

MNG6448
Outdoor Mesh Network Node
User's Manual

Copyright

Nitek reserves the right to change or amend this manual at its sole discretion. You may not duplicate the content of this manual without the written permission of Nitek. This manual contains no implicit or implied warranties as to the usability of the product for your particular application.

About the manual

The purpose of this manual is to provide installation instructions for installing the wireless Mesh unit. This manual is including proposed actions and methods and helping the customer to solve the unpredictable problem. Each installation is different and should be performed by a qualified Technician.

The following graphical conventions are used in this Manual.



Notice: Indicates an important point



Warning Indicates a warning or caution

System Requirement

Two PCs with RJ-45 connector NIC supporting the transfer rate of 10/100Mbps data.

The IP address of NIC should be the same subnet with the AP, the default IP address of AP is 192.168.1.1.

Microsoft Internet Explorer 6 updated with Service Pack 1 or the newer patch Q323308.

Content

Chapter 1 Introduction	
Introduction	4
Network Construction	4
Chapter 2 System Installation	
Items Included in Kit	5
Hardware Installation	5
Chapter 3 System Setup	
Default Setting	6
Using the Web Management	7
Information Page	8
Set the Basic Configuration	9
WAN / LAN Settings	10
Radius Settings	12
HTTP Redirect	13
Firewall Settings	14
Virtual Server.....	15
Chapter 4 Wireless Setup	
Basic Settings.....	16
VAP/VLAN Settings / 802.1Q VLAN Setup in AP Mode	17
Security Profile for VAP 1 Configuration	18
Access Control	20
Advanced Settings	21
Chapter 5 Tools	
Site Survey	22
Link Test.....	22
Chapter 6 Management	
View the General Information	24
View the Device's Link Status	25
Change Password	25
Remote Management.....	26
Upgrade Firmware.....	27
Backup/Restore Settings.....	27
Restore to Factory	27
Event Log	28
Reboot AP	28
Chapter 7 Troubleshooting	
FAQ	29
Glossary	30

Chapter 1 Introduction

Introduction

MNG6448 is a high performance wireless MESH network node unit. The wireless node unit can self-configure, scan the network, and can repair network failures automatically so that the overall performance and the usability achieves the optimization. This unit makes use of an advance algorithm to enhance throughput and lower the time from the center to the edge of the network.

Network Construction

Figure 1 below shows a common construction for a wireless system. Units A, B, C and D are the MESH Node units. The Mesh structure allows data to be sent from group 1 to group 3 directly or indirectly as needed. The Mesh system allows you to construct a wireless network which can reach around buildings and over obstacles.

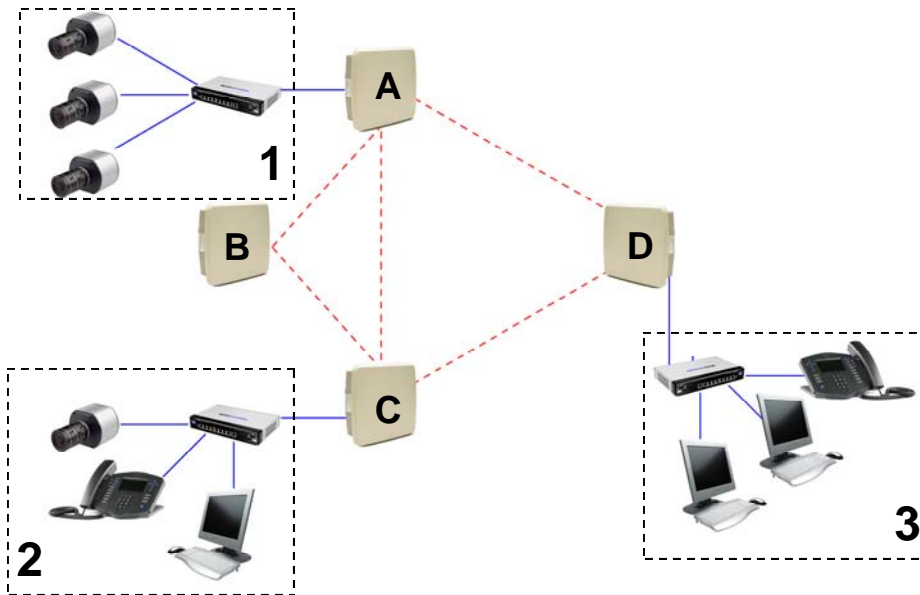


Figure 1 Mesh Structure

Chapter 2 System Installation

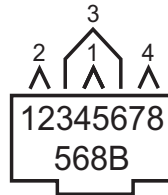
Items Included in Kit

- (1) MNG6448 MESH RADIO UNIT
- (1) PoE (48V, 1A)
- (1) Mounting Hardware Accessory
- (1) Quick Start Manual
- (1) Product CD

Hardware Installation

1. Put an Ethernet cable with RJ-45 connector through the water-tight joint. Make the RJ-45 connector as a 568B wiring configuration:

Terminal	Wire
1	Orange/White
2	Orange
3	Green/White
4	Blue
5	Blue/White
6	Green
7	Brown/White
8	Brown



2. Using the hardware provided mount the Mesh unit in position. Make sure that the antenna connection is facing down. Keep in mind that the antenna cable needs to be as short as possible for maximum performance. Refer to separate mounting guide sheet for illustrations of hardware assemble.

3. Plug water-tight joint side of the Ethernet cable into the Mesh unit. Connect the other end of the cable to the power injector supplied with the unit. Also connect a standard RJ-45 network cable for the power injector to a hub or a terminal.

3. There is a ground connection on the Mesh unit located near the antenna port. The ground connection should be connected to a proper earth ground point.

4. Mount the external antenna for the Mesh unit. It is recommended that the antenna cable be as short as possible. 3 feet would be the most common length. Due to the limited RF power of the Mesh unit any added cable length will lower the maximum system range.



Warning Do not mount Mesh unit or antenna near electric power lines, electric lights or near strong electric power signals

5. Power the unit using the supplied POE inserter.

Chapter 3 System Setup

Default Setting

Diagram 1 Default Settings

User Name	admin
Password	password
Access Point Name	APxxxxxx (xxxxxx indicate the last 6 MAC address of Wireless B)
Country/Region	United States
Ethernet Data Rate	Automatic
IP Address	IP Type: STATIC IP Address : 192.168.1.1 Mask : 255.255.255.0 Gateway: 0.0.0.0 Primary DNS Server: 0.0.0.0 Secondary DNS Server: 0.0.0.0
Country/Region	Taiwan
Wireless Mode	802.11b/g
Data Rate	Best
Output Power	Full
RTS Threshold	2346
Fragmentation Threshold	2346
Wireless Space	10000
Enable Refuse XDos	No
Security Settings	Disable
Current Channel	11
Default Channel	11 / 2.462GHz
Link Test	Local MAC:00:1C:24:xx:xx:xx RF Cable Lose: 2dB Local Antenna Gain: 23dBi Remote Antenna Gain: 23dBi Test Interval: 50ms Test Packet Size: 64byte Test Time: 300s
SNMP Settings	SNMP: Enable Trap Server: 0.0.0.0 Read Community: public Write Community: private

Using the Web Management

Refer to the Quick Start Guide for basic installation configurations

The Web Management provides you with a user-friendly graphical interface. The Mesh unit allows a web browser (MS Internet Explorer 6.0) to monitor and configure the unit.

1. While running a Web Browser, Enter default IP Address: **http://192.168.1.1** in the Address field. After press Enter key you may get a pop up security alert page, the page will show up. If it does click yes button, the login



Figure 3 Security Alarm

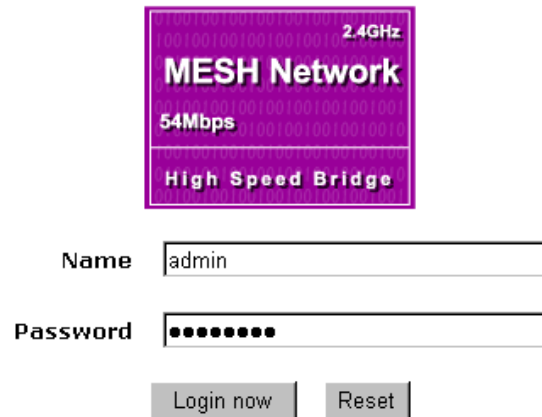


Figure 4 Login

2. Enter default User Name: **admin** and default Password: **password**, then click Login. The home page will show up.

Information Page

MESH Network
2.4GHz
54Mbps
High Speed Bridge
[Logout]

Status
[Information](#)
[Connections](#)
[Statistics](#)

System Setup
[Basic Settings](#)
[IP Settings](#)
[RADIUS Settings](#)
[HTTP Redirect](#)
[Firewall Settings](#)
[Virtual Server](#)

Wireless Setup
[Basic Settings](#)
[VAP/VLAN Settings](#)
[Access Control](#)
[Advanced Settings](#)

Tools
[Site Survey](#)

Information

Access Point Information

Access Point Name	AP400113
MAC Address	00:1c:24:40:01:13
Country / Region	Taiwan
Firmware Version	7.0.0.5

Current IP Settings

Router Mode	Bridge
IP Type	static IP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

Current Wireless Settings

Operating Mode	Access Point
Wireless Mode	Auto (11g/11b)
Channel / Frequency	11 / 2.462GHz
Wireless Bandwidth	20MHz

Security Profiles

No.	Profile Name	SSID	MAC	Security	VLAN	Status
1	AP_Profile1	Wireless	00:1c:24:40:01:13	Open System		Enable
2	AP_Profile2	Wireless	06:1c:24:40:01:13	Open System		Disable
3	AP_Profile3	Wireless	0a:1c:24:40:01:13	Open System		Disable
4	AP_Profile4	Wireless	0e:1c:24:40:01:13	Open System		Disable
5	AP_Profile5	Wireless	12:1c:24:40:01:13	Open System		Disable
6	AP_Profile6	Wireless	16:1c:24:40:01:13	Open System		Disable
7	AP_Profile7	Wireless	1a:1c:24:40:01:13	Open System		Disable
8	AP_Profile8	Wireless	1e:1c:24:40:01:13	Open System		Disable

[Refresh](#)

Figure 5 Information Page

The Information Page displays general information about the Mesh unit.

Set the Basic Configuration

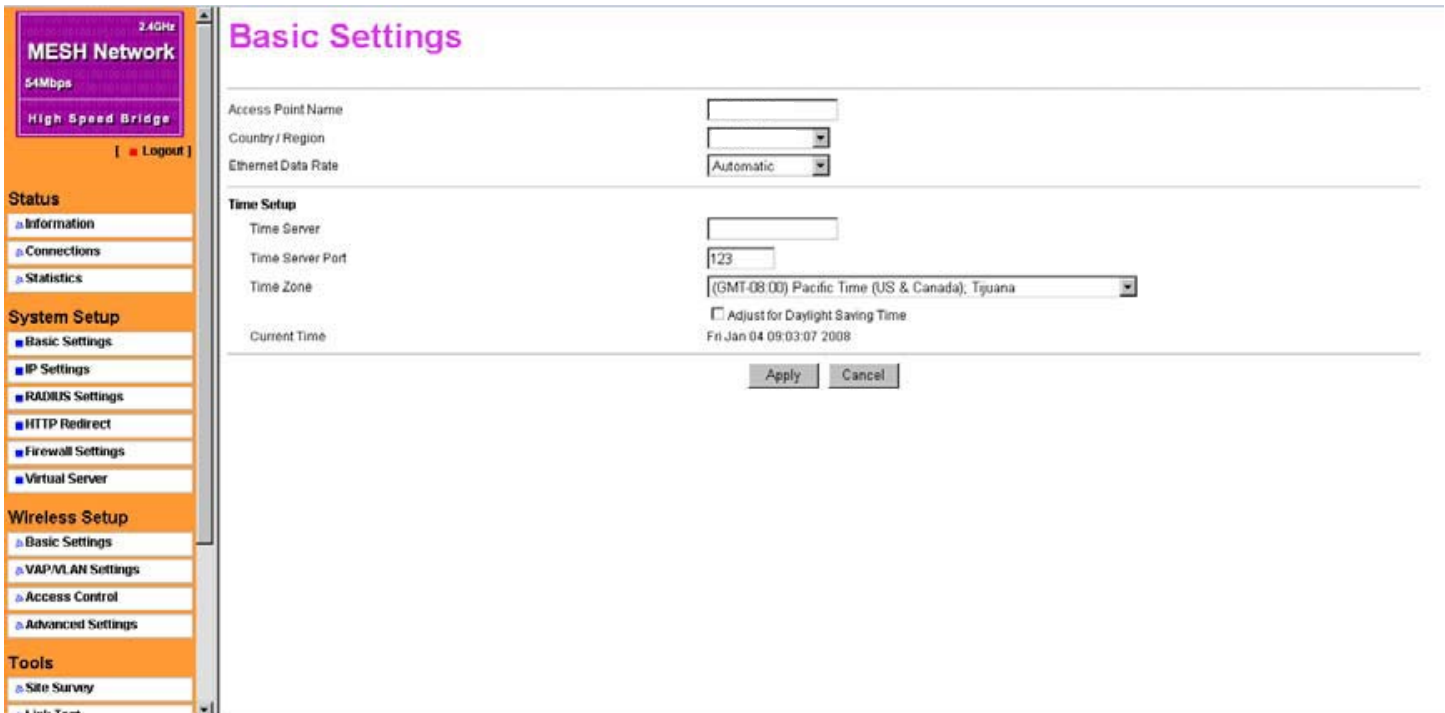


Figure 6 Basic setup

Access Point Name

This is the NetBIOS name of Mesh Unit; you may modify the default name with a unique name up to 15 characters long including numbers from 0 to 9, letters (A-Z; a-z) and dash (-). The name supports WINS so you can ping Mesh Unit using “ping Mesh Unit Name” or use web browser to open web utility by inputting Mesh Unit Name in the IE address.

The default Mesh Unit Name is: APxxxxxx (xxxxxx represents the last 6 digits of MAC address)

The first character of Mesh Unit Name cannot be digits 0 to 9.

Your host must have a TCP/IP address with the same subnet as the Mesh Unit to use WINS.

Country/Region

Select your country or region from the drop-down list. This field displays countries/regions of operation. It is important that you select the proper country of operation. For example: If you chose Russia, but in fact you are in USA, so the operating frequency band and output power might not be consistent with related regulations of the USA.

Ethernet Data Rate

The specifies the Ethernet port's data rate. Automatic is recommended.

IP Address

Static IP: You should manually configure IP address, subnet mask, and the gateway. The Mesh Unit will automatically calculate the subnet mask based on the assigned IP address. Otherwise, you can use 255.255.255.0 as the subnet mask.

DHCP: The Mesh Unit can get IP settings from DHCP Server but Static IP is recommended.

IP Settings

From the system setup, click IP Settings, you'll be navigated into the WAN/LAN Settings.

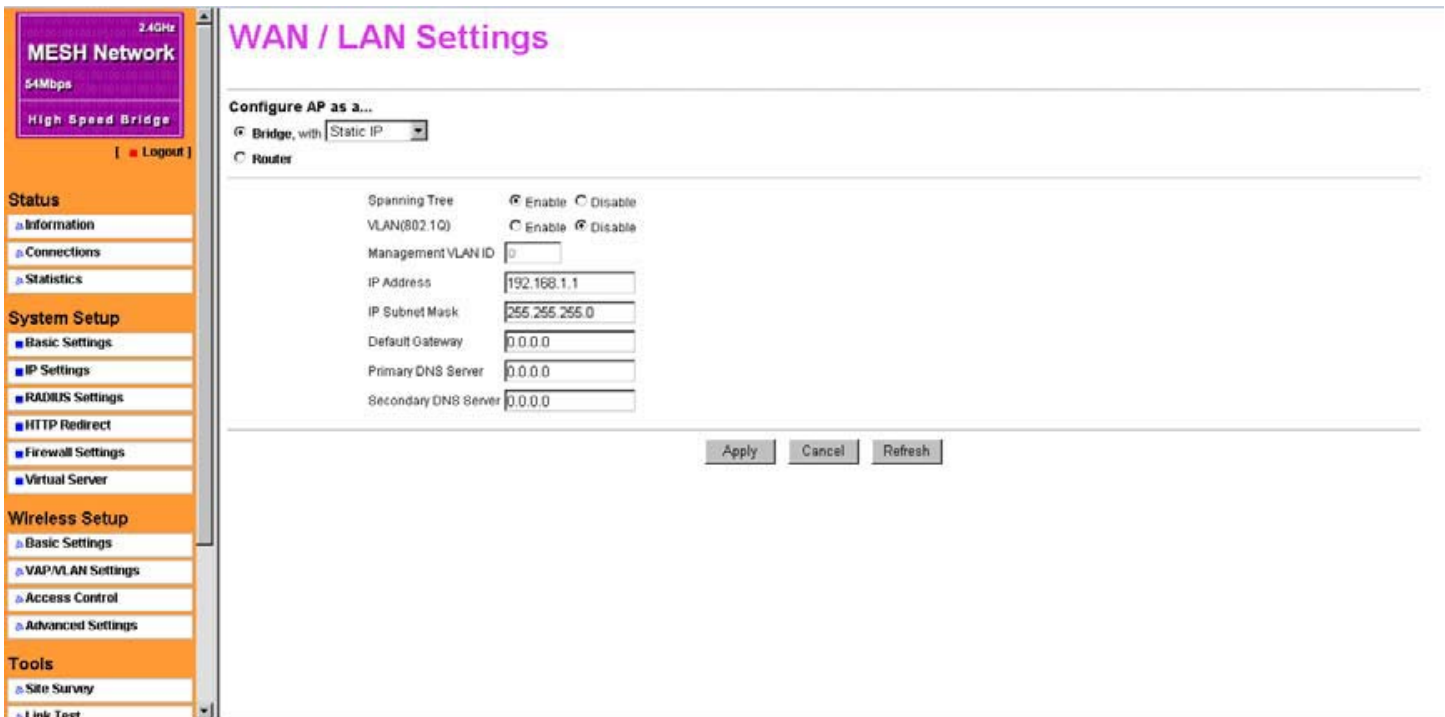


Figure 7 WAN / LAN Settings

Bridge Mode

Bridge Mode: In this mode it will act as a pass-through bridging your network, by associating with various devices. This can extend your radius of your network.

Spanning Tree: Enabling spanning tree can prevent undesirable loops in the network, ensuring a smooth running network. By default, the function is enabled.

Router Mode

The Mesh Unit can function as a router, connecting two distinct networks.

Under the bridging mode, two modes are available, WAN at Ethernet Port and WAN at Wireless Port. You can choose either mode. Under the Access Point mode, it acts as a Router. In general, WAN is designed at the Ethernet port and LAN at the wireless port.

Intentionally Blank

Radius Settings

MESH Network
2.4GHz
54Mbps
High Speed Bridge
[Logout]

Status
Information
Connections
Statistics

System Setup
Basic Settings
IP Settings
RADIUS Settings
HTTP Redirect
Firewall Settings
Virtual Server

Wireless Setup
Basic Settings
VAP/VLAN Settings
Access Control
Advanced Settings

Tools
Site Survey
Link Test

RADIUS Settings

Authentication/Access Control RADIUS Server Login

Primary IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Secondary IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Advanced WPA / 802.1X Parameters

Reauthentication Time: 3600 Seconds
 Global-Key Update
 every 3600 Seconds
 every 1000 X1000 Packets
 Update if any station disassociates

Accounting RADIUS Server Login

Primary IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

Secondary IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

Apply Cancel

Figure 8 Radius Settings

RADIUS (Remote Authentication Dial-In User Service) plays a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing and alarming...etc and allows an organization to maintain user profiles in a central database that all remote servers can share. Since RADIUS is relatively complex to explain, we will focus here on how it acts as an 802.1x authentication server (EAP-aware RADIUS) and assists in enhancing security in Access Point mode.

RADIUS performs the authentication function required to check the credentials of users and intermediate Mesh Units and indicates whether the users are authorized to access the Mesh Units. Enabling RADIUS is therefore the first step toward building up an 802.1x-capable environment. It is also a must-do to accommodate the recently introduced Wi-Fi protected access (WPA-EAP) to wireless networks.

Authentication/Access Control RADIUS Server Configuration: This configuration is required for authentication using RADIUS. IP Address, Port No. and Shared Secret is required for communication with RADIUS Server. A Secondary RADIUS Server can be configured which is used on failure on Primary RADIUS Server.

IP Address: IP address of the RADIUS Server. Default is 0.0.0.0

Port Number: Port number of the RADIUS Server. Default is 1812.

Shared Secret: This is shared between the Wireless Access Point and the RADIUS Server for authenticating the supplicant.

Reauthentication Time: The time interval in seconds after which the supplicant will be authenticated again with the RADIUS Server.

Global-Key Update: A check in this option will enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key.

Update if any station disassociates: A check in this option will refresh global key when any stations disassociated with wireless Mesh Unit.

Accounting RADIUS Server Configuration: This configuration is required for accounting using RADIUS Server. IP Address, Port No. and Shared Secret is required for communication with RADIUS Server. A Secondary RADIUS Server can be configured which is used on failure on Primary RADIUS Server.

IP Address: IP address of the RADIUS Server. Default is 0.0.0.0

Port Number: Port number of the RADIUS Server. Default is 1813.

Shared Secret: This is shared between the Wireless Mesh Unit and the RADIUS Server while authenticating the supplicant.

HTTP Redirect

This enabling HTTP Redirect. By entering the company or origination website (for example, <http://www.nitek.net>). That website will appear first when someone is surfing on internet, via a station connected to your Mesh unit.

HTTP Redirect Settings: Enter the desired website in the URL field. Then click “**Apply**” to save the configuration. The Mesh Network must have internet access to use HTTP Redirect.

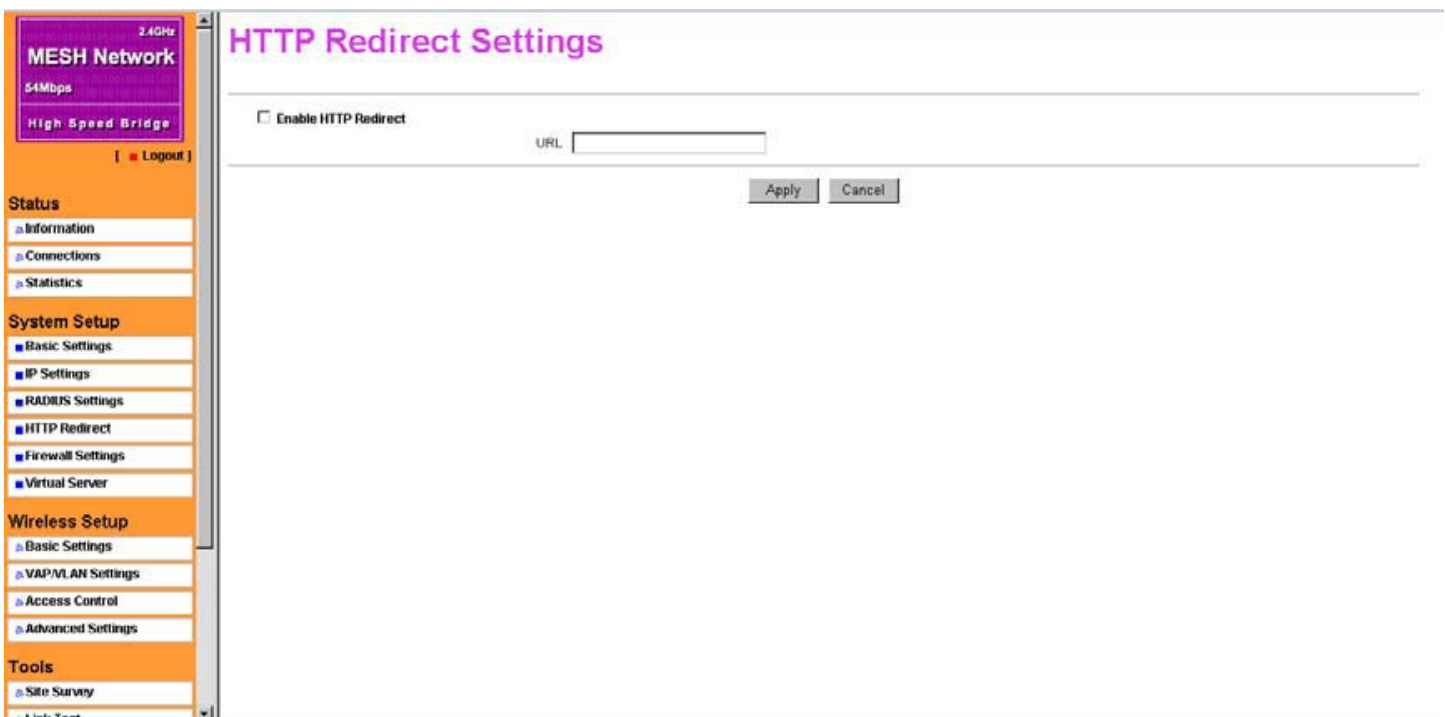


Figure 9 HTTP redirect setting

Firewall Settings

Firewalls are configured to allow “desired” traffic in and to keep “undesired” traffic out. The BRIDGE access point is also qualified for firewall management. Acting as a firewall, the Mesh unit will filter your undesired data and protocols, only delivering the “wanted” data to your PC. Click on the firewall link to display Firewall Management interface.

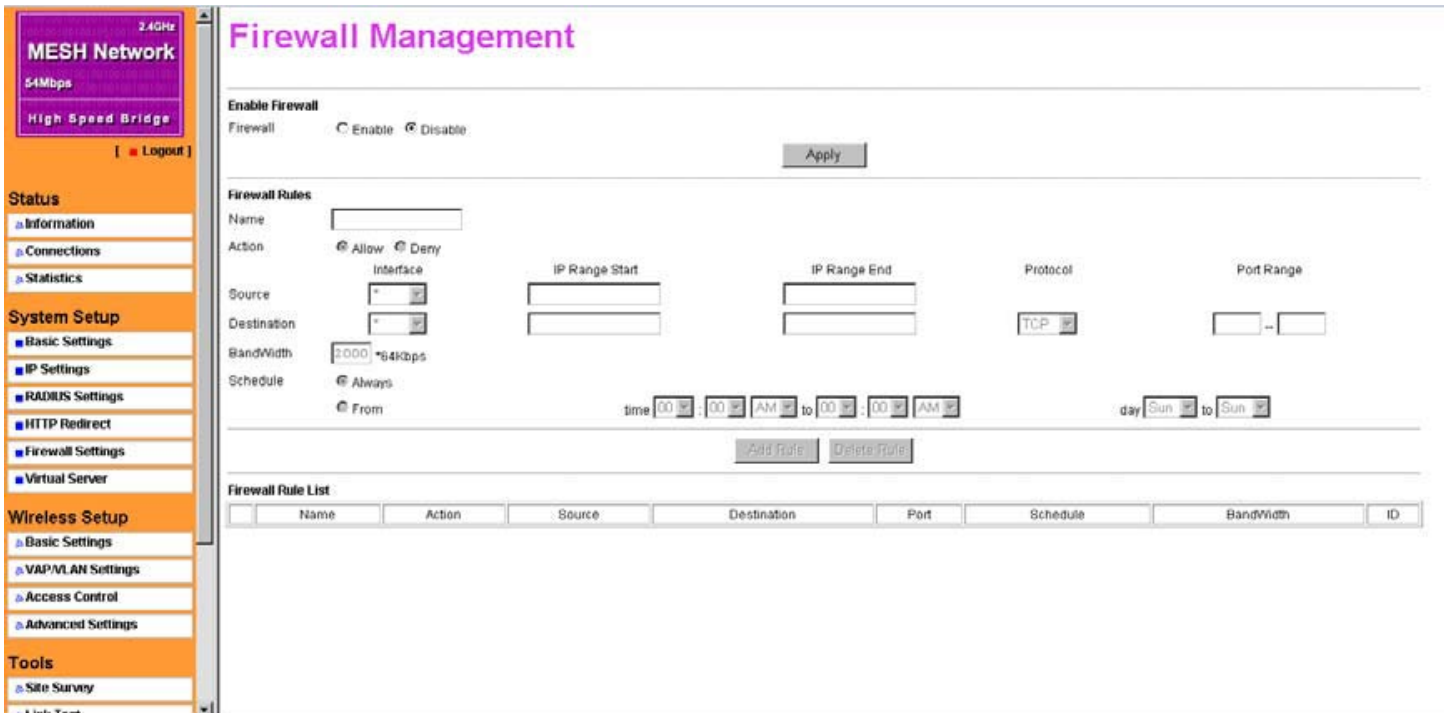


Figure 10 Firewall management

Enable Firewall: The firewall must first be enabled. Check “**Enable**” and click Apply.

Name: Enter a name for the firewall rules in the name field.

Action: **Allow** identifies which IP addresses, are allowed to transmit on the LAN.
Deny identifies which IP addresses, are banned from transition on the LAN.

Interface: This is optional, WAN or LAN.

Destination: This specifies where packets are bound for.

IP Range Start: This specifies the starting-point of your specific IP addresses.

IP Range End: This specifies the ending-point of your specific IP addresses.

Protocol: This is optional, TCP, DCP, ICMP or *. Select which protocol will perform “Allow” or “Deny”.

Port Range: This specifies your IP port range.

Schedule: Allow setting a time when the Mesh unit performs firewall management, by enabling “from” option. “Always”, sets the Mesh unit to perform firewall management permanently.

Virtual Server

Virtual server can be enabled only under Router mode.

In the Access Point mode the Mesh unit acting as a virtual server for heterogeneous network. In the Router mode the Mesh Unit is wirelessly coupled to FTP server, mail server and log server on LAN port; on WAN port, the Mesh unit is coupled to PC. The Mesh unit is the virtual server, so that you have access to download files or get e-mail.

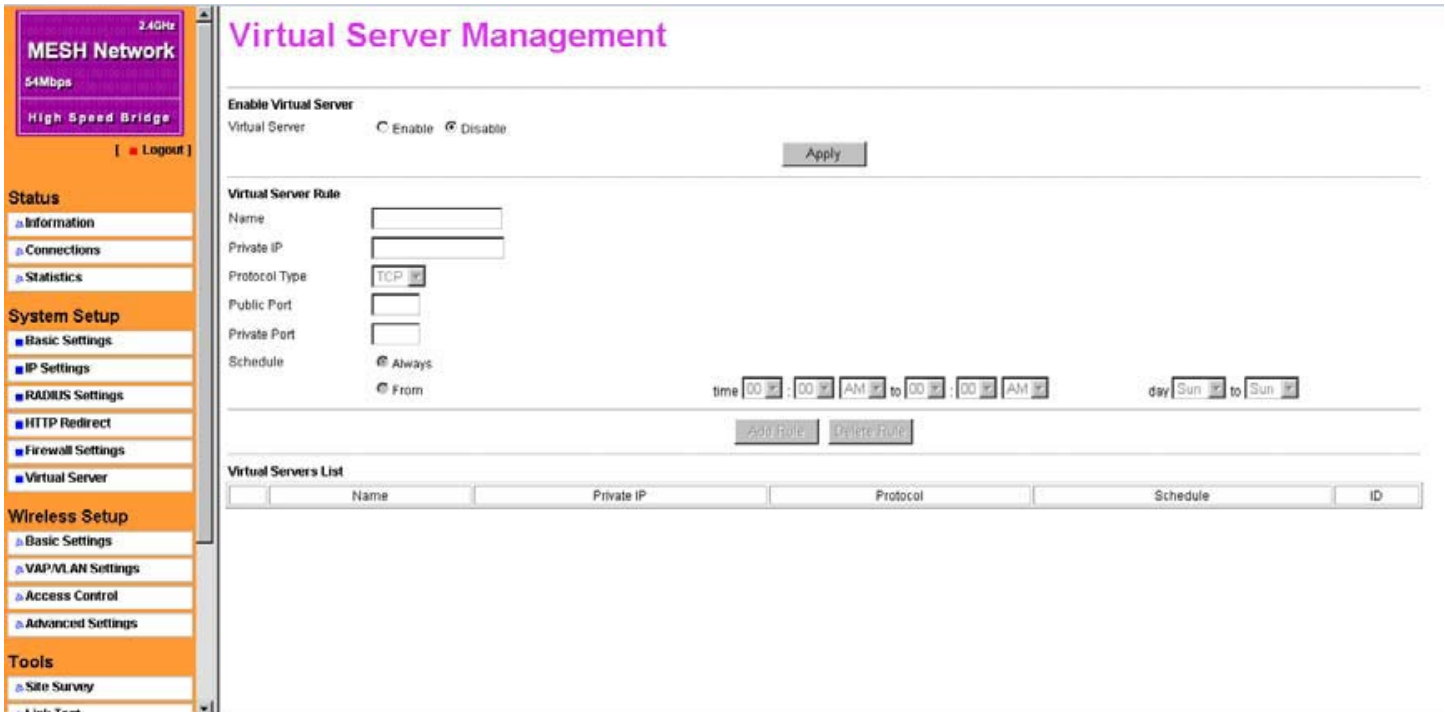


Figure 11 Virtual server

Enable Virtual Server: The Virtual Server must first be enabled. Check “**Enable**” and click Apply.

Name: Enter a name for the Virtual Server.

Private IP: This specifies the IP Address for the LAN.

Protocol Type: This field is optional. TCP or UDP.

Private Port : This specifies your LAN port.

Public Port : This specifies your WAN port.

Schedule: Allow setting a time when the Mesh unit acts as a virtual server, by enabling “from” option. “Always”, sets the Mesh unit to act as a virtual server permanently. When configuration of the virtual server, is completed please click “Add Rule” to save the setting.

Virtual Server List : This provides you with a detailed list of virtual servers.

Chapter 4 Wireless Setup

Basic Settings



Figure 12 Mesh Setting

Operating Mode: Select the operating mode as Mesh Network Enable the mesh function.

Channel / Frequency: The channel which the mesh point currently working on.

Channel	Frequency
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437

Channel	Frequency
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467

Diagram 3 Channel/Frequency List (2.4GHz)

VAP/VLAN Settings / 802.1Q VLAN Setup in AP Mode

In Access Point mode, you could enable 802.1Q VLAN to manage users, You could select one profile to edit as follows:

VAP / VLAN Settings

Security Profiles for Vap, Station Adapter, WDS and Inter Building mode

#	Profile Name	SSID	Security	Enable
1	AP_Profile1	Wireless	Open System	<input checked="" type="checkbox"/>
2	AP_Profile2	Wireless	Open System	<input type="checkbox"/>
3	AP_Profile3	Wireless	Open System	<input type="checkbox"/>
4	AP_Profile4	Wireless	Open System	<input type="checkbox"/>
5	AP_Profile5	Wireless	Open System	<input type="checkbox"/>
6	AP_Profile6	Wireless	Open System	<input type="checkbox"/>
7	AP_Profile7	Wireless	Open System	<input type="checkbox"/>
8	AP_Profile8	Wireless	Open System	<input type="checkbox"/>
	Mesh_profile			<input checked="" type="checkbox"/>

VLAN (802.1Q) Setup

1. AP_Profile1 VLAN ID:

2. AP_Profile2 VLAN ID:

3. AP_Profile3 VLAN ID:

4. AP_Profile4 VLAN ID:

5. AP_Profile5 VLAN ID:

6. AP_Profile6 VLAN ID:

7. AP_Profile7 VLAN ID:

8. AP_Profile8 VLAN ID:

Figure 13 802.1Q VLAN

One device could be used to eight devices. So you could easy setup your network and manage different users. And the eight VAP could set different security to protect your network.

Management VLAN ID: Management VLAN ID is used to manage device and monitor the network.

Security Profile VLAN ID: Security Profile VLAN ID is used to manage VLAN. You could set ID 1~4049.

Security Profile Settings following steps below:

Security Profile for Vap 1 Configuration

MESH Network
2.4GHz
54Mbps
High Speed Bridge
[Logout]

Status
Information
Connections
Statistics

System Setup
Basic Settings
IP Settings
RADIUS Settings
HTTP Redirect
Firewall Settings
Virtual Server

Wireless Setup
Basic Settings
VAP/WLAN Settings
Access Control
Advanced Settings

Tools
Site Survey
Link Test

Security Profile for Vap 1 Configuration

Profile Definition
Security Profile Name: AP_Profile1
Wireless Network Name (SSID): Wireless
Broadcast Wireless Network Name (SSID): Yes No

Network Authentication: Open System

Data Encryption: None

Passphrase:

Key 1:
Key 2:
Key 3:
Key 4:

Wireless Client Security Separation Enable Disable

Figure 14 Security profile

Security Profile Name: Allows you to name to manage different VAP configurations.

Wireless Network Name (SSID): The SSID is a unique ID used by Mesh units, Access Points, and Stations to identify a wireless LAN. Wireless clients associating to any Mesh unit must have the same SSID. The default ESSID is “Wireless”. The ESSID can up to 32 characters

Broadcast Wireless Network Name (SSID): By hiding the SSID, the device cannot be seen when a wireless client scans for local wireless units. The trade-off for the extra security of “hiding” a device may be inconvenience for some valid WLAN clients.

Authentication Type: Choose from the following types.

Open System: Allow any wireless NIC or wireless bridge to connect.

Shared Key: If Shared Key is selected, you need to enabled WEP and enter at least one shared key.

802.1x: IEEE 802.1x is a standard for network access control (port based), which was introduced especially for distributing encryption keys in a wireless network. The Mesh unit supports 802.1x for keeping out unauthorized users and for verifying the credentials of users with RADIUS so that authorized users can access the network and services. To use 802.1x, you will need at least one common Extensible Authentication Protocol (EAP) method on your authentication server, Access Points (authenticator) and stations (supplicant). 802.1x is also used to perform generation and distribution of encryption keys with enabling Data Encryption as WEP from the Access Point to the station as part of or after the authentication process.

WPA with Radius, WPA2 with Radius, WPA & WPA2 with Radius: In cooperation with RADIUS, systems with WPA-EAP will be used with a new encryption method called Temporal Key Integrity Protocol (TKIP) implementation with 802.1x dynamic key exchange.

WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK: Instead of using RADIUS for authentication, systems with WPA-PSK will be configured with a secret password phrase. Enter your password phrase and press “Generate”. You can now create a pre-shared key in the Access Point and copy the characters you input to the station's WPA-PSK entry. A shared secret is only secure as long as no third party knows about it.

You must configure RADIUS Server Settings with either Legacy 802.1x or WPA with RADIUS option.

Data Encryption: Select the desired option, if enabled, the keys must be entered, and other wireless stations or bridge must use the same keys. The default is None.

Options are:

None

WEP 64 bit: 10 Hexadecimal digits (any combination of 0-9, a-f, or A-F)

WEP 128 bit: 26 Hexadecimal digits (any combination of 0-9, a-f, or A-F)

WEP 152 bit: 32 Hexadecimal digits (any combination of 0-9, a-f, or A-F)

TKIP: Automatically enabled with either WPA with RADIUS or WPA-PSK authentication type is selected.


AES: Automatically enabled with either WPA2 with RADIUS or WPA2-PSK authentication type is selected.

TKIP+AES: Automatically enabled with either WPA & WPA2 with RADIUS or WPA-PSK & WPA2-PSK authentication type is selected.

Security Encryption Keys (Hex)

Pass-phrase: To use the pass-phrase for generating the keys, enter a pass-phrase and click the “**Generate Keys**” button. You can also enter the keys directly. These keys must match the other wireless stations or bridges. Only 8 to 63 characters can be entered.

Key1~~Key4: Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data. The four entries will be disabled if WPA with RADIUS authentication option is selected.

 **Notice:** The Access Point and the stations must have the same Authentication Type, Data Encryption and Key, otherwise they can not connect.

You must first set Radius parameters to use 802.1X, WPA with Radius, WPA2 with Radius, WPA & WPA2 with Radius.

Access Control

The optional Access Control window lets you block the network access privilege of the specified stations through the Mesh unit. This provides an additional layer of security. There are two kinds of ACL.

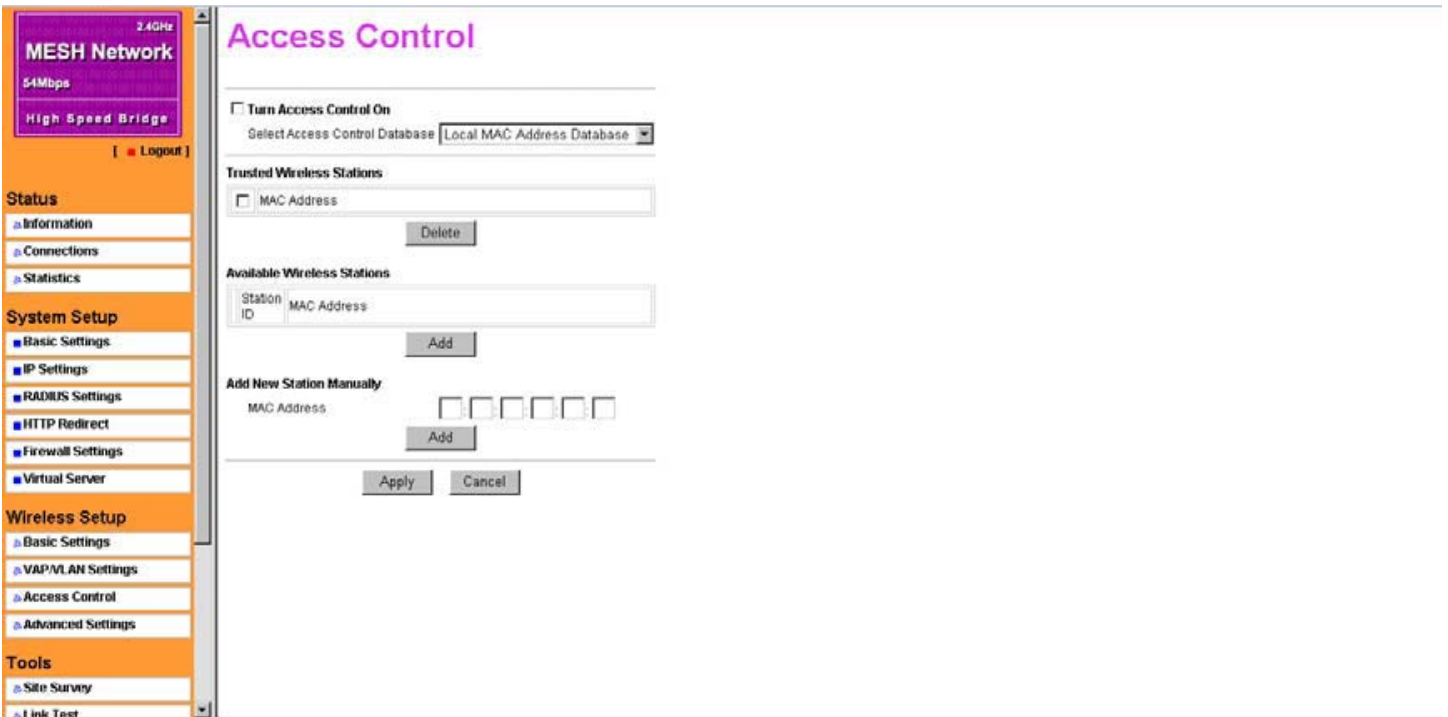


Figure 15 Access control

To enable the Local MAC Address Database, check **Turn Access Control On** and click the Apply button. Only stations in the Trust list can connect to the Mesh unit and stations in the Reject list cannot connect with the Mesh unit. To maintenance the Available Wireless Stations list, while you set Radius parameters, you could use RADIUS MAC Address Database to control stations connections.

Advanced Settings

The default advanced wireless LAN parameters is recommended but can optimize if needed by using the advanced wireless settings.

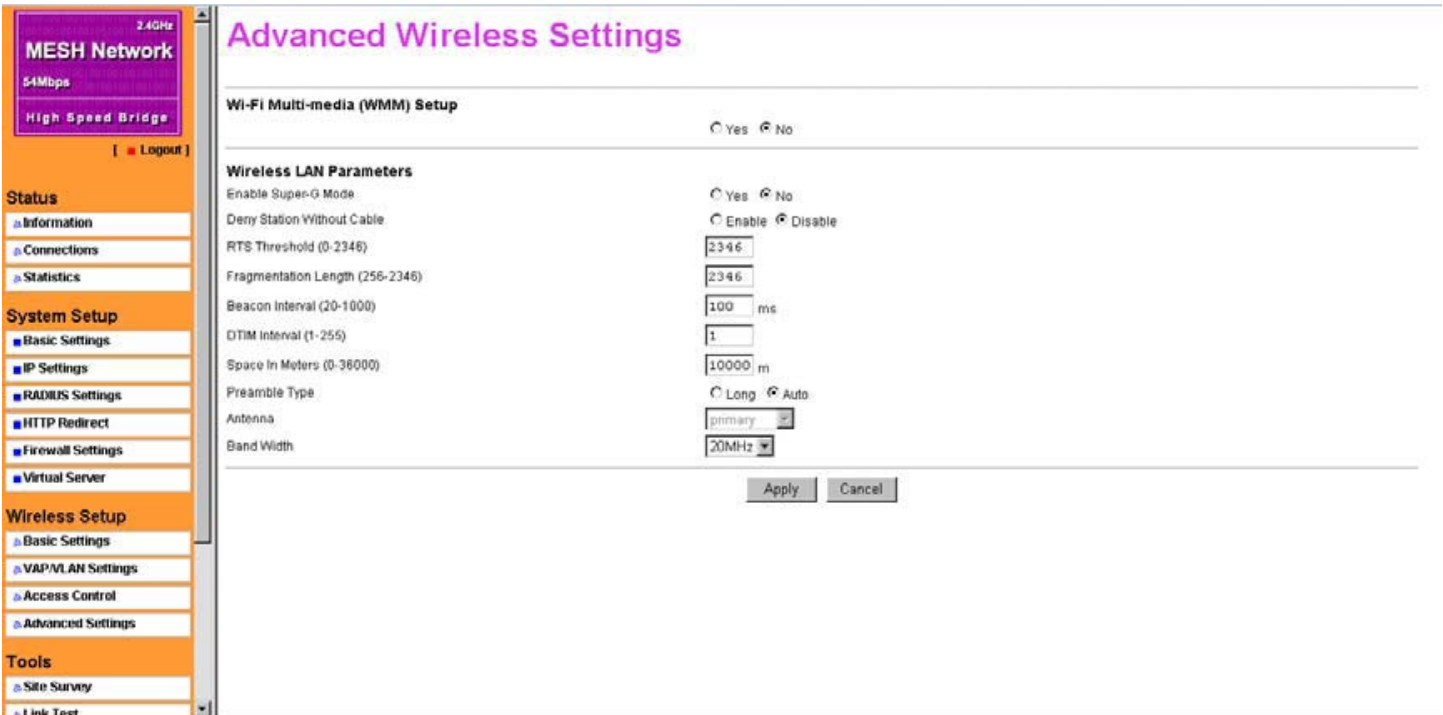


Figure 16 Advanced wireless settings

RTS Threshold: Packet size determines whether the Mesh unit uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission.

Fragmentation Length: This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

Beacon Interval: Specifies the data beacon rate between 20 and 1000 milliseconds.

DTIM Interval: The Delivery Traffic Indication Message specifies the data beacon rate between 1 and 255.

Preamble Type: Along transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better through put.

Chapter 5 Tools

Site Survey

Site Survey provides you with a table of adjacent Mesh units connected to your bridge. In terms of each connected Mesh unit, Site Survey provides unit information, including SSID, BSSID, RSSI, channel mode, connection status and encryption.

The screenshot shows the 'Site Survey' page in a web interface. On the left is a navigation sidebar with sections: Status, System Setup, Wireless Setup, and Tools. The main content area is titled 'Site Survey' and contains a table with the following data:

Index	SSID	BSSID	RSSI(dBm)	Channel	Mode	Connections Status	Encryption
1		00:18:a7:42:6c:2b	-50	1 / 2.412 GHz	802.11g only	-	Enable
2	Wireless	00:19:70:27:0:77	-49	6 / 2.437 GHz	802.11g only	-	Disable
3	TSC	00:22:b0:94:d9:3b	-66	6 / 2.437 GHz	802.11g only	-	Enable
4	Wireless	00:19:70:27:0:78	-52	6 / 2.437 GHz	802.11g only	-	Disable
5		00:24:82:31:94:d1	-42	6 / 2.437 GHz	802.11b only	-	Enable
6	PBX-AP	00:24:82:71:94:d1	-41	6 / 2.437 GHz	802.11b only	-	Enable
7		00:60:b3:35:58:85	-60	10 / 2.457 GHz	802.11g only	-	Enable

Below the table is a 'Scan' button.

Figure 17 Site survey

Link Test

The screenshot shows the 'Link Test' page in a web interface. On the left is a navigation sidebar. The main content area is titled 'Link Test' and contains configuration fields for a link test:

- Local MAC: 00:1c:24:40:01:13
- RF Cable Loss(0-10): 1 dB
- Local Antenna Gain(0-99): 15 dBi
- Remote Antenna Gain(0-99): 15 dBi
- Test Interval (1-60000): 50 ms
- Test Packet Size (64-1514): 64 byte
- Test Time (60-86400): 300 s

Below these fields is a table with the following headers:

Remote MAC	Elapsed Time	Tx Pkt Num	Rx Pkt Num	Local Signal Level	Remote Signal Level
------------	--------------	------------	------------	--------------------	---------------------

At the bottom of the configuration area are 'Apply', 'Start', and 'Stop' buttons.

Figure 18 Link test

To optimize the communication between your LAN, link test is designed to test the parameters that indicates communication quality.

RF Cable Loss: Input the value of local and remote RF Cable loss.

Local Antenna Gain: Input a value for the Local Antenna Gain.

Remote Antenna Gain: Input the value for the Remote Antenna Gain.

Test Interval: Input a value for the Send Packet Interval.

Test Packet Size: Input the value of Send Packet Size.

Test Time: Input a value for the Test Time.



Notice: For accurate test results, you should make sure that the Link Test settings are correct.

The signal strength (dBm) is a negative value, the lower the absolute value is, the better the signal strengthens. For a greater throughput in the wireless network, you should adjust the signal strength for a better signal.

The signal strength (Percent) is just a reference value. It relies on not only the real signal strength but also the academic signal strength which relies on the Link Test settings. So you should take the signal strength (dBm) as a reference when adjusting antennas.

Chapter 6 Management

View the General Information

MESH Network 2.4GHz
54Mbps
High Speed Bridge
[Logout]

Status

- Information
- Connections
- Statistics

System Setup

- Basic Settings
- IP Settings
- RADIUS Settings
- HTTP Redirect
- Firewall Settings
- Virtual Server

Wireless Setup

- Basic Settings
- VAP/VLAN Settings
- Access Control
- Advanced Settings

Tools

- Site Survey
- Link Test

Information

Access Point Information

Access Point Name: AP400113
 MAC Address: 00:1c:24:40:01:13
 Country / Region: Taiwan
 Firmware Version: 7.0.0.5

Current IP Settings

Router Mode: Bridge
 IP Type: static IP
 IP Address: 192.168.1.1
 IP Subnet Mask: 255.255.255.0
 Default Gateway: 0.0.0.0

Current Wireless Settings

Operating Mode: Access Point
 Wireless Mode: Auto (11g/11b)
 Channel / Frequency: 11 / 2.462GHz
 Wireless Bandwidth: 20MHz

Security Profiles

No.	Profile Name	SSID	MAC	Security	VLAN	Status
1	AP_Profile1	Wireless	00:1c:24:40:01:13	Open System		Enable
2	AP_Profile2	Wireless	06:1c:24:40:01:13	Open System		Disable
3	AP_Profile3	Wireless	0a:1c:24:40:01:13	Open System		Disable
4	AP_Profile4	Wireless	0e:1c:24:40:01:13	Open System		Disable
5	AP_Profile5	Wireless	12:1c:24:40:01:13	Open System		Disable
6	AP_Profile6	Wireless	16:1c:24:40:01:13	Open System		Disable
7	AP_Profile7	Wireless	1a:1c:24:40:01:13	Open System		Disable
8	AP_Profile8	Wireless	1e:1c:24:40:01:13	Open System		Disable

Refresh

Figure 19 Information

The General Information page displays current settings and statistics of your Mesh unit and is a Read only. Any settings must be changed on other pages.

View the Device's Link Status

This page displays both wired Ethernet and wireless interface network traffic. Click Refresh to update the current statistics.

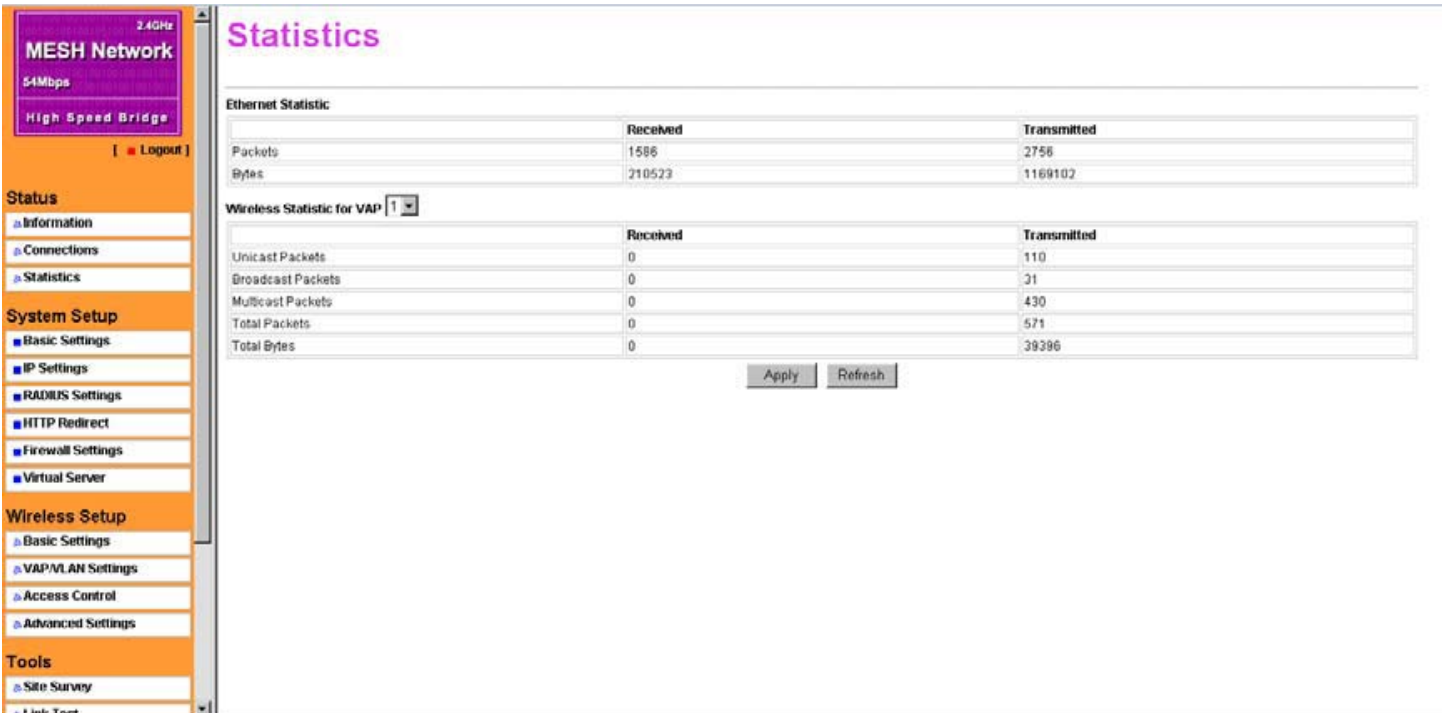


Figure 20 Statistics

Change Password

Change Password

Current Password

New Password

Repeat New Password

Restore Default Password Yes No

Apply Cancel

Figure 21 Change Password

You can use the Change Password page to change the Mesh unit administrator's password for accessing the Settings pages.

1. To change the password, first enter the old password. The default password for the Mesh unit is: **password**.
2. Then enter a new password and enter it again in the Repeat New Password box to confirm. The maximal length of the password is 19 characters.
3. Click "Apply" to have the password changed or click "Cancel" to keep the current password.
4. Be sure to write down the new password and store it in a secure location.

Remote Management

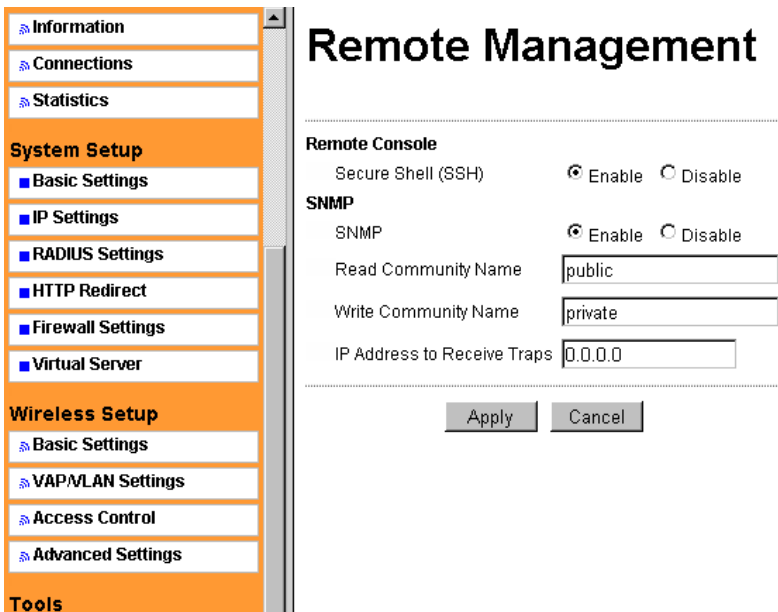


Figure 22 Remote management

The Mesh unit supports SNMP. You should first set SNMP settings and then get MIB file from Mesh unit by ftp.

1. “Enable” the Secure Shell (SSH)
2. “Enable” SNMP
3. Set the Trap Server Address
4. Set the Read-only Community
5. Set the Read-write Community
6. Click the “Apply” button to save setting

Get MIB file by ftp

1. Login to Mesh unit by ftp.
2. Input command “get mesh.mib”, you will find the MIB file in the current directory.

```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 1.1.3)
User (192.168.1.1:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files. Login successful. Have fun.
```

Figure 23 get mib

Upgrade Firmware

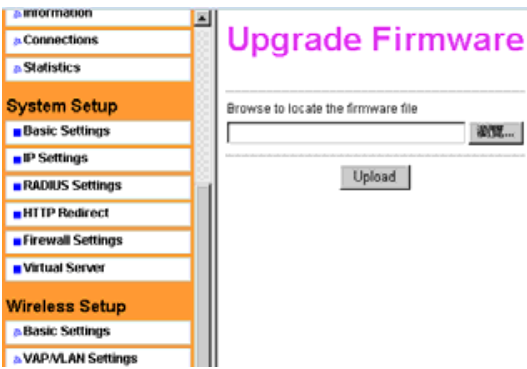


Figure 24 Upgrade firmware

1. Open Upgrade Firmware page
2. Click browse button and select the firmware file on local hard disk.
3. Click “Upload” button.
4. After upgrade, login again and check the software version.

Backup/Restore Settings

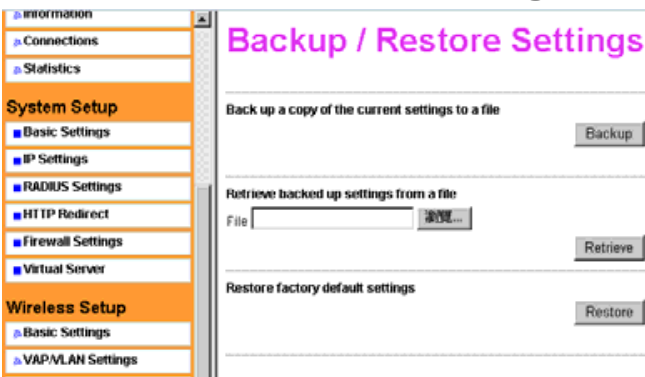


Figure 26 Backup /Restore setting

Backup

1. Select the BACKUP/RESTORE.
2. Click “Backup” button to save a cbackup file to hard disk.

Retrieve Backed up Settings

1. Select the BACKUP/RESTORE.
2. Click “Browse” button to locate the backup file you want to retrieve
3. Click “Retrieve” button, the Mesh unit will restart when complete.

Restore to Factory Default

1. Select the BACKUP/RESTORE.
2. Click “Restore” button, the Mesh unit will restart when complete.

Event Log

Event Log

Enable SysLog

Syslog Server IP Address: 0.0.0.0

Syslog Server Port Number: 514

Apply Cancel

Event Log Window

Time	Wlan	Event
Fri Dec 21 00:56:22 2007	WLAN0	00:60:B3:8E:A7:BB is ready in service.
Fri Dec 21 00:56:22 2007	WLAN0	00:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	00:60:B3:8E:A7:BB is ready in service.
Thu Dec 20 23:42:21 2007	WLAN0	1E:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	1A:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	16:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	12:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	0E:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	0A:60:B3:8E:A7:BB stop service.
Thu Dec 20 23:42:21 2007	WLAN0	06:60:B3:8E:A7:BB stop service.

Refresh Save As Clear

Figure 26 Event log

You could check system log to view the operations between the Mesh unit and the Station, such as authentication, connection.

Reboot AP

Reboot AP

Reboot access point Yes No

Apply Cancel

Figure 27 Reboot AP

By selecting Yes on “Reboot AP” page and then click on “Apply” button the Mesh unit with Reboot.

Chapter 7 Troubleshooting

Frequently Asked Questions

Q 1. How can I know the MAC address of the Mesh unit?

The MAC address is written in a label which is in the bottom of Mesh unit. Also, it is located on **Information** page of WEB configuration.

Q 2. Why the throughput is not so high?

You should adjust antenna for the highest signal strengthens.
If you cannot get a higher signal strengthens, try to changing the wireless Channel/Frequency.
Check whether there is other wireless equipments nearby and make sure they do not interfere with the Mesh unit.

Q 3. Why two Mesh units cannot connection after setup?

Check that "Country/Region" are set the same.
Check that the "Channel/Frequency" are set the same.
Check that "Data Encryption" and "Key" are set the same.

Q 4. The wireless Mesh units becomes unstable, you get ping timed out and lose packet during heavy use?

This situation may occur if the wireless network/units were disturbed by something. Try the following steps:
Check whether every joint point of network is good, such as the Ethernet ports and antenna connection.
Change the Channel/Frequency of the system.
Use Link Test to check the system.
Check to see if there is other wireless equipments disturbing the Mesh unit.
Restart the Mesh unit.
Restore the Mesh unit to its last settings.
Check the network environment for a virus computer.

Q 5. Can I adjust output power?

Use the **Wireless LAN** page to adjust the Output Power.

Output Power Settings

	Full	1/2	1/4	1/8	Min
Output Power	15dbm	12dbm	9dbm	6dbm	3dbm

Q 6. I cannot open the WEB interface for a remote Mesh on local network?

This kind of setup will slow the response of remote Mesh unit WEB Server so just waiting for several minutes or restarting remote Mesh unit. We recommend setting up a Mesh unit through the local wired Ethernet port.

Glossary

802.11g	IEEE802.11g uses the 2.4 GHz frequency for greater range. 802.11g supports bandwidth up to 54 Mbps and is backwards compatible with 802.11b.
Access Point	In a wireless local area network (WLAN), an Access Point is a station that transmits and receives data (sometimes referred to as a transceiver). An Access Point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each Access Point can serve multiple users within a defined network area; as people move beyond the range of one Access Point, they are automatically handed over to the next one. A small WLAN may only require a single Access Point; the number required increases as a function of the number of network users and the physical size of the network.
WEP	Wired Equivalent Privacy is a data encryption protocol for 802.11 wireless networks. All wireless nodes and access points on the network are configured with a 64-bit, 128-bit or 152-bit Shared Key for data encryption.
Access Control	This function is only valid under AP mode, invalid under the mode of bridge graft. Used in MAC address to filter.
Bridge	Bridge is the device that connects and transmits data packets with two subnets by the same protocol and it works in the LLC layer of OSI.
DHCP or DHCP Client or DHCP Server	DHCP stands for "Dynamic Host Configuration Protocol". DHCP purpose is to enable individual computers (DHCP Client) on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.
Encryption	For the security of transmit data in network, the data should be encrypted before transmit and decrypt received data.
IP Address	Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
LAN&WAN	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
MAC Address	Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.
NetBIOS	Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.
Ping	A command line program in Windows, use it to check the connection whether is reachable.
Router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Graphical User Interface (GUI)	In this kind of user interface, user can use Microsoft Internet Explorer or other browser to control, guard and manage the device.
WINS Server	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.