: static route

Active: Enable

Save changes

Back to top | Help?

- **Subnet:** Specify the subnet IP address.
- **Netmask:** Specify the subnet mask for the IP address.
- **Direct:** Select the route as direct or indirect.
- **Device:** Select the interface from the drop-down list.
- **Comments:** You may include comments or a description.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- 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.

**Any changes to the parameter to this page is not recommended.
Please refer to documentation for more information.**

Active: Enable

TOS value (0 ~ 16): 16

Willingness: Disable

Willingness level (0 ~ 7): 4

Hysteresis: Disable

Hysteresis Scaling (0 ~ 1.00): 0.50

Hysteresis THR High (0 ~ 1.00): 0.80

Hysteresis THR Low (0 ~ 1.00): 0.30

Link Quality Type: 0

Link Quality Size (3 ~ 128): 10

Poll Rate (0.02 ~ 10.0): 0.05

TC Type: 0

MPR (1 ~ 20): 1

Shared Key:

Reconfirm Shared Key:

Save changes

- **Note:** Any changes to the parameters on this page are not recommended. .
- **Active:** Choose to enable or disable the OLSR feature.
- **TOS Value:** Specify a TOS value for the IP header of the control traffic.
 - 0: normal service.
 - 2: minimize monetary cost
 - 4: maximize reliability
 - 8: maximize throughput
 - 16: minimize delay. (Default)
- **Willingness:** Choose to enable or disable the willingness service. Willingness will be calculated dynamically if disabled.
- **Willingness Level:** Specify a willingness level between 0 and 7.
- **Hystereisis:** Choose to enable or disable Hystereisis. This increases link robustness but delays neighbor registration.
- **Hystereisis Scaling:** Specify a level between 0 and 1.0
- **Hystereisis THR High:** Specify a level between 0 and 1.0
- **Hystereisis THR Low:** Specify a level between 0 and 1.0
- **Link Quality Type:** Specify a link quality type.
- **Link Quality Size:** Specify a link quality size between 3 and 128
- **Poll Rate:** Select a poll rate between 0.02 and 10.
- **TC Type:** Specify the amount of neighbor information that must be send in a TC message.
 - 0: only send MPR selectors. (Default)
 - 1: send MPR selectors and MPRs
 - 2: send all neighbors
- **MPR:** Specify the number of MPRs that the node should select for every two hops.
- **Shared Key:** Specify the shared key and then re-type it into the next field for confirmation.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

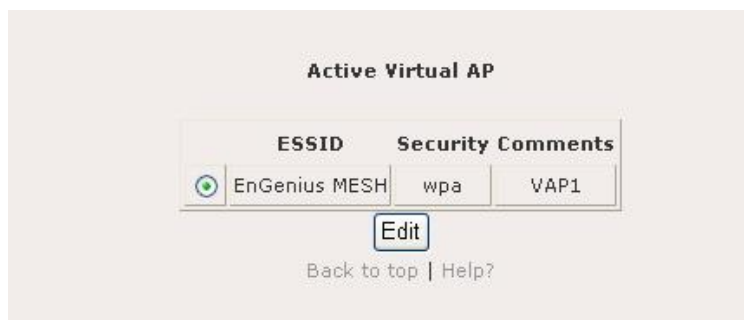
3.4 Security



- Click on the **Security** link on the navigation drop-down menu. This menu includes Mesh SSID, MAC address filter, and VLAN. The configuration steps for each option are described below.

3.4.1 MSSID

- In this section you may configure the SSID, beacon interval, RTS threshold, fragmentation threshold, DTIM interval, data rate, security type, and 802.1x.



- Click on the **Edit** button to modify the default values.

ESSID	EnGenius MESH
Broadcast SSID	Enable
Beacon Interval	100
RTS Threshold	2346
Fragmentation Threshold	2346
DTIM interval	1
Datarate	auto
Security	WPA (1 & 2)
WPA Type	TKIP
802.1x	True
Save changes	

- **ESSID:** The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- **Broadcast SSID:** Select enable (visible) or disable (invisible). This is the SSID broadcast feature. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **Beacon Interval:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 1 and 65535. The default value is 2346.
- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **DTIM Interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **Data Rate:** Select a transmission rate from the drop-down list. It is recommended to use the automatic option.
- **Security:** Select WEP or WPA (1&2)
 - **WEP** is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The

type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

- **WPA** (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **WPA Type:** The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **802.1x:** Select true or false from the drop-down list to enable or disable 802.1x.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.4.2 MAC Address Filter

- This feature is used to restrict certain MAC address from accessing the Internet. These filters can be used for securing and restricting your network.

Active

Type

MAC Access List

	MAC	Type	Comments	Active
<input checked="" type="radio"/>	00:11:22:33:33:77	allow	allow mac	Enabled
<input type="radio"/>	22:33:44:55:66:77	deny	deny mac	Enabled

Action

- **Active:** Choose to enable or disable the MAC address filter feature.
- **Type:** Choose to allow or deny access for the MAC addresses.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- **MAC Access List:** Click on the **Add** button to insert a MAC address.

MAC: 00 11 22 33 33 77

Type: Allow

Comments: allow mac

Active: Enable

Save changes

Back to top | Help?

- **MAC:** Specify the MAC address.
- **Type:** Select Allow or Deny.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable the filter on this MAC address.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.4.3 VLAN

- A Virtual LAN is a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which make them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Active VLAN

ID	Name	IP	Netmask	Comments
0	vlan0	172.20.215.1	255.255.255.0	Default VLAN

Edit

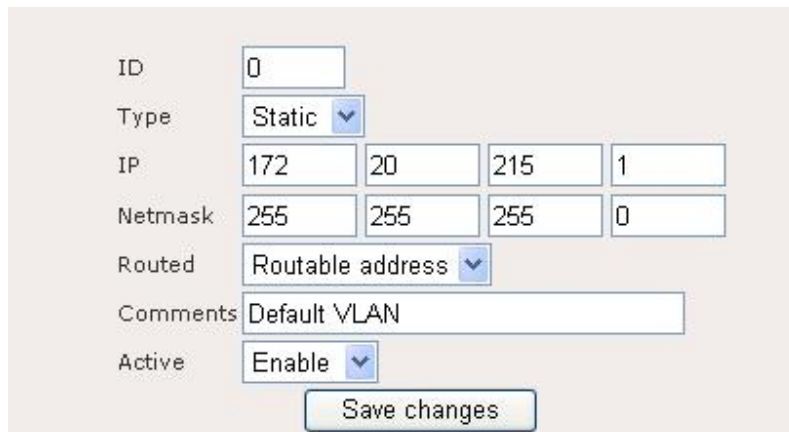
Inactive VLAN

VLAN1

Edit

Back to top | Help?

- Click on the **Edit** button to modify the existing VLAN.



The screenshot shows a configuration form for a VLAN. The fields are as follows:

ID	<input type="text" value="0"/>			
Type	<input type="button" value="Static"/>			
IP	<input type="text" value="172"/>	<input type="text" value="20"/>	<input type="text" value="215"/>	<input type="text" value="1"/>
Netmask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Routed	<input type="button" value="Routable address"/>			
Comments	<input type="text" value="Default VLAN"/>			
Active	<input type="button" value="Enable"/>			

- **ID:** Specify the VLAN tag ID.
- **Type:** Select the VLAN type from the drop-down list.
- **IP:** Specify the IP address for the VLAN tag.
- **Netmask:** Specify the subnet mask for the IP address.
- **Routed:** Select if the VLAN is routed through the routing table or NAT.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable this VLAN entry.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.5 Services



- Click on the **Services** link on the navigation drop-down menu. This menu includes PPTP Server, Mobile IP, Traffic Shaping, Route Watchdog System Watchdog, and SSHD. The configuration steps for each option are described below.

3.5.1 PPTP Server

- PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a username and password (provided by your ISP) to gain access to the Internet. The supported authentication protocols are PAP and CHAP

Active	Enable			
Server IP	10	20	215	1
Client IP Start	10	20	215	2
Client IP End	10	20	215	11

Save changes

PPTP User List

Username	IP	Comments	Active
pptp1	0.0.0.0	Management VPN	Enabled

Action: Add

Save changes

- Active:** Choose to enable or disable this the PPTP Server feature.
- Server IP:** Specify the IP address of the server.

- **Client IP Start:** Specify the starting address for the client.
- **Client IP End:** Specify the ending address for the client.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- Click on the **Add** button to insert an entry into the PPTP user list.

Username: pptp1

Password: ●●●●●●

Reconfirm Password: ●●●●●●

IP: 64 65 78 54

Comments: Management VPN

Active: Enable

Save changes

[Back to top](#) | [Help?](#)

- **Username:** Specify the PPTP username.
- **Password:** Specify the PPTP password and then re-type it into the next field for confirmation.
- **IP:** Specify the IP address of the PPTP server.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable this VLAN entry.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.5.2 Mobile IP

- This section allows you to configure the Mobile IP service.

Active: Enable

Netname: EnGenius

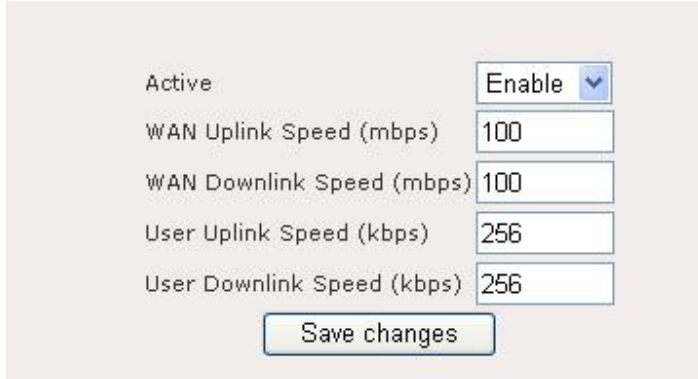
MLRD IP: 172 20 215 9

Save changes

- **Active:** Choose to enable or disable the mobile IP service.
- **Netname:** Specify a name for the service.
- **MLRD IP:** Specify the IP address of the mobile registrar server.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.5.3 Traffic Shaping

- The traffic shaping feature allows you to limit the bandwidth allocation to the users.



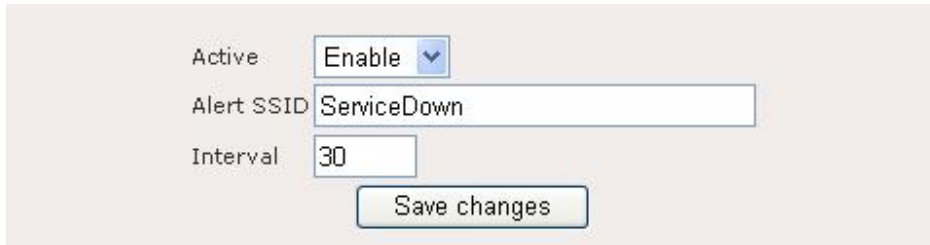
Active	Enable ▾
WAN Uplink Speed (mbps)	100
WAN Downlink Speed (mbps)	100
User Uplink Speed (kbps)	256
User Downlink Speed (kbps)	256

Save changes

- **Active:** Choose to enable or disable the traffic shaping feature.
- **WAN Uplink Speed (Mbps):** Specify the maximum uplink speed.
- **WAN Downlink Speed (Mbps):** Specify the maximum downlink speed.
- **User Uplink Speed (Kbps):** Specify the maximum user uplink speed.
- **User Downlink Speed (Kbps):** Specify the maximum user downlink speed.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.5.4 Route Watchdog

- This section allows you to configure the route watchdog feature.



Active	Enable ▾
Alert SSID	ServiceDown
Interval	30

Save changes

- **Active:** Choose to enable or disable the feature.
- **Alert SSID:** Specify an alert SSID.
- **Interval:** Specify the watchdog interval (seconds).
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.5.5 System Watchdog

- This section allows you to configure the system watchdog feature.

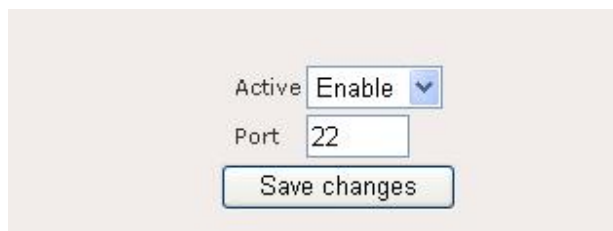


Active:
Interval:

- **Active:** Choose to enable or disable the feature.
- **Interval:** Specify the watchdog interval (seconds).
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.5.6 SSHD (Secure Shell Daemon)

- This section allows you to configure the SSHD (Secure Shell Daemon) feature.



Active:
Port:

- **Active:** Choose to enable or disable the feature.
- **Port:** Specify the port number.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.6 QoS



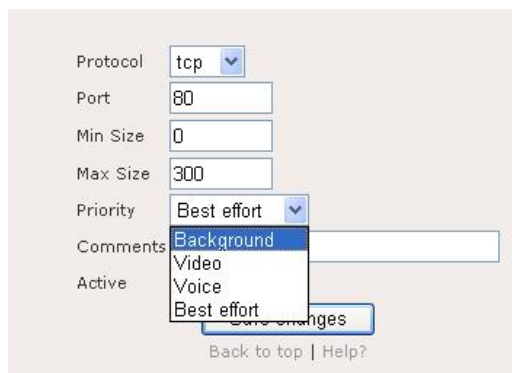
- Click on the **QoS** link on the navigation drop-down menu. This menu includes QoS Table and WMM. The configuration steps for each option are described below.

3.6.1 QoS Table

- This section allows you to QoS (Quality of Service) feature of the device.



- Select **Add** from the drop-down list to insert a new QoS entry.



- **Protocol:** Specify the protocol.
- **Port:** Specify the port number.
- **Min Size:** Specify the minimum packet size.
- **Max Size:** Specify the maximum packet size.
- **Priority:** Select the QoS priority from the drop-down list. Background, Video, Voice, or Best Effort.
- **Comments:** You may include comments or a description.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.6.2 WMM (Wireless Multimedia)

- Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories), however it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

WME List			
	Interface	Comments	Active
<input checked="" type="checkbox"/>	ath0	default adhoc	Enabled
<input type="checkbox"/>	wlan0	default AP	Enabled

Action:

- Select **Add** from the drop-down list to insert a new WME entry.

Interface:
 Comments:
 Active:

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

[Back to top](#) | [Help?](#)

-
- **Interface:** Select an interface from the drop-down list.
 - **Comments:** You may include comments or a description.
 - **Active:** Choose to enable or disable this feature.
 - **CWMIN:** Specify the minimum value of CW in WMM.
 - **CWMAX:** Specify the Highest CW value as used in WMM.
 - **AIFS:** Specify the inter-frame spacings in WMM.
 - **TX OP LIMIT:** Schedule the transmission OPs as defined in WMM.
 - **ACM:** Choose to enable or disable the ACM as defined in WMM.
 - **NO ACK POLICY:** Specify the ACK policy of WMM.
 - Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.7 System Management



- Click on the **System Management** link on the navigation drop-down menu. This menu includes HTTPD, SNMP, Syslog Server, Firmware Upgrade, SNMP Trap, and Security configuration. The configuration steps for each option are described below.

3.7.1 HTTPD

- This device can be managed through a web-browser that supports the HTTP protocol. On this page you can configure the settings for the management page.

Active Enable

Port

Username

Password

Reconfirm Password

Certificate Password

Reconfirm Certificate Password

Access Control Enable

Access Control List

	Device	Subnet	Netmask	Comments	Active
<input checked="" type="radio"/>	MESH	-	-	Mesh	Enabled
<input type="radio"/>	WAN	-	-	WAN	Enabled
<input type="radio"/>	VLAN0	-	-	VLAN	Enabled

Action

- **Active:** Choose to enable or disable this feature.
- **Port:** Specify the port number.
- **Username:** Specify a user name.
- **Password:** Specify a password and then re-type it into the next field for confirmation.
- **Certificate Password:** Specify the password for the authentication certificate and then re-type it into the next field for confirmation.
- **Access Control:** Choose to enable or disable access control.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- Click on the **Add** button to insert an entry into the access control list.



The screenshot shows a web form for configuring access control. The form has four rows of input fields:

- Device:** A drop-down menu with 'MESH' selected.
- Using:** A drop-down menu with 'Device' selected.
- Comments:** A text input field containing 'Device' and 'Network' on separate lines.
- Active:** A drop-down menu with 'Enable' selected.

Below the form is a 'Save changes' button and a link 'Back to top | Help?'.

- **Device:** Select an interface from the drop-down list.
- **Using:** Select device or network from the drop-down list.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable this feature.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.7.2 SNMP

- Simple Network Management Protocol (SNMP) is used to monitor devices for conditions that warrant administrative attention.

Active

Version

Port

v2 Read Community

Reconfirm v2 Read Community

v2 Read-write Community

Reconfirm v2 Read-write Community

v3 Read Username

v3 Read-write Username

v3 Password

Reconfirm v3 Password

v3 Passphrase

Reconfirm v3 Passphrase

Access Control

Access Control List

	Device	Subnet	Netmask	Comments	Active
<input checked="" type="radio"/>	MESH	-	-	Mesh	Enabled
<input type="radio"/>	WAN	-	-	WAN	Enabled
<input type="radio"/>	VLAN0	-	-	VLAN	Enabled

Action

- **Active:** Choose to enable or disable this feature.
- **Version:** Select the SNMP version from the drop-down list: v1, v2c, v3, or all
- **Port:** Specify the SNMP port number.
- **v2 Read Community:** Specify the v2 read community password and then re-type it into the next field for confirmation.
- **v2 Read-write Community:** Specify the v2 read/write community password and then re-type it into the next field for confirmation.
- **v3 Read Username:** Specify the v3 read username
- **v3 Read-write Username:** Specify the v3 read username
- **v3 Password.** Specify the v3 read password and then re-type it into the next field for confirmation.
- **v3 Passphrase:** Specify the v3 read password and then re-type it into the next field for confirmation.
- **Active:** Choose to enable or disable access control.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.7.3 SysLog Server

- This device can automatically send system logs to a SysLog server. On this page you may configure the SysLog notice and server IP address.



Active	Enable
Klog	Disable
Level	Notice
Remote Syslog	Enable
Remote Server Address	172.20.215.6

Save changes

- **Active:** Choose to enable or disable this feature.
- **Klog:** Choose to enable or disable this feature.
- **Level:** Select a logging level from the drop-down list.
- **Remote Syslog:** Choose enable to remotely control the syslog feature.
- **Remote Server Address:** Specify the IP address of the remote syslog server.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.7.4 Firmware Upgrade

- Click on the **Firmware** link in the navigation menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.



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

Current Version: 1.0.1305

Select a firmware to upgrade:

- Ensure that you have downloaded the appropriate firmware from the vendor's website.
- Click on the **Browse** button to select the firmware and then click on the **Upload** button.
- **Note:** Please do not power off the device during the firmware upgrade as they may cause permanent damage to the device.

3.7.5 SNMP Trap

- The Trap feature is used to report a system alert to a server. This page allows you to enable the trap function of certain feature and then send to an assigned server.

The screenshot displays the SNMP Trap configuration interface. It is divided into two main sections. The upper section contains a list of features, each with a corresponding dropdown menu to select its trap status. The lower section features a table titled 'Trap Server List' and an 'Add' button.

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

Save changes

Trap Server List				
	Version	Trap to	Comments	Active
<input checked="" type="radio"/>	3	172.20.215.4	ver 3	Enabled
<input type="radio"/>	2c	172.20.215.2	ver 3	Enabled

Action: Add

Save changes

- **Configuration:** Choose to enable or disable this trap.
- **Security:** Choose to enable or disable this trap.
- **Wireless:** Choose to enable or disable this trap.
- **Operational:** Choose to enable or disable this trap.
- **Flash:** Choose to enable or disable this trap.
- **Tftp:** Choose to enable or disable this trap.
- **Image:** Choose to enable or disable this trap.
- **Auth failure:** Choose to enable or disable this trap.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- Click on the **Add** button to insert an entry into the Trap Server list.

IP	<input type="text" value="172"/> <input type="text" value="20"/> <input type="text" value="215"/> <input type="text" value="3"/>
Community	<input type="password" value="••••••"/>
Reconfirm Community	<input type="password" value="••••••"/>
Version	<input type="button" value="2c"/> ▾
Comments	<input type="text" value="ver 2c"/>
Active	<input type="button" value="Enable"/> ▾
<input type="button" value="Save changes"/>	

- **IP:** Specify the IP address of the Trap Server.
- **Port:** Specify the SNMP port number.
- **v2 Read Community:** Specify the v2 read community password and then re-type it into the next field for confirmation.
- **Version:** Select the SNMP version from the drop-down list: v1, v2c, v3, or all
- **Active:** Choose to enable or disable access control.
- **Comments:** You may include comments or a description.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.7.6 Webserver Certificate / IPsec Management (RSA, X.509)

- Click on the **Configuration** link in the navigation menu This section allows you to upload a web-certificate to the device and manage the IPsec, RSA, and X509 certificates.

Upload New Webserver Certificate

Upload certificate as PEM file (*.pem):

IPSEC Management

- **Upload New Webserver Certificate:** Click on the **Browse** button to select the certificate and then click on the **Upload** button.
- **Manage RSA:** Click on the **Manage RSA** button to upload a private RSA key.



Existing Public Key

Local Public RSA Key in RFC 2537 Format

Upload Key-Pair

Please select a Private RSA key to upload:

- **Upload Key-Pair:** Click on the **Browse** button to select the certificate and then click on the **Upload** button.
- **Manage X509:** Click on the **Manage X509** button to upload a local and remote certificate from the CA (Certification Authority).



Local Certificate

Existing local certificate:
None

Existing root certificate authority:
None

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

Remote Certificate

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

Existing Certificate:
None

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

- **Local Certificate:** Click on the **Browse** button to select the certificate and then click on the **Upload** button.
- **Remote Certificate:** Click on the **Browse** button to select the certificate and then click on the **Upload** button.

3.8 Login Setup / Captive Portal



- Click on the **Login Setup** link on the navigation drop-down menu. This menu includes Login Parameters, RADIUS, Local Users Database, Webspaces, and Customize Login. The configuration steps for each option are described below.

3.8.1 Login Parameters

- Click on the **Login Parameters** link in the navigation menu. This section allows you to configure the settings of the Captive Portal. A captive portal directs a user to a specific web-page before proceeding to surf the Internet.

Webbased Authentication	Enable <input type="button" value="v"/>
Redirect to URL	<input type="text"/>
POP3 Email Push	Enable <input type="button" value="v"/>
External Login Server	Disable <input type="button" value="v"/>
External Server URL	<input type="text"/>
Default Idle Timeout	<input type="text" value="300"/>
Default Session Timeout	<input type="text" value="65000"/>
Login using HTTP	Enable <input type="button" value="v"/>
HTTP Port	<input type="text" value="3000"/>
Login Using HTTPS	Enable <input type="button" value="v"/>
HTTPS Port	<input type="text" value="3001"/>
Internal Web Space	Enable <input type="button" value="v"/>
Web Space Port	<input type="text" value="3002"/>
Default Language	<input type="text" value="English"/>
Multiple Login	Disable <input type="button" value="v"/>
1X LOGIN	Enable <input type="button" value="v"/>
<input type="button" value="Save changes"/>	

- **Webbased Authentication:** Choose to enable or disable web-based authentication.
- **Redirect to URL:** Specify the URL to redirect users after being successfully authenticated.
- **POP3 Email Push:** drop down menu to enable or disable Push email to not authenticated users.
- **External Login Server:** drop down menu to enable or disable External Login Server.
- **External Server URL:** Specify the URL for the external server.
- **Default Idle Timeout:** Specify the idle timeout in seconds.
- **Default Session Timeout:** Specify the idle session time out in seconds.
- **Login using HTTP:** Choose to enable or disable login with HTTP.
- **HTTP port:** Specify the HTTP port number used in captive login.
- **Login using HTTPS:** Choose to enable or disable login with HTTPS.
- **HTTPS port:** Specify the HTTPS port number used in captive login.
- **Internal Web Space:** Choose to enable or disable the internal web space feature.
- **Web space port:** Specify the port number for the internal web space.
- **Default Language:** Enter the default login language
- **Multiple Login:** Choose to enable or disable multiple user login.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.

3.8.2 RADIUS

- Click on the RADIUS link in the navigation menu. Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol This section allows you to configure the RADIUS server authentication and accounting settings. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this device. Furthermore, it may be necessary to configure the RADIUS Server to allow this device to authenticate users.

Active

NAS ID

Called Station ID

NAS Port

NAS Port Type

Interim Update Interval

RADIUS Server List

	Name	Type	Port	Comments	Active
<input checked="" type="radio"/>	172.20.215.11	1	2365	radius	Enabled
<input type="radio"/>	172.20.215.12	2	2365	radius	Enabled

Action

- **Active:** Choose to enable or disable this feature.
- **NAS ID:** Specify the name/ID of the Network Access Server.

- **Called Station ID:** Specify the name/ID of the called station.
- **NAS port:** Specify the port number of the Network Access Port.
- **NAS port type:** Type the NAS port type.
- **Interim Update Interval:** Specify the number of seconds after which the client must re-register with the RADIUS server.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect.
- Click on the **Add** button to insert an entry into the RADIUS server list.

Server Name: 172.20.215.11

Server Type: Authenticate

Server Port: 2365

Server Secret: ●●●●●●

Reconfirm Server Secret: ●●●●●●

Comments: radius

Active: Enable

Save changes

Back to top | Help?

- **Server Name:** Specify the IP address of the RADIUS server.
- **Server Type:** Select authenticate or accounting from the drop-down list.
- **Server Port:** Specify port number of the RADIUS server.
- **Server Secret:** Specify the shared secret of the RADIUS server, and then re-type it into the next field for confirmation.
- **Comments:** You may include comments or a description.
- **Active:** Choose to enable or disable this feature.
- Click on the **Save Changes** button to store and changes and then **reboot** the device in order for the changes to take effect

3.8.3 Local Users Database

- Click on the **Local Users Database** link in the navigation menu. This section displays the list of users and allows you to add more users.

User 'USER3' has been added

List of Users

Username	action
USER1	Delete Change Password
USER2	Delete Change Password
USER3	Delete Change Password

Add new user

Add user

- Click on the **Add User** button to insert a new user into the database.

- **Username:** Specify a user name.
- **New Password:** Specify a password for the user name and then re-type it into the next field for confirmation.
- Click on the **Add** button to insert the new user into the database.

3.8.4 Webspace

- Click on the **Webspace** link in the navigation menu. This section allows you to upload html files for the captive portal.

- Click on the **Browse** button to select the html file and then click on the **Upload** button.

3.8.5 Customize Login

- Click on the **Customize Login** link in the navigation menu. This section allows you to upload language specific files for the captive portal.

- Click on the **Browse** button to select the language file and then click on the **Upload** button.
- **Add Language:** Specify the language and then click on the **Add** button.
- **Default language:** Select the default language from the drop-down list and then click on the **Change** button.

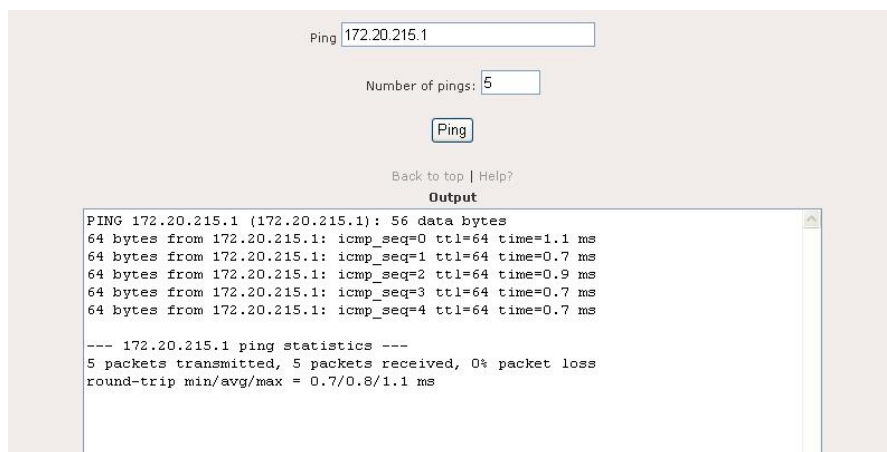
3.9 Tools



- Click on the **Tools** link on the navigation drop-down menu. This menu includes ping, ifconfig, route, TFTP. The configuration steps for each option are described below.

3.9.1 Ping


- Click on the **Ping** link on the navigation drop-down menu. This option allows you to ping other devices in order to test connectivity.



- **Ping:** Specify the IP address that you would like to ping.
- **Number of pings:** Specify the number of times to ping the IP address.

3.9.2 Ifconfig

- Click on the **Ifconfig** link on the navigation drop-down menu. This option displays the interface configuration, which includes IP address, MAC address, Tx/Rx bytes, and error packets. Click on the **Ifconfig** button to view the output.



The screenshot shows the 'Ifconfig' page with a 'Back to top | Help?' link and an 'Output' section. The output displays the configuration for four interfaces: ath0, ath1, ixp0, and ixp1. Each interface configuration includes details such as link encapsulation, hardware address, IP address, broadcast address, subnet mask, MTU, metric, and statistics for packets and bytes transmitted and received.

```

Output
ath0  Link encap:Ethernet  HWaddr 00:02:6F:49:45:31
      inet addr:10.20.215.1  Bcast:10.255.255.255  Mask:255.0.0.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3209 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B)  TX bytes:211914 (206.9 KiB)

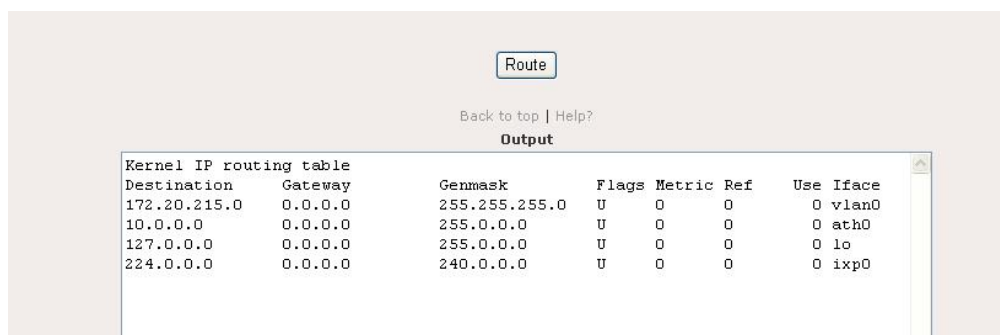
ath1  Link encap:Ethernet  HWaddr 00:02:6F:49:45:32
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:70222 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3913 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1268675 (1.2 MiB)  TX bytes:3465781 (3.3 MiB)

ixp0  Link encap:Ethernet  HWaddr 00:22:33:00:0A:77
      UP BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:219 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:256
      RX bytes:0 (0.0 B)  TX bytes:129210 (126.1 KiB)

ixp1  Link encap:Ethernet  HWaddr 00:22:33:00:0A:78
      UP BROADCAST MULTICAST  MTU:1500  Metric:1
  
```

3.9.3 Route

- Click on the **Route** link on the navigation drop-down menu. This option displays the routing table, which includes destination IP, gateway IP, subnet mask, flags, metrics, and interface. Click on the **Route** button to view the output.



The screenshot shows the 'Route' page with a 'Back to top | Help?' link and an 'Output' section. The output displays the 'Kernel IP routing table' with columns for Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Iface.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.20.215.0	0.0.0.0	255.255.255.0	U	0	0	0	vlan0
10.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	ath0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
224.0.0.0	0.0.0.0	240.0.0.0	U	0	0	0	ixp0

3.9.4 TFTP

- Click on the **TFTP** link on the navigation drop-down menu. This option allows you to upload a configuration to the device.

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

TFTP to

Operation

File Name

Type of File

- **TFTP to:** Specify the IP address
- **Operation:** Select put or get from the drop-down list.
- **File Name:** Specify the file name.
- **Type of File:** Select config or firmware from the drop-down list.
- Click on the **Execute** button to begin the process.

3.10 Status



- Click on the **Status** link on the navigation drop-down menu. This menu includes System, Interface, Services, Users, Mobile IP, Topology, and System Log. The configuration steps for each option are described below.

3.10.1 System Status

- Click on the **Status** link on the navigation drop-down menu. This option displays the system uptime, CPU speed, free RAM, and firmware version.

System Uptime:	0 days, 1 hrs, 26 minutes
CPU Speed:	527.56
Average CPU usage: (Since boot)	3.70 %
Average CPU usage: (Last two seconds)	1.47 %
Free RAM:	49065984 byte
Firmware Release Version	1.0.1305
Back to top Help?	

3.10.2 Interface Status

- Click on the **Interfaces** link on the navigation drop-down menu. This option displays the details of the WAN, MESH, and VLAN0 interface. Click on the Get Details button for each interface to view the status.



3.10.2.1 WAN Interface Status

- Click on the **Get Details** button for the WAN interface. This section displays the hardware MAC address, IP type, IP address, broadcast address, netmask, MTU, and Tx/Rx packet information.



3.10.2.2 MESH Interface Status

- Click on the **Get Details** button for the MESH interface. This section displays the hardware MAC address, IP type, IP address, broadcast address, netmask, MTU, and Tx/Rx packet information. On the wireless interface it displays the ESSID, 802.11 band, frequency, MAC address, data rate, tx output power, encryption key, and QoS.


```

Hardware Address: 00:02:6F:49:45:31
IP Type:         static
IP Address:      10.20.215.1
Broadcast Address: 10.255.255.255
Netmask:        255.0.0.0
MTU:            1500
Rx bytes:       0 (0.0 B)
Tx bytes:       219722 (214.5 KiB)
Rx packets:     0
Rx errors:      0
Rx dropped:     0

```

Wireless Information

```

ESSID:          EnGenius Backhaul
Band:           802.11a
Frequency:      5.26 GHz
Cell:           02:02:6F:49:45:31
Rate:           auto
Max Tx-Power:  18 dBm
Encryption Key: off
Quality:        0/94

```

3.10.3 Services Status

- Click on the **Services** link on the navigation drop-down menu. This option displays the current status of the following services: DHCP server, DNS server, Dynamic DNS, IPsec, L2TPC, Mobile IP, NTP client,, OLSR, PPPoE, PPTP server, routedog, SSHD, SNMP server, Syslog server, traffic shaping, and web servers.

Status

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

[Back to top](#) | [Help?](#)

3.10.4 Users Status

- Click on the **Status** link on the navigation drop-down menu. This option displays the list of users that are currently connected to the device.



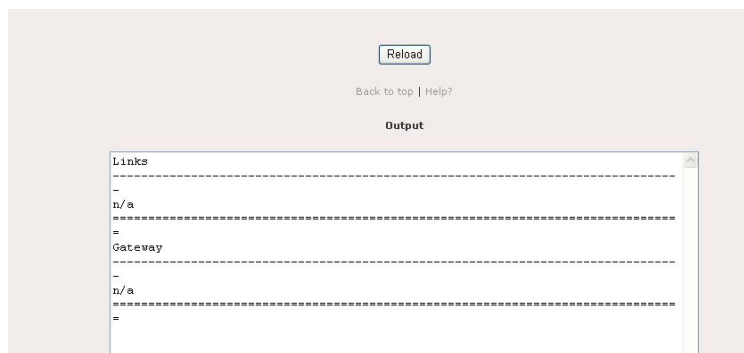
3.10.5 Mobile IP Status

- Click on the **Mobile IP** link on the navigation drop-down menu. This option displays the current status of the Mobile IP feature. Click on the **Get Status** button to view the output.



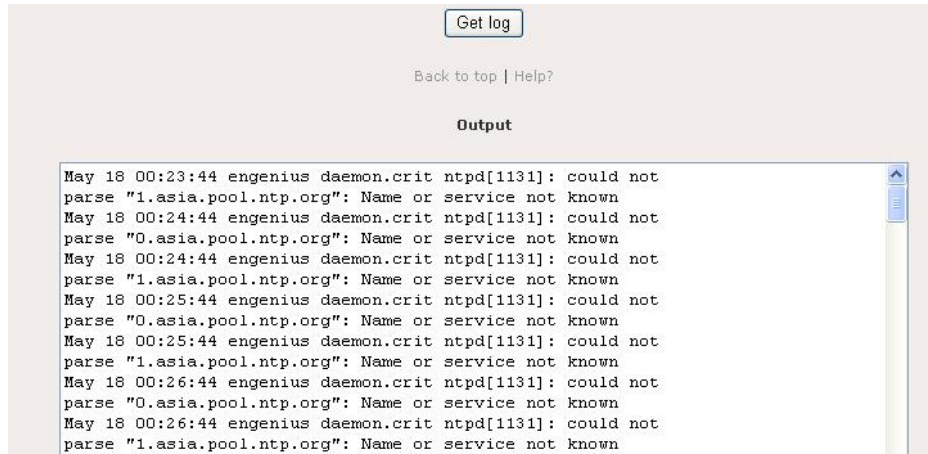
3.10.6 Topology Status

- Click on the **Topology** link on the navigation drop-down menu. This option displays the current status of the topology feature. Click on the **Reload** button to view the output.



3.10.7 System Log Status

- Click on the **System Log** link on the navigation drop-down menu. This option displays the list of events by date and time.. Click on the **Get Log** button to view the output.

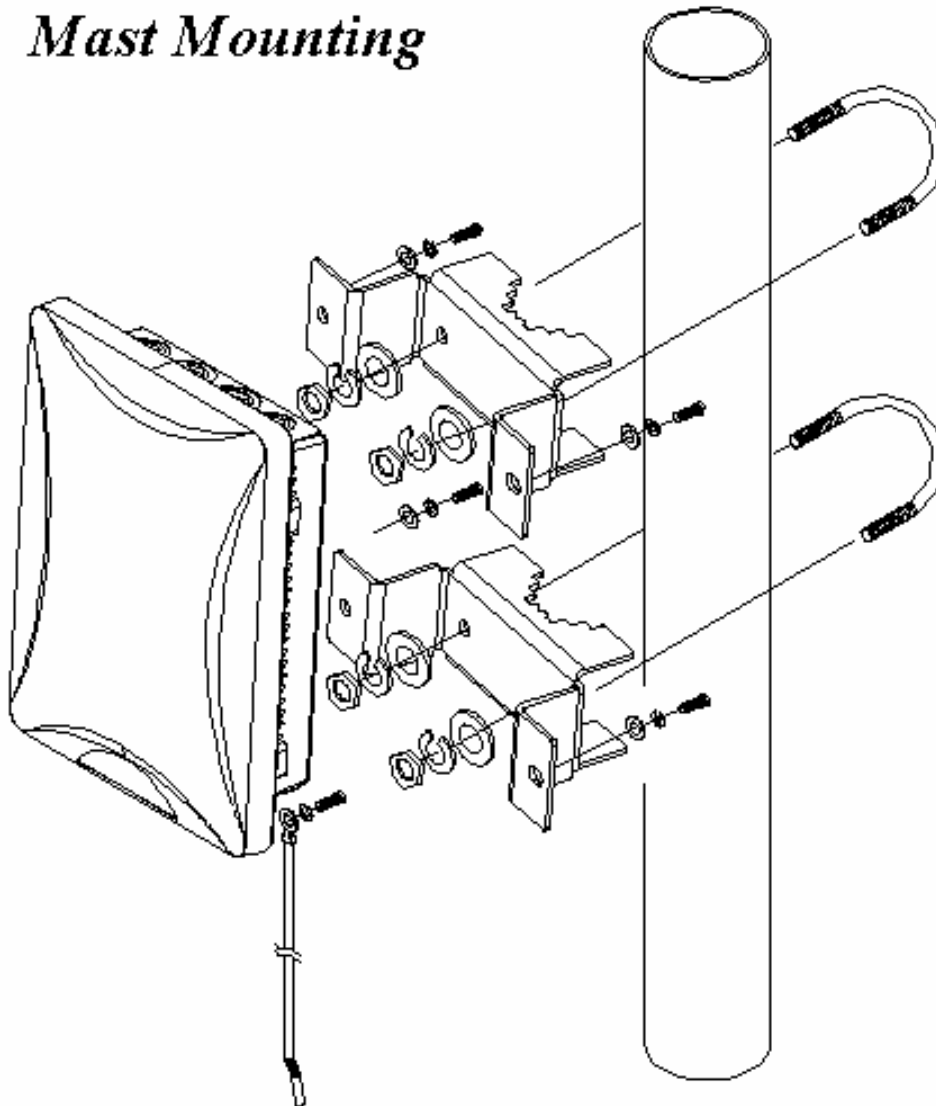


The screenshot shows a web interface for viewing system logs. At the top, there is a 'Get log' button. Below it, there is a link 'Back to top | Help?'. The main content area is titled 'Output' and contains a terminal window displaying the following log entries:

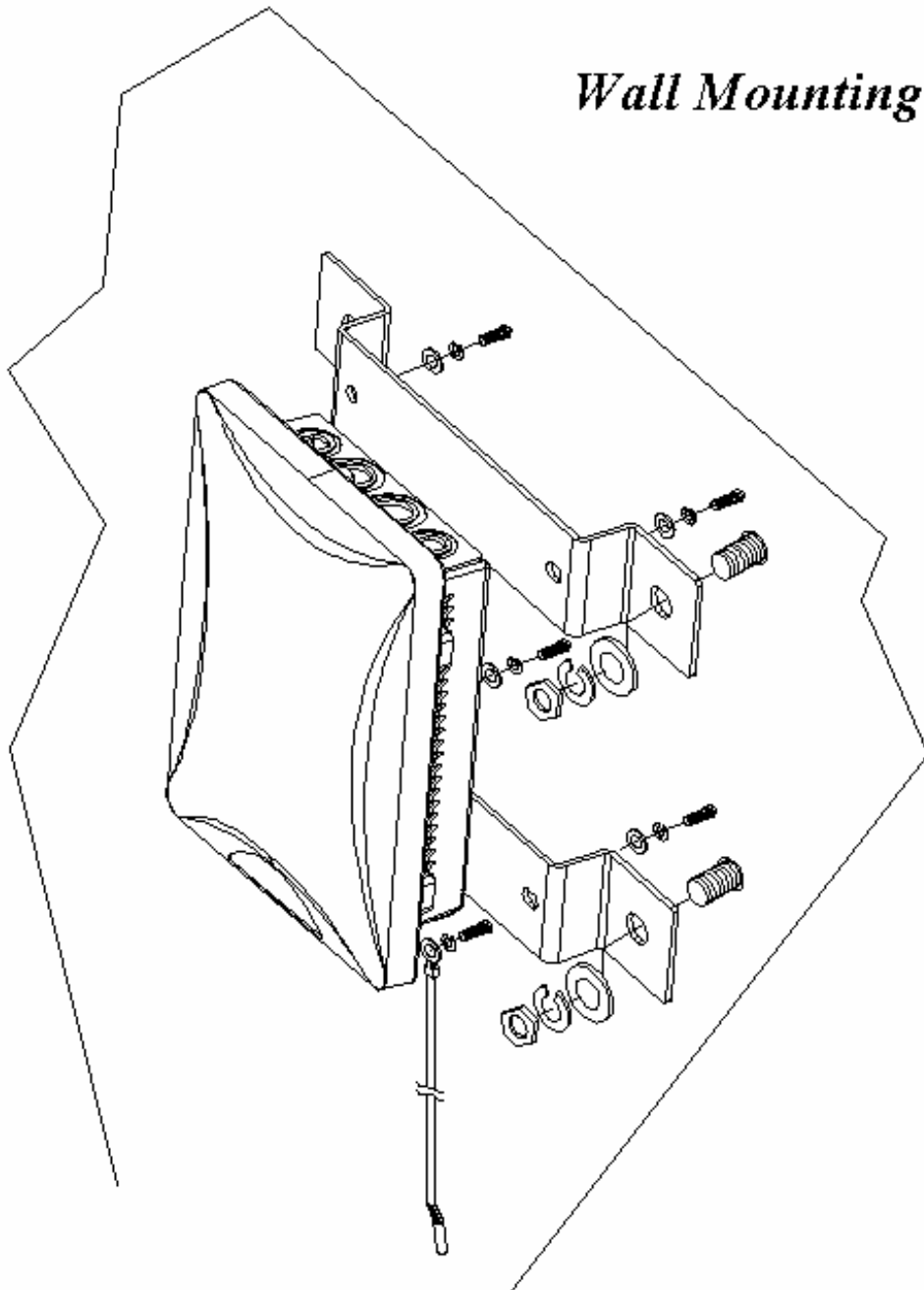
```
May 18 00:23:44 engenius daemon.crit ntpd[1131]: could not
parse "1.asia.pool.ntp.org": Name or service not known
May 18 00:24:44 engenius daemon.crit ntpd[1131]: could not
parse "0.asia.pool.ntp.org": Name or service not known
May 18 00:24:44 engenius daemon.crit ntpd[1131]: could not
parse "1.asia.pool.ntp.org": Name or service not known
May 18 00:25:44 engenius daemon.crit ntpd[1131]: could not
parse "0.asia.pool.ntp.org": Name or service not known
May 18 00:25:44 engenius daemon.crit ntpd[1131]: could not
parse "1.asia.pool.ntp.org": Name or service not known
May 18 00:26:44 engenius daemon.crit ntpd[1131]: could not
parse "0.asia.pool.ntp.org": Name or service not known
May 18 00:26:44 engenius daemon.crit ntpd[1131]: could not
parse "1.asia.pool.ntp.org": Name or service not known
```

Appendix A – Mast Mounting

Mast Mounting



Appendix B – Wall Mounting



Appendix C – Glossary

8

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Ad-hoc network

Peer-to-Peer network between wireless clients

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B**Backward Compatible**

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C**Cable modem**

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D**Data**

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

DB-25

A 25 pin male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dB_i

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the same time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E**EAP**

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F**Fiber optic**

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G**Gain**

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H**H.323**

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I**ICMP**

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J**Java**

A programming language used to create programs and applets for web pages

K**Kbps**

Kilobits per second

Kbyte

Kilobyte

L**L2TP**

Layer 2 Tunneling Protocol

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

M**MAC Address**

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O**OFDM**

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P**Password**

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q**QoS**

Quality of Service

R**RADIUS**

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass through the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U**UDP**

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V**Virtual Private Network**

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W**Wake on LAN**

Allows you to power up a computer though it's Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X**xDSL**

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y**Yagi antenna**

A directional antenna used to concentrate wireless signals on a specific location

Appendix D – Specifications

Wireless Information

Wireless Standard

IEEE 802.11a

IEEE 802.11b/g

Media Access Protocol

CSMA/CA

RF Modulation

802.11a: OFDM

802.11g: OFDM

802.11b: DSSS

Data Rates

802.11a: 6, 9, 12, 18, 24, 36, 48, 54Mbps

802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps

802.11b: 1, 2, 5.5, 11Mbps

Frequency Band

802.11a:

5.15~5.35GHz,

5.47~5.725GHz, 5.725~5.825GHz

802.11b/g:

U.S., Europe and Japan product covering 2.4 to 2.484 GHz, programmable for different country regulations

Modulation Technology

802.11a/g:

OFDM (64-QAM, 16-QAM, QPSK, BPSK)

802.11b:

DSSS (DBPSK, DQPSK, CCK)

Operating Channels

802.11b/g

11 for North America, 14 for Japan, 13 for Europe

802.11a

US/Canada:12 non-overlapping channel (5.15~5.35GHz, 5.725~5.825GHz)

Europe:19 non-overlapping channel (5.15~5.35GHz, 5.47~5.825GHz)

Japan:4 non-overlapping channel (5.15~5.25GHz)

China:5 non-overlapping channel (5.725~5.85GHz)

Receive Sensitivity (Typical)

802.11a:

-88dBm @ 6Mbps,

-70dBm @ 54Mbps

802.11g:

-90 dBm @ 6Mbps,

-74 dBm @ 54Mbps

802.11b:

-95 dBm @ 1Mbps

-90 dBm @ 11Mbps

Available transmit power (Typical)

EOM-8670 (FCC)

● 4.92~5.08 GHz

17 dBm @6~36Mbps

16 dBm @48Mbps

15 dBm @54Mbps

● 5.18~5.24 GHz

17 dBm @6~36Mbps

16 dBm @48Mbps

15 dBm @54Mbps

● 5.26~5.32 GHz

20 dBm @6~24Mbps

18 dBm @36Mbps

16 dBm @48Mbps

15 dBm @54Mbps

● 5.745~5.825GHz

18 dBm @6~24Mbps

16 dBm @36Mbps

14 dBm @48Mbps

13 dBm @54Mbps

● 2.412~2.462 GHz (IEEE802.11g)

25 dBm @6~24Mbps

23 dBm @36Mbps

22 dBm @48Mbps

21 dBm @54Mbps

● 2.412~2.462 GHz (IEEE802.11b)

25 dBm @1~11Mbps

EOM-8670 (ETSI)

● 4.92~5.08 GHz

20 dBm @6~36Mbps

16 dBm @48Mbps

15 dBm @54Mbps

● 5.18~5.32 GHz

20 dBm @6~36Mbps

16 dBm @48Mbps

15 dBm @54Mbps

● 5.52~5.70 GHz

19 dBm @6~24Mbps

17 dBm @36Mbps

15 dBm @48Mbps

14 dBm @54Mbps

● 5.745~5.825GHz

18 dBm @6~24Mbps

16 dBm @36Mbps

14 dBm @48Mbps

13 dBm @54Mbps

● 2.412~2.472 GHz (IEEE802.11g)

25 dBm @6~24Mbps

23 dBm @36Mbps

22 dBm @48Mbps

21 dBm @54Mbps

● 2.412~2.472 GHz (IEEE802.11b)

25 dBm @1~11Mbps

RF Connector

2 x N-type (WLAN1 / WLAN2)

Operating Mode

WLAN1

Backhaul mode

WLAN2

AP mode

Auto Channel Selection

Yes

WLAN Security

WEP-64/128, WPA, WPA2

Hide SSID

Yes

System

Management

- HTTP / HTTPS/ SSH
- Windows Management Utility
- SNMP v2c/v3
- Firmware upgrade via utility/HTTPS
- Syslog

Windows Management Utility Features

- MESH AP discovery
- MESH AP status
- MESH AP setup, upgrade, reboot
- User status, activity

System Operating Mode

- Gateway
- Relay*

*Remark: In Relay mode, Ethernet functionality will be disabled except power feeding

WAN Connection Type (Gateway mode)

- Fixed IP
- PPPoE
- DHCP client

Security

- Authentication:
 - 802.11i (WPA, WPA2)
 - 802.1x (including EAP-TLS/TTLS)
- Encryption: Open, WEP-64/128, TKIP, AES
- MAC address access control list
- 802.1Q VLAN Support
- MSSID Support in client access mode
- VPN pass-through

- Hidden SSID

- HTTP login

- HTTPS login

QoS

- WMM
- Bandwidth control

Networking Standard Protocol / Standard

- IEEE 802.3 (Ethernet)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.11a (5GHz WLAN)
- IEEE 802.11b/g (2.4GHz WLAN)
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 1034, 1035 DNS
- RFC 1058 RIP
- RFC 1119 SNTPv2
- RFC 1541 / 2131 / 3046 DHCP client / Server
- RFC 1631 NAT
- RFC 2068 / 2616 HTTP
- RFC 2516 PPPoE
- RFC 2865,2866 RADIUS

General

Dimension

TBD

Weight

TBD

Power Connector

1 x Proprietary Ethernet / Power connector with water proof

Power Requirement

48V DC, 0.375A (proprietary PoE)

Environmental Protection Rating

IP 68

Environmental Specification

Operating Temperature: -20 ~ 70 Degree C

Storage Temperature: -30 ~ 80 Degree C

Relative Humidity: 0 ~ 90% non-condensing

Regulatory Compliance

FCC Part 15 B & C, R&TTE Directive 1999/5/EC, EN 300 328, EN 301 489, EN 60950

Appendix E – FCC Interference Statement

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 the 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 of the following measures:

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix F – Index

8

802.11b, 74
802.11g, 78
802.1x, 5, 20, 35, 37, 84

A

Access Control, 71
Ad-hoc, 7, 71
antennas, 4, 5, 9
Applications, 6
Auto IP, 11, 12, 13, 32

B

backhaul, 4
Beacon Period, 19, 36

C

Captive Portal, 54
Certificate, 31, 48, 52, 53

D

DDNS, 22, 26, 27
Default Gateway, 10, 26
DHCP Connection, 23
DHCP Server, 21
DHCPD, 13, 21
DMZ, 73, 74
DNS, 10, 22, 26, 64, 74, 84
DTIM, 18, 19, 36
Dynamic DNS, 26, 27, 28, 29, 30, 74
Dynamic IP Address, 22, 23

E

Encryption Key, 19, 20
ESSID, 19, 36, 63

F

FCC Interference Statement, 85, 86
Features & Benefits, 4
Firewall, 11, 18, 28, 29, 74
Firmware Upgrade, 47, 50
Fragment Threshold, 19, 36
Frequency, 19, 78, 83
FTP, 26, 75, 76, 81

G

Gigabit, 75
Glossary, 71

Ground Cable, 5

H

H.323, 75
Hardware Installation, 9
HTTPD, 11, 47
https://, 10
Hysteresis, 34

I

Ifconfig, 11, 59
Infrastructure, 7, 76
Interface Status, 63
IP Address Configuration, 22
IPSec, 31, 52, 64

L

L2TP, 31, 77
LED, 77
Logging In, 10

M

MAC Address Filter, 37, 38
Mast / Wall Mounting, 9
Mast Mounting, 67
MESH Interface, 32, 63
Mobile IP, 8, 11, 40, 41, 62, 64, 65
MPR, 34
MSSID, 35, 84
MTU, 77

N

NAT, 4, 11, 18, 27, 28, 29, 39, 78, 84
NIC, 78
NTP, 11, 18, 30, 64, 78

O

OLSR, 4, 32, 34, 64
Operation Mode, 12, 13

P

Package Contents, 5
Ping, 11, 59, 78
PoE injector, 5
POP3, 55, 79
power adapter, 5, 9
PPPoE, 22, 23, 24, 26, 64, 79, 84
PPTP, 77, 79
PPTP Server, 11, 40

Q

QoS, 44, 79

R

RADIUS, 11, 20, 54, 55, 56, 79, 84
Reboot, 17
Restore Configuration from a File, 17
Restore to Factory Defaults, 16
Route Watchdog, 40, 42
Routing, 4, 11, 32, 33, 79
RSA, 52, 79
RTS Threshold, 19, 36

S

Safety, 5
Services Status, 64
SIP, 80
SNMP, 4, 5, 11, 47, 48, 49, 51, 52, 64, 77, 80, 84
Specifications, 83
SPI, 80
SSHD, 11, 40, 43, 64
SSID, 19, 36, 80
Static IP address, 22
Static Routing, 32
SysLog Server, 11, 50
System Backup, 12, 16
System Log Status, 66
System Requirements, 6
System Status, 62

System Watchdog, 11, 40, 43

T

TFTP, 11, 59, 60, 61, 81
Topology Status, 65
TOS, 34
Traffic Shaping, 11, 40, 42
Transmission Rate, 36
Transmit Power, 19

U

Users Database, 11, 54, 56
Users Status, 65

V

Visibility Status, 36
VLAN Tagging, 24
VPN, 5, 11, 18, 31, 76, 79, 81, 84

W

Wall Mounting, 68
WAN Settings, 22
WDS, 82
Webspace, 54, 57
WEP, 19, 20, 36, 37, 82
Wi-Fi Mesh Networks, 7, 8
Willingness, 34
WLAN Configuration, 18
WMM, 5, 11, 44, 45, 46, 84
WPA Security, 20
WPA Type, 20, 37

X

X.509, 52

Z

Zero Config, 11, 12, 14